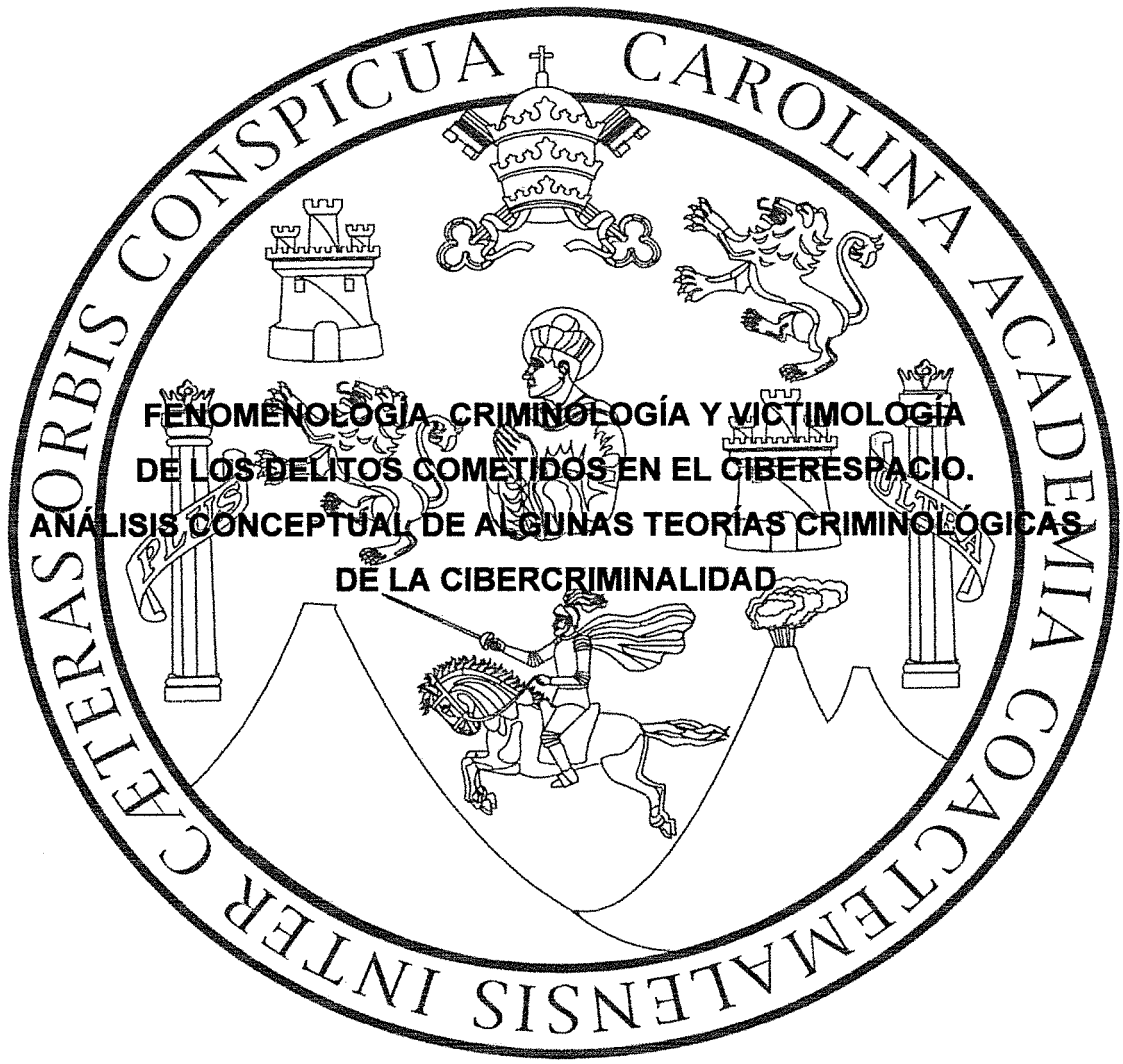
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES



FENOMENOLOGÍA, CRIMINOLOGÍA Y VICTIMOLOGÍA DE LOS DELITOS COMETIDOS EN EL CIBERESPACIO. ANÁLISIS CONCEPTUAL DE ALGUNAS TEORÍAS CRIMINOLÓGICAS DE LA CIBERCRIMINALIDAD

LIC. ROALDO ISAÍAS CHÁVEZ PÉREZ

GUATEMALA, ABRIL DE 2024

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
ESCUELA DE ESTUDIOS DE POSGRADO
MAESTRÍA EN DERECHO PENAL

FENOMENOLOGÍA, CRIMINOLOGÍA Y VICTIMOLOGÍA DE LOS DELITOS COMETIDOS EN EL CIBERESPACIO. ANÁLISIS CONCEPTUAL DE ALGUNAS TEORÍAS CRIMINOLÓGICAS DE LA CIBERCRIMINALIDAD

TESIS

Presentada a la honorable Junta Directiva
de la
Facultad de Ciencias Jurídicas y Sociales
de la
Universidad de San Carlos de Guatemala
Por el licenciado

ROALDO ISAÍAS CHÁVEZ PÉREZ

Tutor
DR. ANÍBAL GONZÁLEZ DUBÓN

Previo a conferírsele el Grado Académico de

MAESTRO EN DERECHO PENAL
(Magister Scientiae)

Guatemala, abril de 2024

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	M.Sc.	Henry Manuel Arriaga Contreras
VOCAL I:	Lcda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Rodolfo Barahona Jácome
VOCAL III:	Lic.	Helmer Rolando Reyes García
VOCAL IV:	Br.	Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br.	Gustavo Adolfo Oroxom Aguilar
SECRETARIO:	Lic.	Wilfredo Eliú Ramos Leonor

CONSEJO ACADÉMICO DE ESTUDIOS DE POSGRADO

DECANO:	M.Sc.	Henry Manuel Arriaga Contreras
DIRECTOR:	Dr.	Luis Ernesto Cáceres Rodríguez
VOCAL:	Dr.	Carlos Estuardo Gálvez Barrios
VOCAL:	Dra.	Herminia Isabel Campos Pérez
VOCAL:	Dr.	William Enrique López Morataya

TRIBUNAL QUE PRACTICÓ
EL EXAMEN PRIVADO DE TESIS

PRESIDENTE:	Dr.	Saúl González Cabrera
VOCAL:	Dr.	Luis Ernesto Cáceres Rodríguez
SECRETARIO:	Dr.	Aníbal González Dubón

RAZÓN: «El autor es el propietario de sus derechos de autor con respecto a la tesis sustentada». (Artículo 5 del Normativo de Tesis de Maestría y Doctorado de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, Escuela de Estudios de Posgrado).

Guatemala, 06 de octubre del año 2023.

Doctor
Luis Ernesto Cáceres Rodríguez
Director Escuela de Estudios de Postgrado
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

Estimado Doctor Cáceres Rodríguez:

Lo saludo respetuosamente deseándole bienestar en sus actividades al frente de la Escuela de Estudios de Postgrado.

Por medio de resolución **RES. D.E.E.P. D. P. 128-2023** de la Dirección de la Escuela de Estudios de Postgrado, de fecha veintiocho de septiembre de dos mil veintitrés, se me nombró para su tutoría, la **Tesis de Maestría en Derecho Penal** del Licenciado **ROALDO ISAÍAS CHÁVEZ PÉREZ**, titulada ***"FENOMENOLOGÍA, CRIMINOLOGÍA Y VICTIMOLOGÍA DE LOS DELITOS COMETIDOS EN EL CIBERESPACIO. ANÁLISIS CONCEPTUAL DE ALGUNAS TEORÍAS CRIMINOLÓGICAS DE LA CIBERCRIMINALIDAD".***

Después de revisar y discutir el informe final que contiene la **Tesis de Maestría en Derecho Penal** del Licenciado **Roaldo Isaías Chávez Pérez** y realizadas las observaciones correspondientes, es mi opinión que su contenido llena los requisitos que exige el Normativo de Tesis de Maestría y Doctorado de la Escuela de Estudios de Postgrado, por lo que emito mi dictamen favorable a la misma, para que continúe el trámite correspondiente y pueda ser defendida en su examen privado.

Quedo a sus órdenes y me suscribo respetuosamente:

DOCTOR ANIBAL GONZÁLEZ DUBÓN

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
ESCUELA DE ESTUDIOS DE POSGRADO

Guatemala, 23 de abril de 2024

Doctor:
Luis Ernesto Cáceres Rodríguez
Director de la Escuela de Estudios de Posgrado
Facultad de Ciencias Jurídicas y Sociales
-USAC-

Distinguido doctor Cáceres Rodríguez:

Con base en su solicitud expresa en la carta a mi persona con fecha cuatro de marzo de dos mil veinticuatro, en donde se me pide dictamen gramatical; asimismo, según los Artículos 7, 9 y 21 del Normativo de Tesis de Maestría y Doctorado de la Escuela de Estudios de Posgrado, de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala.

Le informo que el licenciado: **ROALDO ISAÍAS CHÁVEZ PÉREZ,** de la **Maestría en Derecho Penal**, ha realizado las correcciones y recomendaciones de ortografía, redacción y estilo, a su trabajo de tesis, cuyo título final es: **FENOMENOLOGÍA, CRIMINOLOGÍA Y VICTIMOLOGÍA DE LOS DELITOS COMETIDOS EN EL CIBERESPACIO. ANÁLISIS CONCEPTUAL DE ALGUNAS TEORÍAS CRIMINOLÓGICAS DE LA CIBERCRIMINALIDAD.**

Asimismo, manifiesto que se ha utilizado un léxico adecuado a los requerimientos de una investigación científica, que llene las exigencias de la técnica jurídica y los principios exegéticos y hermenéuticos de la ciencia del Derecho. Esto, en consonancia con las normas, consideraciones y recomendaciones de la Real Academia Española, para utilizar el lenguaje, tecnicismos y neologismos de manera actualizada y como primera fuente teleológica idónea, para el conocimiento.

Dicho trabajo, presenta las partes requeridas en el instrumento legal *supra* anotado, según lo establece la Escuela de Estudios de Posgrado. De esta forma, el sustentante, ha referido con el modelo latino de citas a pie de página, las fuentes bibliográficas, para dejar los créditos de las teorías que han fundamentado la investigación.

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
ESCUELA DE ESTUDIOS DE POSGRADOS

La metodología, técnicas y doctrinas que el estudiante y su parte tutora presentaron, fueron respetadas en su totalidad y ningún planteamiento fue conculcado, para mantener el fundamento teórico original del documento presentado.

De esta manera se procedió con la revisión, exclusivamente en lo que corresponde a la gramática, ortografía, redacción y estilo, para comprobar que el cuerpo capitular contenga los requerimientos y extensión mínimos; con ello, se adecuó la diagramación pertinente y se cotejó el índice, los títulos, subtítulos, la parte conceptual introductoria y las conclusiones, según los enlaces externos que se describen en la bibliografía consultada.

En virtud de lo anterior, se emite: **DICTAMEN FAVORABLE**, a efecto de continuar con el trámite correspondiente.

Cordialmente.

"ID Y ENSEÑAD A TODOS"

Dr. William Enrique López Morataya
Revisor de Gramática
Col. 6144

welm
c. c. interesada/o, archivo.

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

D.E.E.P. ORDEN DE IMPRESIÓN

LA ESCUELA DE ESTUDIOS DE POSTGRADO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, Guatemala, 12 de agosto del año dos mil veinticuatro.----------

En vista de que el Licenciado Roaldo Isaías Chávez Pérez, aprobó el examen privado de Tesis en la **Maestría en Derecho Penal** lo cual consta en el acta número 100-2023 suscrita por el Tribunal Examinador y habiéndose cumplido con la revisión gramatical, se autoriza la impresión de tesis titulada **"FENOMENOLOGÍA, CRIMINOLOGÍA Y VICTIMOLOGÍA DE LOS DELITOS COMETIDOS EN EL CIBERESPACIO. ANÁLISIS CONCEPTUAL DE ALGUNAS TEORÍAS CRIMINOLÓGICAS DE LA CIBERCRIMINALIDAD"**. Previo a realizar el acto de investidura de conformidad con lo establecido en el Artículo 21 del Normativo de Tesis de Maestría y Doctorado.----------

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Facultad de Ciencias Jurídicas y Sociales
Escuela de Estudios de Postgrado
DIRECTOR

Dr. Luis Ernesto Cáceres Rodríguez
DIRECTOR DE LA ESCUELA DE ESTUDIOS DE POSTGRADO

DEDICATORIA

A DIOS:	Por proporcionarme sabiduría para la culminación exitosa de esta meta.
A MIS PADRES:	Casimiro Emilio Chávez (D.E.P.) y Anita Pérez de Chávez, por sus sabios consejos.
A MI ESPOSA:	Mercedes Carrillo de Chávez, por su apoyo y por no soltar mi mano en todo este camino.
A MIS HIJOS:	Cristian, Roaldo y Ana Lucía, con todo mi amor.
A MIS NIETOS:	Jonathan Roberto, Cristian David, José Roaldo y Andrés Emilio, con mucho amor, que este triunfo sea un ejemplo por seguir.
A MI FAMILIA:	Especialmente a mis hermanos Luis Emilio, Luis Adolfo, Hilda Aracely, Sergio Darío y demás familia.
A MIS AMIGOS:	Con cariño y gratitud.
A:	La Tricentenaria Universidad de San Carlos de Guatemala y en especial a la Escuela de Estudios de Posgrado de la Facultad de Ciencias Jurídicas y Sociales.
A USTED, LECTOR:	Con aprecio.

ÍNDICE

Pág.

Introducción i

CAPÍTULO I

1. Fenomenología de los delitos cometidos en el ciberespacio 1
   1.1. Definición de conceptos 1
   1.2. Evolución del concepto de delincuencia informática al de cibercriminalidad 2
   1.3. Los conceptos de "cibercrimen" y "cibercriminalidad" 7
   1.4. El cibercrimen como categoría ontológica 12

CAPÍTULO II

2. La criminología de los delitos cometidos en el ciberespacio 17
   2.1. La criminología del cibercrimen 17
   2.2. El ciberespacio como ámbito del cibercrimen 23
   2.3. El ciberdelincuente 25
   2.4. Objetivos en el ciberespacio 33
   2.5. La vigilancia del ciberespacio 43

CAPÍTULO III

3. La victimología de los delitos cometidos en el ciberespacio..... 49
   3.1. Tipología de cibercrímenes y de cibervíctimas 49
   3.2. Las víctimas en el ciberespacio 53
   3.3. Algunos ámbitos particulares de victimización en el ciberespacio 61
      3.3.1. Comercio y banca electrónica 61
      3.3.2. Redes sociales y medios de comunicación social 64
         3.3.2.1. Conducta de la víctima y cibercriminalidad social 64

CAPÍTULO IV

4. Tipología de algunos delitos cometidos en el ciberespacio atendiendo a la Incidencia de las Tecnologías de Información y Comunicación -TICS- en la conducta criminal 71
4.1. Clasificación de acuerdo a la incidencia de las TIC en la criminología del ciberespacio 71
4.2. Ciberataques puros 73
4.2.1. El hacking 74
4.2.2. Infecciones de malware y otras formas de sabotaje cibernético 80
4.2.2.1. Malware 82
4.2.2.2. Sabotaje de *insiders* 87
4.2.2.3. Ataques DoS 87
4.2.2.4. *Spam* 93
4.3. Ciberataques réplica 94
4.3.1. Los ciberfraudes (*auction fraud* y otros) 95
4.3.1.1. Los ciberfraudes burdos o scam 98
4.3.1.2. El *phishing* 100
4.3.2. *Identity theft* y cibersuplantación de identidad o *spoofing* 110
4.3.3. El ciberespionaje 113
4.3.4. Ciberblanqueo de capitales y ciberextorsión 116

CONCLUSIÓN 119
BIBLIOGRAFÍA 121

INTRODUCCIÓN

Es preciso indicar en este exordio que, para llegar a comprender el cibercrimen y 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. Se debe pensar también, en la relación que guarda el uso del ciberespacio con los extensos patrones de la vida diaria. 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 aquellos que utilizan estos servicios con menos frecuencia.

Con la expansión mundial de Internet, se ha demostrado que esta tecnología facilita la comisión de delitos, aunque su consolidación no haya implicado la aparición de nuevas conductas antisociales o ilícitas. Las clásicas figuras delictivas, ya presentes antes de su irrupción en nuestra realidad diaria, simplemente se han encontrado con un nuevo canal o medio que facilita enormemente su comisión, aunque también su persecución y enjuiciamiento.

No obstante, la generalización del uso de redes de transmisión de datos, en realidad sobre todo de Internet, ha favorecido la utilización de nuevos conceptos en los análisis de lo que puede considerarse es el derecho penal informático, al menos en sentido si no conceptual, sí descriptivo.

Así, un sector de la doctrina empieza a prescindir incluso del término "delito informático" (o delincuencia informática, si se niega la existencia de aquél) para sustituirlo por otros como ciberdelito, ciberdelitos, cibercriminalidad, etc.


ESCUELA DE ESTUDIOS DE POSTGRADO
FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
U.D.C.G.
SECRETARIA

El término *cibercrimen* se ha señalado que describe 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.

Se estaría ante una nueva generación de delitos, que en lugar de tener una vinculación con los sistemas informáticos o, mejor, además de tenerla, se caracterizan por la vinculación que tienen con el uso de redes de transmisión de datos, siendo su relación con los sistemas informáticos secundaria respecto a la que tienen con las redes de transmisión de datos. Es por eso esta vinculación con las redes de transmisión de datos lo que les otorgaría su carácter particular. En todo caso, no puede negarse que todo lo que es cibernético o telemático es también, al mismo tiempo, informático, mientras que no ocurre lo mismo en sentido inverso, siendo por tanto mucho más omnicomprensiva esta última categoría.

El problema investigado se formuló de la forma siguiente: ¿cómo pueden definirse la fenomenología, la criminología y la victimología de los delitos cometidos en el denominado ciberespacio?

La hipótesis se diseñó de la siguiente manera: la fenomenología de los delitos cometidos en el ciberespacio se define como aquellos delitos cuya característica esencial es el rol central que las tecnologías de la información y la comunicación -TIC- juegan en su comisión. Es decir, el papel que la utilización de las TIC tiene que ver con el aspecto esencial del delito; en sentido amplio se trata de una concepción 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.

La criminología de los delitos cometidos en el ciberespacio puede definirse como: a) las causas de la comisión de los delitos en el denominado ciberespacio, la cual tiene que ver con la relación entre la evolución tecnológica y la modificación actual de la delincuencia; y b) la tipología de las conductas criminales o delincuenciales realizadas en el ciberespacio que ha evolucionado del *hacking* a otros tipos como *phishing*, los ciber-fraudes, el *identity theft* o *spoofing*, el *cyber bullying,* el *ciberstalking,* el *online hate speech*, y otras figuras novedosas; así como la prevención de dichos crímenes.

La victimología de los delitos cometidos en el ciberespacio, puede definirse como el estudio de la cibervíctima y su comportamiento; el riesgo delictivo de los bienes jurídicos protegidos y la valoración en el ciberespacio según la teoría de Yar, acerca de las cuatro propiedades conformantes que debe tener un objetivo para ser adecuado (VIVA: *Value, Inertia, Visibility and Accessibility*); 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. Esto, porque desde el punto de vista de la *teoría de las actividades cotidianas*, el comportamiento de la víctima en el ciberespacio es un importante predictor de su victimización.

El presente informe de investigación consta de cuatro capítulos. En el capítulo uno, se analiza el tema de la fenomenología de los delitos cometidos en el ciberespacio; en el

capítulo dos, se trata el tópico de la criminología de los delitos cometidos en el ciberespacio; en el capítulo tres, se desarrolla el problema de la victimología de los delitos cometidos en el ciberespacio; y, en el último capítulo, se realiza la síntesis de la tipología de los delitos cometidos en el ciberespacio, atendiendo a la incidencia de las TIC en la conducta criminal. Por último, se trató de arribar a una conclusión que sea verosímil con la hipótesis formulada en el diseño de la investigación.

CAPÍTULO I

1. Fenomenología de los delitos cometidos en el ciberespacio

1.1. Definición de conceptos

Utilizar en el ámbito científico algunos neologismos (palabras o expresión de nueva creación en una lengua) procedentes de la traducción al idioma español de términos de otros idiomas, deviene en muchos casos inevitable y, en muchas ocasiones, arriesgada, dado que generalmente no es posible una identificación completa de sentidos mediante la traducción de términos procedentes de otros idiomas.

Los académicos que en los Estados Unidos de América, Inglaterra, Australia y algunos otros países han tratado, desde muy diversas ciencias sociales, el fenómeno del denominado *cibercrimen*, no suelen hablar de *cybercriminality*, ni de *cyberdelinquency*, sino de *cybercrime*; en el idioma español, en cambio, se vienen utilizando, indiscriminadamente, los términos cibercrimen, ciberdelito, cibercriminalidad, ciberdelincuencia, en muchos casos para referirse todos ellos a un mismo significado y en otras pretendiéndole otorgar sentidos distintos.

A esto hay que agregar que en el ámbito jurídico y criminológico se utilizan en los países de habla hispana otros conceptos, los de criminalidad informática, delito informático, etc., también procedentes de términos ingleses y alemanes como son respectivamente *computer crime* y *Computerkriminalität*, para referirse, en muchos casos, al mismo fenómeno al que generalmente se hace 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, resulta necesario 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.

Así, se debe analizar 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.

1.2. Evolución del concepto de delincuencia informática al de cibercriminalidad

La categoría de los delitos informáticos, como constructo doctrinal que se usó por la doctrina penal alemana y española durante los años setenta, ochenta, y noventa del siglo XX y al principio de este 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.

"De acuerdo con la caracterización de delitos informáticos, tanto por el medio utilizado, como por el objeto sobre el que recaía el ataque, que conllevaba que formasen parte de la misma tanto aquellos comportamientos delictivos realizados a través de procesos electrónicos, 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, difícilmente podía decirse que los tipos

que la conformaban tuvieran problemas dogmáticos idénticos o, cuanto menos, distintos a los de otras figuras delictivas".[1]

Tampoco la doctrina se empeñaba en buscar algún tipo de identidad de bienes jurídicos en todos los delitos económicos. Siguiendo la categorización de Sieber, "el patrimonio y el orden económico, bienes personalísimos como la intimidad o la libertad sexual, y otros bienes supraindividuales o difusos, se consideraban protegidos por los delitos informáticos".[2]

La categoría de los delitos informáticos, o quizá mejor, de la criminalidad o delincuencia informática, no definía un bien jurídico protegido común a 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 el sabotaje o daños informáticos, el *backing* o acceso ilícito a sistemas informáticos, la sustracción de servicios informáticos, el espionaje informático o la piratería informática de obras del ingenio tipo logias de

---

[1] Corcoy Bidasolo, M.; Joshi, U. **Delitos contra el patrimonio cometidos por medios informáticos.** En: **Revista RJC. No. 3.** Pág. 134.

[2] Sieber, U. **Tecnología de la información y reforma de la ley penal.** Pág. 15.

conducta especifica que la doctrina penal considera merecedoras de respuesta penal y sobre las que se analizaba su posible incardinación en los tipos penales tradicionales o la reforma de los mismos, e incluso la creación de tipos nuevos, para una mejor protección de los intereses dignos de tutela".[3] 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, la denominación de delitos informáticos por la de cibercrimen y cibercriminalidad en referencia esta vez al término anglosajón *cybercrime* procedente de la unión entre el prefijo *cyber*, derivado del término *cyberspace*, y el término *crime*, como concepto que sirve para englobar la delincuencia en el espacio de comunicación abierta universal que es el ciberespacio.

"En inglés, parece estar imponiéndose este término frente a otros como *computercrime*, u otros en los que se utilizan prefijos como *virtual, online, high-tech, digital, computer-related, Internet-related*, electronic, y e-".[4] 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 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.

---

[3] Gutiérrez Francés, M. L. **En torno a los fraudes informáticos en el derecho español**. En: **Revista AIA.** Pág. 7.

[4] De la Cuesta Arzamendi, J. L. **Derecho penal informático.** Pág. 67.

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. Esto ha tenido su correlato en el ámbito legal: a partir del siglo XXI empezaron a preocupar ya no solo la información que pudieran contener los sistemas informáticos y la afectación a la intimidad o el patrimonio que pudiera derivarse del acceso a ella, sino el ciberespacio en el que los mismos interactuaban y los crímenes que allí se producían y que podían afectar a muchos otros nuevos bienes jurídicos como la indemnidad sexual, la dignidad personal o la propia seguridad nacional".[5]

Todo ello, ha llevado a la utilización de un término, el de *cibercrimen*, que logra englobar todas las tipologías de comportamientos que deben estar, y además alcanza mejor que otros el que debe ser un propósito esencial de cualquier concepto que sirve para nombrar a una categoría: "enfatizar aquello que une a todo lo que la conforma que, en este caso, es Internet y las TIC como medio de comisión delictiva".[6]

Al fin y al cabo, si bien internet, la red más popular y a través de la cual se realizarán prácticamente todas estas infracciones, es en sí misma un medio informático y, por tanto, todos los ciberdelitos podrían entrar dentro de la categoría de los delitos informáticos, "con la utilización del término cibercriminalidad se pone de manifiesto que sus implicaciones de riesgo van más allá de la utilización de tecnologías informáticas y se relacionan mucho más con el hecho de que estos comportamientos están unidos en

[5] Wall, D. **Cibercrimen: la transformación del crimen en la era de la información.** Pág. 44.
[6] Clouch, J. **Principio del cibercrimen.** Pág. 409.

la actualidad a redes telemáticas, con los particulares problemas político-criminales que ello plantea en la actualidad".[7]

Además, al tener en cuenta no solo el aspecto *informacional* sino también el comunicativo de las TIC, se hace referencia a un catálogo más amplio de infracciones que incluye las que se relacionan con el mal uso de las comunicaciones personales entre particulares a través de redes telemáticas o con la introducción y mala utilización de 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, 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.

[7] Quintero Olivares, G. **Internet y derecho penal. Imputación de los delitos y determinación de la competencia. La Ley Penal.** En: **Revista de derecho penal.** Pág. 6.

1.3. Los conceptos de "cibercrimen" y "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.

Resulta claro 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, entonces, 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) relacionadas con el ciberespacio (sentido tipológico), o para tratar de 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)".[8]

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 Artículo 1973, que sanciona el acceso informático ilícito, o el del Artículo 183 *bis*, que castiga el denominado *online child grooming.*

Evidentemente ambos sentidos, el tipológico y el normativo, son aceptables, y será el contexto el que determine que se está 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 Código Penal 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, 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, 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 y que, en todo caso, puede

[8] Maíllo, A. **Introducción a la criminología.** Pág. 68.

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".[9]

El cibercrimen (o la cibercriminalidad) 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 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 nivel internacional, para la prevención de su realización y la mejor investigación procesal de las mismas".[10]

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 se esté ante un cibercrimen no bastará con que se utilicen las TIC para realizar el comportamiento criminal, sino que se exigirá que tal uso

---

[9] Yar, M. **Cibercrimen y sociedad.** Pág. 9.

[10] Romeo Casabona, C. M. **El cibercrimen: nuevos retos jurídicos-penales, nuevas respuestas político-criminales.** Pág. 8.

tenga que ver con algún elemento esencial del delito. No se está 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". Este 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.

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.* Es opinión del sustentante que en ambos casos el uso es correcto y que el contexto permite diferenciar uno u otro sentido.

Más relevante es, en cambio, la cuestión de la concepción amplia o restringida del cibercrimen (o de la cibercriminalidad). Estas dos concepciones son aplicables tanto al

sentido normativo como al tipológico, pero es en relación con este último donde tal diferenciación adquiere más importancia.

Pues bien, si se utiliza el término de forma amplia, se puede definir como cibercrimen cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo además por este último 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, se utiliza el término de forma restringida, y si bien se pueden utilizar variados criterios para restringir la categoría, lo usual será acudir a la propia idea de la realización del delito por medio de las TIC. Conforme a esto, se estará 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.

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

lesiva de los intereses económicos de la víctima solo puede realizarse por medio de Internet".[11]

1.4. El cibercrimen como categoría ontológica

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

Es este 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 describe el cibercrimen como "aquel delito cuya característica esencial es el rol central que las TIC juegan en su comisión".[12] 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 solo 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

[11] Wall, D. S. **¿Qué son los cibercrímenes?** Pág. 59.
[12] Yar, M. **Op. Cit.** Pág. 9.

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 las teoría del cibercrimen, 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 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 solo 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".[13]

Por consiguiente, desde este punto de vista, se entiende por cibercrimen cualquier delito en el que las TIC juegan un papel determinante en su con creta 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.

Se debe reconocer que no todos los comportamientos que se integran dentro de las diferentes tipologías de cibercrímenes pueden ser reputados delictivos conforme a la mayoría de sistemas penales. 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 signifcativos, 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 esa tesitura, la idea es un estudio criminológico del cibercrimen en el que no se analizan figuras delictivas, sino modalidades de comportamiento. Esto significa que se harán referencias 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 conllevan dinámicas comisivas complejas repletas de pasos previos, que en algunos casos podrán ser reputados como tentativas delictivas y

[13] Jewkes, Y. **Cibercrimen.** Pág. 106.

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.

Además, es importante analizar 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, interesa el cibercrimen como una categoría amplia en aras a la prevención del mismo, de modo que limitarse a las conductas que están presentes en el Código Penal resultaría contradictorio con estos objetivos.


ESCUELA DE ESTUDIOS DE POSTGRADOS
FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
USAC
SECRETARIA

CAPÍTULO II

2. La criminología de los delitos cometidos en el ciberespacio

2.1. La criminología del cibercrimen

Es algo sorprendente, y para otros también criticable, 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, que conlleva la constatación de un espacio de oportunidad criminal cuya identificación y análisis puede ser esencial a efectos preventivos".[14]

Sin embargo, en esto último es en lo que la criminología parece estar centrando sus esfuerzos los últimos años. Así, y "si bien se pueden encontrar en los últimos diez años

[14] Serrano Maíllo, A. **Oportunidad y delito.** Pág. 200.

interesantes estudios de criminología aplicada a la cibercriminalidad en las que se manejan teorías como la del autocontrol, la decisión racional, la del aprendizaje social, el control social o el etiquetamiento, 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, la teoría de las actividades cotidianas de Cohen y Felson".[15]

En realidad, tiene sentido si se toma en consideración que la teoría de las actividades cotidianas, como parte del germen de todas las actuales teorías de la oportunidad o del día a día que en los últimos años "parecen estar en el centro de los principales debates criminológicos superando las expectativas que se marcaban para la criminología ambiental y que han dado lugar, en conjunción con la teoría de la decisión racional, a los desarrollos sobre la prevención situacional del delito, 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".[16]

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

---

[15] Cohen, L.; Felson, M. **Cambio social y tendencias de la tasa de delincuencia: un enfoque de actividad rutinaria.** En: **Revista de derecho penal y criminología.** Pág. 98.

[16] Garrido, V; Stangeland, P.; Redondo, S. **Principios de criminología.** Págs. 56 y 2006.

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 este el que el delito dependerá de la relación entre víctimario, víctima y mecanismos de protección, divergirá en la manifestación concreta de estos mismos factores, fruto de la especialidad del medio en que convergen.

En todo caso, lo que hace especialmente apta esta teoría, 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".[17]

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".[18] Es obvio que este enfoque tiene especial sentido ante un tipo de criminalidad como el que se 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 solo 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*, 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.

---

[17] Garland, D. **La cultura del control. Crimen y orden social en la sociedad contemporánea.** Pág. 128.
[18] Medina Ariza, J. J. **El control social del delito a través de la prevención situacional.** En: **Revista de derecho penal constitucional.** Pág. 281.

"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, pero también lo es que aquellas teorías que ponen más énfasis en la relación de lo ambiental o espacial con la propia motivación del criminal reflejarán mejor los cambios que puede suponer para el crimen como evento el que el lugar de realización sea el ciberespacio".[19]

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.

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 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.

---

[19] 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.** Pág. 3.

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

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, al humilde parecer del sustentante, 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 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: solo 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, lo cual se hacía de manera implícita, pero no explícitamente, con la teoría de las actividades cotidianas que es perfectamente apta para explicar el evento cibercrimen.

2.2. El ciberespacio como ámbito del cibercrimen

"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".[20] Por supuesto, el lugar de comisión de un crimen puede ser el ciberespacio que difiere en su arquitectura del espacio físico en el que solo 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, 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 elementos, será distinto.

Por lo anterior, 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 altera los factores del crimen, pero sí la concreta

[20] Cohen, L. E.; Felson, M. **Op. Cit.** Pág. 590.

expresión de los mismos y, por tanto, de múltiples elementos que deberían ser tomados en consideración en aras a la prevención del delito.

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, se debe 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, la TAC aporta la idea de que para la comprensión del delito no solo 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 cibercrimen, como el delito en el espacio físico, es la confluencia de las partes en el todo.

2.3. El ciberdelincuente

"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".[21] 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 cercanía entre agresor y víctima para la (ciber) delincuencia tal y como sí se requería generalmente en el espacio físico. Mientras que lo usual en la criminalidad suele ser que el delincuente realice el delito cerca de su propia residencia, 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.

---

[21] 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: **Revista electrónica de ciencia penal y criminología.** Pág. 39.

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, 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 expandiéndose, por tanto, el ámbito potencial de oportunidad criminal.

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".[22]

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

---

[22] Bottoms, A. E.; Wiles, P. **Criminología ambiental.** En: Maguire, M.; Gan, R.; Reiner, R. **Manual de criminología.** Pág. 323.

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 *backers* 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, costos 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. Así, mientras que el criminal en el espacio físico tiene que tener en cuenta el costo, 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 señalar que "las TIC pueden actuar como un multiplicador de fuerza que hace que personas con mínimos recursos puedan generar grandes daños para múltiples personas y bienes en el ciberespacio".[23] Además, la expansión del ámbito comunicativo al que puede acceder un agresor motivado supone el ciberespacio conlleva una multiplicación de la potencialidad lesiva que de una conducta por comparación con lo que ocurre en el espacio físico.

Aunque hay armas sofisticadas que permiten causar daños a múltiples bienes en el espacio físico y real, lo general es que la producción de da nos a bienes existentes en lugares distintos (y desde luego en países distintos seria 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, pues el agresor puede no solo 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.

---

[23] Yar, M. **La novedad del ciberdelito: una evaluación a la luz de la teoría de la actividad rutinaria.** En: **Revista electrónica de derecho penal y criminología.** Pág. 411.

Además, el ciberespacio no solo 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.

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.

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. Por último, "el agresor puede utilizar uno o múltiples sistemas informaticos 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".[24]

Todo eso, por supuesto, ejecutado por el agresor desde y sobre cualquier parte del mundo. 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

[24] McQuade, S. C. **Cibercrimen.** En: Maguire, M.; Gan, R.; Reiner, R. **Op. Cit.** Pág. 482.

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, y al unir el ciberespacio a miles de millones 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".[25] 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.

Además, 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.

Asimismo, 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.

---

[25] Hutchings, A.; Hayes, H. **Teoría de la actividad rutinaria y victimización por *phishing*: ¿quién es atrapado en la "red"?** Pág. 435.

A esto es a lo que, al 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".[26] Propiamente el agresor motivado no desaparece, sino 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 este 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.

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 in mediatamente, y sin quererlo, en emisor de un nuevo ataque en una cadena sucesiva que ni siquiera es controlada por el propio autor del crimen.

[26] Alshalan, A. **Miedo al cibercrimen y victimización: análisis de una encuesta nacional.** Pág. 146.

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 que tiene que acceder a la comunicación, con la transmisión de contenido el 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".[27]

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.

Por otra parte, "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 ofrecer un refugio aparentemente seguro en el que ocultarse, lo cual a su vez le permite reinventarse y adoptar nuevos personajes virtuales con los que quizá, cometer delitos".[28] 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, frenos de la motivación criminal que le convierten en un *motivated offender*.

[27] Agustina Sanllehí, J. R. **La arquitectura digital de internet como factor criminógeno.** En: **IEJCS.** Pág. 9

[28] Yar, M. **Op. Cit.** Pág. 421.

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".[29] Porque no solo 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. De momento, sin embargo, ello no parece posible, pues el anonimato no solo sirve a propósitos criminales, sino también a otros lícitos relacionados con la sencillez de la accesibilidad al ciberespacio que difícil mente sería compatible con otros sistemas de identificación que, además, podrían ser sencillamente falseados.

2.4. Objetivos en el ciberespacio

En realidad, lo que se ha afirmado hasta el momento del agresor motivado tiene consecuencias directas en el elemento "objetivo adecuados": el crecimiento del ámbito de riesgo no es solo 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

[29] Pittaro, M. L. **El acoso cibernético: un análisis sobre el acoso y la intimidación en línea.** En: **Revista de victimología.** Pág. 189.

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 solo es figurativa: no hay motivación sin objetivo y viceversa.

En todo caso, debe precisarse lo que supone el incremento potencial de las posibilidades de contacto entre agresor y víctima en el ciberespacio, 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.

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.

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[30] para definir los bienes preferidos por los ladrones (*Concealable, Removable, Available, Valuable, Enjoyable and Disposable),* 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 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

[30] Clarke, R. V. **Productos: comprender, anticipar y reducir la demanda de productos robados.** Pág. 23.

ejemplo, se pueden 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 a menores.

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.

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 victimización. 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 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".[31]

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

[31] Jaishankar, K. **Cibercriminología. Explorando los crímenes de internet y el comportamiento criminal.** Pág. 269.

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.

Se encuentra aquí, pues, la primera divergencia de las condiciones que hacen adecuado un objetivo para el cibercrimen, con las que, con el acrónimo VIVA, Felson definió como condiciones o criterios que reflejar la adecuación del objetivo para el delito: "el valor del objetivo del crimen, su inercia, la visibilidad física del mismo y su accesibilidad. La diferencia estriba en que previamente a todo ello, la introducción del objeto por parte de la propia víctima en el ciberespacio es condición primera y principal para su adecuación al cibercrimen".[32]

Ahora bien ¿y los demás caracteres del acrónimo VIVA? ¿Son válidos para el cibercrimen? Se tratará 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.

---

[32] Felson, M. **Crimen, oportunidad y vida diaria.** Pág. 55.

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 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".[33] 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.

[33] **Ibid.** Pág. 56.

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".[34] Al parecer, el intento de Yar es vano. La evolución actual de las TIC contradice lo que afirma, y salvo en casos excepcionales los bienes en el ciberespacio apenas se diferenciarán 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".[35] 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, 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".[36] Si a ello se agrega 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.

---

[34] Yar, M. **Op. Cit.** Pág. 420.
[35] Felson, M. **Op. Cit.** Pág. 58.
[36] Yar, M. **Op. Cit.** Pág. 421.

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. Señala Yar que "es esencia del ciberespacio su carácter público, por lo que todo en él está visible a nivel mundial".[37] Esto solo 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 de 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. Alshalan, 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 backing,* con la interacción de la

[37] **Ibid.**

víctima en el ciberespacio concretada en su frecuencia de acceso y el tiempo pasado en Internet". [38]

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 y, exclusivamente para la infección por virus, con el hecho de tener hijos que acceden al ciberespacio".[39]

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 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".[40]

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. También por medio de un estudio empírico de ecuaciones estructurales para la evaluación de la relevancia de

---

[38] Alshalan, A. **Op. Cit.** Pág. 123.
[39] **Ibid.** Pág.126.
[40] Yucedal, B. **Victimización en el ciberespacio: una aplicación de las teorías de exposición a la actividad rutinaria y al estilo de vida.** En: **Revista electrónica de ciencia penal y criminología.** S. p.

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".[41]

Y esto es así con otro tipo de cibercrímenes. Así, en un estudio de Ybarra 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, y ya hemos visto anteriormente que también había una intensa relación entre la interacción de la víctima en chats y demás con la victimización por online *grooming* o delitos similares".[42]

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 solo 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 esta "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.

---

[41] Choi, K. **Victimización por delitos informáticos y teoría integrada: una evaluación empírica.** En: **Revista latinoamericana de estudios de seguridad.** Pág. 321.

[42] Ybarra, M. L.; Mitchell, K. **Exposición a la pornografía de internet en niños y adolescentes: una encuesta nacional.** Pág. 473.

Se hace patente, pues, que las condiciones para la adecuación del objetivo del crimen VIVA no son transportables al ciberespacio, excepto en el caso del valor. Este 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, 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.

2.5. La vigilancia del ciberespacio

No se puede 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. Se hace referencia 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 se han 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, 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.

Como señalaron Farrell y Pease, "la noción de guardián capaz se convierte en importante, pero también compleja, cuando pensamos en el cibercrimen".[43] 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 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.

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

[43] Farrell, G.; Pease, K. **Criminología y seguridad.** En: Grill, M. **Manual de seguridad.** Pág. 43.

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. Estos 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.

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"[44] y a las mismas conclusiones llega Choi respecto al que él considera elemento esencial de la TAC.

Pero se trata en todo caso, y a criterio del sustentante, de unos guardianes capaces íntimamente ligados con el elemento objetivo adecuado: no son sistemas de protección incorporados o que funcionen de forma autónoma al comportamiento del propio sujeto

[44] Yucedal, B. **Op. Cit.** Pág. 117.

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"[45] generalmente eran cercanos a la víctima (vecinos, ciudadanos anónimos, etc.), 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 preponderan te en el caso del cibercrimen, dado que de ella depende en parte, no solo 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.

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.

---

[45] Cohen, L.; Felson, M. **Op. Cit.** Pág. 590.

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".[46] 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.

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.

---

[46] Grabosky, P. **Criminalidad virtual: vino viejo en nuevas botellas.** En: **Revista de ciencia política.** Pág. 68.

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.

CAPÍTULO III

3. La victimología de los delitos cometidos en el ciberespacio

3.1. Tipología de cibercrímenes y de cibervíctimas

Se debe recordar que, al hablar de cibercriminalidad, se hace en sentido amplio como concepto que engloba 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 interesan, la variedad de objetivos sobre los que pueden actuarlas, 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, se estima 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. Estos 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 se vive, 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 participes de ataques de todo tipo a otros usuarios, empresas o instituciones públicas. Los principales 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".[47]

[47] Pratt, T. C.; Holtfreter, K; Reisig, N. D. **Op. Cit.** Pág. 283.

3.2. Las víctimas en el ciberespacio

La víctima y su comportamiento son siempre elementos determinantes del evento criminal acontecido. Sin embargo, 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 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 se tiene en cuenta, además, que también al no existir distancias en internet, el desplazamiento del cibercriminal hacia otros objetivos resulta no solo 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 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)*[48] 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.[49] 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 cyberbarassment,* extorsión y *backing.*

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 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

[48] Yar, M. **Op. Cit.** Pág. 421.
[49] Alshalan, A. **Op. Cit.** Pág. 123.

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 pro grama, cargue involuntariamente el virus; y, derivado de la segunda, que el uso de instrumentos digitales de seguridad tales como cortafuegos, antivirus o programas antispyware como guardianes capaces puede determinar su riesgo de victimización".[50]

Este estudio de Yucedal, en realidad apenas difiere, excepto en el objeto, del que, a criterio del sustentante, 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.

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

[50] Yucedal, B. **Op. Cit.** Pág. 117.

ordenadores personales que no tienen instalados programas de seguridad informática, que utilizan mucho Internet y que realizan conductas de riesgo en línea".[51]

Pese que hay otros autores, como Marcum, Bossler y Holt[52] que han obtenido resultados contradictorios con respecto a la tenencia de sistemas de seguridad informática, donde no tenerlos no reduce la victimización, incluso llegando al extremo contrario, donde tener un antivirus correlaciona positivamente con la victimización de malware, 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, solo 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) que en la mayoría de los casos un ordenador infectado no muestra síntomas fácilmente reconocibles por el usuario, y que solo 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

[51] Choi, K. **Op. Cit.** Pág.321.
[52] Bossler, A. M.; Holt, T. J. **Actividades en línea, tutela e infección por malware. IJCC.** Pág. 400.

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, pero también descargar software, juegos o media pirata",[53] realizar determinadas actividades de ocio como comprar pasar más horas conectados, visitar páginas web para adultos, realizar comportamientos desviados como acceder de forma ilícita a sistemas informáticos, modificar archivos de otros, realizar *cyberstalking*, piratear media y proporcionar información personal supone un riesgo como por ejemplo, el nombre completo, el estado civil, la orientación sexual, colgar fotos

[53] Yucedal, N. **Op. Cit.** Pág. 23.

personales y vídeos en las redes sociales o divulgar el número de tarjeta de crédito a través de mensajes.

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 demográficos 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 "esta 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".[54]

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 las mujeres, lo cual 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".[55]

Trabajos posteriores han tenido resultados diferentes frente a la variable género, donde los investigadores han tratado de solventar estas discrepancias atribuyéndolo a los

---

[54] Marcum, C. D. **Teoría de la victimización de adolescentes online y construcciones de actividades de rutina.** Pág. 26.
[55] Alshalan, A. **Op. Cit.** Pág. 83.

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*".[56] La causa no es el comportamiento de las mujeres en Internet, sino que los ciberacosadores las perciben como un objetivo atractivo (*atracctive target*).

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*; 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).

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. Como explica Yucedal, "los hombres con mayor nivel de educación participan en más actividades básicas (uso de correo

[56] Bossler, A. M.; Holt, T. J. **El efecto del auto control sobre la victimización en el ciberespacio.** En: **Diario de Investigación sobre crimen y delincuencia.** Pág. 227.

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)".[57]

También está generalmente admitido 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".[58] 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.

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".[59]

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 sí más tiempo pasado supone una mayor exposición en la medida que correlaciona positivamente con

---

[57] Yucedal, B. **Op. Cit.** Pág. 140.
[58] Pratt, T. C.; Holtfreter, K.;Reisig, N. D. **Op. Cit.** Pág. 283.
[59] Alshalan, A. **Op. Cit.** Pág. 146.

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.

3.3. Algunos ámbitos particulares de victimización en el ciberespacio

3.3.1. Comercio y banca electrónica

Los estudios de victimización que se han 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 backing 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 estas 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".[60] 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".[61] Si se tiene en cuenta que el número de usuarios de Internet que realizan transacciones económicas utilizando la red sigue incrementándose, se puede comprender la importancia de este factor y la necesidad de incrementar la protección para los compradores en el ciberespacio.

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,

[60] Pratt, T. C.; Holtfreter, K.; Reisig, N. D. **Op. Cit.** Pág. 281.
[61] Marcum, C. D. **Op. Cit.** Pág. 370.

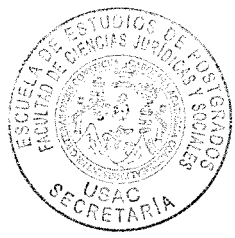
además, ocupan niveles de ingresos más bien altos".[62] De hecho, parece que existe una relación entre tener altos ingresos y tener un nivel formativo más alto, con el hecho de comprar más por medios online. Y aún más clara parece la relación entre el género y la actividad de compra online.

Según todos los estudios, los hombres suelen hacer más compras online que las mujeres. 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 se tiene en cuenta que muchos de los ciberfraudes existentes tienen que ver con esta actividad (los fraudes de subasta y otros, como se vio, 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.

---

[62] Ratchford, B. T.; Talukadar, D.; Lee, M. **Un modelo de elección del consumidor de internet como fuente de información.** Pág. 8.



3.3.2. Redes sociales y medios de comunicación social

3.3.2.1. 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. Sin embargo, 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), donde 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 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 videos 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".[63]

Además, hay algunas conductas en particular que entrañan especial riesgo, como puede ser el compartir con extraños los datos personales en internet. En todo caso, es

[63] Reyns, B. **Ser perseguido en línea alcance y naturaleza de la victimización del ciberstalking de un estilo de vida.** S. P.

necesario y 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 este 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 esta la razón definitiva, son los jóvenes los que de forma más generalizada usan las herramientas de intercomunicación social existentes en el ciberespacio, y no solo 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 se ha denominado cibercriminalidad social o personal. Se hipnotiza a que los jóvenes son más victimizados por el tipo de actividades que realizan, sin embargo, Ngo y Paternoster afirman que "a mayor edad, más probabilidad de sufrir una infección de malware y de sufrir difamación en línea".[64]

Puede ser también que como apuntan Bossler y Holt, "para las mujeres en el harassment, los jóvenes de por sí pueden ser un blanco atractivo (sobre todo en

[64] Ngo, F.; Paternoster, R. **Victimización por delito cibernético: un examen de los factores de nivel individual y situacional. IJCC.** Pág. 783.

ciberacoso sexual)".[65] 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.

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, 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 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 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, en el que detectaron que un 41 por 100 de los encuestados de una muestra válida de 974

[65] Bossler, A. N.; Holt, T. J. **Examen de la aplicabilidad de la teoría de actividades rutinarias de estilo de vida para la victimización por delito cibernético.** Pág. 16.

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 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".[66] 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 que no están casadas o divorciadas.

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 *cyber stalking* frente a al 32 por 100 de los hombres".[67] También tienen más riesgo los jóvenes porque están conectados a una variedad de medios electrónicos para comunicarse.

---

[66] Bocij, P. **Víctimas del ciberstalking: un estudio exploratorio del acoso perpetrado a través de internet.** Pág. 23.
[67] Reyns, B. **Op. Cit.** Pág. 149.

En todo caso el predictor que Ryens ha 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 previamente 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.

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 contacto con extraños.

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.

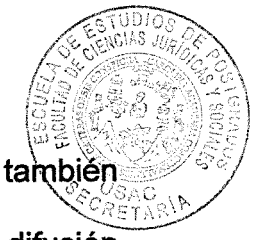
CAPÍTULO IV

4. Tipología de algunos delitos cometidos en el ciberespacio atendiendo a la Incidencia de las Tecnologías de Información y Comunicación -TICS- en la conducta criminal

4.1. Clasificación de acuerdo a la incidencia de las TIC en la criminología del ciberespacio

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 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".[68]

Se trata, al igual que las sistematizaciones que se han desechado y de otras muchas de una clasificación de carácter débil, en cuanto que la misma debe servir solo 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 se denominarán *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 se hace referencia 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

[68] Wall, D. S. **Op. Cit.** Pág. 59.

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 dificulta des 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 este, sin embargo, de identificar las diferentes modalidades de cibercriminales, situándose en estas tres categorías definidas al efecto.

4.2. 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 solo en ese ámbito que es Internet. A los efectos que interesan, lo que esto supone es el surgimiento en internet de todo un conjunto de conductas ilícitas, 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.

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 solo

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.

4.2.1. El hacking

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, consiste 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 ciento 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. Generalmente los data breaches se realizan como forma de espionaje informático y entrarían ya, pues, en el otro tipo de ataques". [69]

Se podría describir el *backing* 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

---

[69] Baker, W. **Informe de investigaciones de incumplimiento de datos 2010. Un estudio realizado por el equipo de Verizon Risk en cooperación con los servicios secretos de los Estados Unidos.** Disponible en: https://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf

que tiene capacidad potencial de utilizarlo o de acceder a cualquier tipo de información que esté en el sistema.

El hacking, en este sentido amplio, es la actividad de los hackers consistente en la superación de cualquier barrera informática, bien sea para el acceso a un sistema, 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, "se puede hablar de *backing* 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".[70]

El *backing*, en el sentido estricto que ahora interesa de acceso a los sistemas informáticos, se puede llevar a cabo de muy distintas formas, si bien generalmente, el

[70] Wall, D. S. **Op. Cit.** Pág. 59.

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 involuntaria mente 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 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 este 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.

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 se diga 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, descubriendo sus carencias o sus posibilidades y haciéndolo más seguro o más abierto, según las preferencias y necesidades"[71]. Con el paso del tiempo, sin embargo, se ha ido asociando socialmente la idea de hacking a la propia cibercriminalidad.

La razón 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 tradicional mente 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

[71] Rosenzweig, R. **Magos, burócratas, guerreros y hackers: escribiendo la historia de internet.** En: **AHR.** Pág. 153.

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 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 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 *backing*.

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 solo 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, puede llevar a la desaparición de una forma de proceder en Internet que ha sido esencial para la creación y consolidación del sistema, 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".[72]

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, 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 llevado, por una parte, a una relativización de la significación del hacker, que ya no es uno entre millones sino tan solo 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.

---

[72] Ortiz de Urbina, Gimeno, I. **Memento práctico penal y económico de la empresa 2011-2012.** Pág. 92.

Si a esto se une 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 des aparición, 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.

4.2.2. 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*",[73] 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

[73] Romeo Casabona, C. M. **Los delitos de daños en el ámbito informático.** En: **CPC. Memento práctico penal y económico de la empresa 2011-2012.** Pág. 91.

datos de terminales concretos y determinados, con fines industriales o de daño individual.

Íntimamente relacionado con este sabotaje informático se debe identificar el sabotaje cibernético, por otros denominado *cibervandalismo*, inclusivo 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 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".[74]

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 solo 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 con un 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.

4.2.2.1. 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.

---

[74] **Ibid.** Pág. 93.

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. Además, no solo 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".[75]

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.

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

[75] Hoar, S. B. **Tendencias en cibercrimen: el lado oscuro del internet.** En: **Justicia criminal.** Pág. 5.

que en realidad espían nuestros hábitos en Internet (qué páginas se visitan, cuando se conectan las personas, qué programas se bajan, 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 los noventa 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".[76] 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 in formación 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 eco nómicamente 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

[76] Hughes, L. A.; DeLone, G. J. **Virus, gusanos y caballos troyanos: ¿crímenes graves, molestos o ambos?** En: **SSCR.** Pág. 79.

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 con figuración 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".[77]

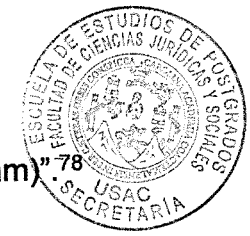
La auténtica amenaza que supone en la actualidad la infección de malware no deriva tanto del sabotaje a los sistemas o a los datos y las pérdidas que ello puede conllevar,

[77] **Ibid.** Pág. 82.

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 hacker 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 de más, 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*). "Una botnet puede ser instruida por su controlador para realizar funciones de muy diverso tipo, entre las que destacan los ataques de denegación de servicio, 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)".[78] 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 infectados como *bots*, el doble de lo que había reparado durante el segundo trimestre de 2009.

4.2.2.2. 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 esta, 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.

4.2.2.3. 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 sepa rada 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

[78] Pinguelo, F. M.; Muller, B. W. **Crímenes virtuales, daños reales: un primer sobre los delitos cibernéticos en estados unidos y los esfuerzos para combatir los cibercriminales.** En: **VJLT.** Pág. 133.

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 solo 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 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".[79]

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. 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 incluso como forma de perjudicar a un competidor en algún tipo de servicio en Internet.

En los últimos años, sin embargo, también se han utilizado este tipo de ataques con finalidades de hacktivismo político, esto es, de difusión de mensajes de protesta en internet generalmente dirigidos contra organismos o Estados que, según las comunidades de usuarios de Internet, ponen en riesgo la idea del ciberespacio abierto que ellos defienden. En 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

[79] Sinrod, E. J.; Reilly, W. P. **Los delitos cibernéticos: un enfoque práctico para la aplicación de las leyes federales sobre delitos informáticos.** Pág. 4.

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. 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. 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".[80]

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".[81] Evidentemente, el peligro de estos ataques es mucho mayor, puesto que complican las estrategias defensivas del servidor

[80] Maciá Fernández, G. **Ataques de denegación de servicio a baja tasa contra servidores.** Pág. 63.
[81] Sinrod, E. J.; Reilly, W. P. **Delitos cibernéticos: un enfoque práctico para la aplicación de las leyes federales sobre delitos informáticos.** Pág. 45.

o sistémico 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.

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 backtivismo político, la denegación de servicios supondrá la negación de la libre expresión de contenidos en la Red. "En todos ellos, sin embargo, no solo 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".[82] Esto hace que la DoS sea una coacción (sin violencia, eso sí) 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,

[82] Morales García, O. **Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del consejo de Europa sobre cyber-crime.** En: **CDJ.** Pág. 31.

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.

Por tanto, si se suma el DoS a los otros ataques analizados dentro de ese cajón de sastre denominado sabotaje cibernético, y se realiza una recapitulación acudiendo a la terminología de los bienes jurídicos protegidos se puede 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 socioeconómico 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.

Ya en el plano del 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 determinado momento.

Evidentemente, no todo sabotaje informático causa tales daños. Más bien, debido a los sistemas de seguridad existentes, tanto en forma de anti virus 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.

4.2.2.4. *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 bote 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".[83]

Pese a que el principal riesgo que conlleva la recepción de correos *spam* estriba en la posibilidad de ser infectado por algún tipo de *ware* que sea posteriormente utilizado para defraudar a la víctima, tampoco debe despreciarse la enorme gravedad que supone el mero hecho de recibir corre indeseados en el caso de ser infectado por ellos.

Según un estudio sobre los costes económicos del *spam*, este representa un coste para las empresas de Estados Unidos de casi 9000 millones de dólares al año, 2500 millones para las de Europa y 500 millones para los prestadores de servicios. Estas macrocifras aún llaman más la atención cuando se concretan en el coste para las empresas que supone la limpieza de *spam*: entre 600 y 1000 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.

4.3. Ciberataques réplica

Además de los intereses y bienes surgidos en el ciberespacio, este 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 se debe sumar, como realizadas en él,

---

[83] Yeargain, J. W.; Settoon, R. P.; McKay, S. E. **Acto de spam 2003: como spamear legalmente.** En: **JSeC.** Pág. 15.

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 punto de que lo que en el espacio territorial podía apenas tener relevancia dañina, puede adquirirla significativamente en el espacio virtual.

4.3.1. 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; las estafas de inversión; las estafas piramidales realizadas a través de Internet. las conocidas estafas de la lotería; 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".[84] Una variedad de fraudes que va transformándose (o adaptándose, conforme a la terminología que utilizaremos más tarde constantemente.

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 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 in formar sobre la reputación de los vendedores. Cada una de estas acciones puede ser objeto de fraude.

---

[84] Stadler, W. A. **Fraude en internet.** En: **Fisher, B. S.; lab, S. P. Enciclopedia de victimología y prevención del crimen.** S. P.

Chua y Wareham 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 pos subasta 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".[85]

4.3.1.1. 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".[86] Es esta más bien una categoría genérica que podría englobar a casi todos los fraudes, si bien se suele utilizar como referencia de los más burdos de ellos, aquellos en los que el engaño es poco elaborado y en los que el error de la víctima puede ir más allá de lo común.

En este caso se podría 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

---

[85] Chua, C. E. H.; Wareham, J. **Lucha contra el fraude de las subastas en internet. Una computación de evaluación y propuesta.** Pág. 32.
[86] YAR, M. **Op. Cit.** Pág. 81.

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.

De este modo, los ciberdelincuentes basan sus mensajes en ciertos principios del comportamiento humano que han sido estudiados, entre otros, por Stajano y Wilson.[87] 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 de los equipos.

---

[87] Stajano, F.; Wilson, P. **Comprendiendo a las víctimas de fraude: siete principios para la seguridad de sistemas.** Pág. 9.

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.

4.3.1.2. 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, o pesca de incautos, definido por el grupo mundial antiphishing como el mecanismo criminal que emplea ingenie ría social y subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias".[88]

[88] Jaishankar, K. **Crímenes relacionados con la identidad en el ciberespacio: examinando el phishing y su impacto.** En: **IJCC.** Pág. 12.

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, en un mensaje en el que se hacía referencia al phishing en el ámbito de la creación fraudulenta de cuenta tas de usuario de American Online (AOL). 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[89] 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

[89] Gordon, S.; Chess, D. M. **Donde hay humo hay espejos: la verdad sobre los caballos trojanos en internet.** En: **Revista electrónica de derecho penal y criminología.** S. P.

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.

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 screenloggers; en 2004 utilizaron por primera vez una web falsa y desde 2006 es habitual el phishing por VoIP".[90] Esta evolución no solo 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.

De igual modo, se ha producido una especialización en los delincuentes que realizan este tipo de estafas: no es extraño encontrar grupos de ciberdelincuentes que se organizan diferenciando entre mensajeros, recolectores y cajeros. Los primeros, bien sean *spammers* o *backers*, remiten un gran número de correos, general mente 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.

---

[90] Ollman, G. **La guía del phishing: entendiendo y previniendo los ataques de phishing.** Pág. 34.

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".[91] 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, mensaje en una red social e incluso en videojuegos con múltiples participantes. 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, se puede 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

[91] Myers, S. **Introducción al phishing.** En: Jokobson, M.; Myers, S. **Phishing y contramedidas: entendiendo el creciendo problema del robo de identidad electrónico.** Pág. 3.

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 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, se puede encontrar ebay-login.com en lugar de eBay, y también es posible encontrar imitaciones más burdas tales como ebay.com.phishsite.com.

Por su puesto 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.

Se podría 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, se sitúa 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.

Los siguientes son tipos de *phishing* en función del destinatario:

- **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, se encuentra 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".[92] 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 paste es siquiera un cliente de un banco, sino los empleados de entidades que 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.

---

[92] Fernández Teruelo, J. G. **Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de red.** En: **Revista de derecho penal constitucional.** Pág. 217.

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. 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".[93] 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 se encuentran los *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 estas, los *bosts file*

[93] Emigh, A. **Robo de identidad online: tecnología de phishing, puntos de reloj y contramedidas.** Pág. 6.

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 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, 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 median, te 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 enlace que redirige al sujeto, aparentemente, a una página web de la entidad que en realidad no es tal v 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 solo 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. 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 objetivos 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, Real Player 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.

4.3.2. *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. 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".[94]

Aunque, como recuerdan los autores pioneros del estudio del *spoofing*, la suplantación de personalidades también se produce fuera del mundo virtual, 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 suplantar a la persona y actuar directamente haciéndose pasar por ella; 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, internet no solo es el medio a través del cual se puede realizar el *identity theft*, sino que es la razón del gran riesgo que conlleva el mismo en la actualidad, al haber aumentado significativamente en el ciberespacio la necesidad de utilizar los

---

[94] Chawki, M.; Abdel Whab, M. **Robo de identidad en el ciberespacio: problemas y soluciones.** En: **LE.** Pág. 23.

datos personales para realizar transacciones, operaciones o acciones, no siempre comerciales, por parte de los titulares de esa identidad.

Hay que tener en cuenta, por otro lado que, si bien el robo de identidad suele realizarse habitualmente 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 solo encierra un riesgo para el patrimonio de las personas, sino también para muchos otros bienes jurídicos como posteriormente se analizará en profundidad.

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 *bot* 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 re mite a la web falsa, y, por último, es el *mail spoofing*, "consistente en la suplantación de la dirección de correo electrónico de otras personas o entidades, utilizada generalmente para enviar spam o como comienzo de la dinámica de ataque del phishing".[95]

4.3.3. 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), ya sea de carácter empresarial para el descubrimiento de secretos comerciales, o 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.

---

[95] Isla Cortés, J. I. M. **Seguridad en redes informáticas.** Pág. 88.

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 este que después envía a otro sistema. Por medio del spyware se puede acceder a información personal o a secretos de empresa obtenidos en correos electrónicos y otro tipo de mensajes, pero generalmente este tipo de software lo que recaba es 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 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 in formación que no están destinadas a él. En realidad, lo que hacen los *packer 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, las denominadas cookies, "archivos que almacenan información del usuario en su propio sistema y que sirven para que los sitios web identifiquen al visitante".[96]

[96] Casanovas, P. **Internet y pluralismo jurídico: formas emergentes de regulación.** Pág. 104.

"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".[97]

De este modo, la conservación de esa información permite al remiten te, 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 Red".[98] 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.

4.3.4. 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. 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

---

[97] Poullet, Y. **Hacia nuevos principios de protección de datos en un nuevo entorno TIC.** En: **Revista de internet, derecho y política.** Pág. 136.

[98] Morón Lerma, E. **Derecho penal y nuevas tecnologías. Panorama actual y perspectivas futuras.** En: Casanovas, P. **Internet y pluralismo jurídico: formas emergentes de regulación.** Pág. 106.

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".[99]

En cuanto a las webs de juego online, estas 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. Se está haciendo referencia a la extorsión realizada por cibercriminales, generalmente por bandas organizadas, consistente en la solicitud de importantes cantidades económicas a cambio de cesar en la realización de algún tipo de ciberataque o incluso de empezar a ejecutarlo.

Al igual que en los casos de extorsión normal, el criminal aprovecha el hecho de que para la víctima puede resultar más sencillo, e incluso beneficioso, atender a la solicitud del criminal y no recibir el ataque que ser víctima de él y tratar de defender se posteriormente. En el caso de los comportamientos cibercriminales estas conductas

[99] Williams, P. **Crimen organizado y cibercrimen: sinergias, tendencias y respuestas.** Pág. 4.

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.

CONCLUSIÓN

El surgimiento de la dogmática de los ciberdelitos y de los tipos penales tan variados y contingentes, no es de estos últimos años. Es un problema universal que las sociedades están afrontando desde hace tiempo. Lo importante es que la tecnología avanza.

Los ciberdelincuentes buscan formas de vulnerar los sistemas informáticos y otros, para la comisión de los ciberdelitos. Por esa razón, la comunidad internacional ha tendido a realizar todo tipo de actividades y medidas tendentes a contrarrestar los efectos de estas conductas. Un precedente importante, es lo realizado por el Consejo de Europa, que ha logrado que los países miembros incluyan dentro de su respectiva legislación nacional, normas que les permitan hacer frente a los ciberdelitos.

También es importante precisar el aporte de la Organización de Cooperación y Desarrollo Económico -OCDE-, la cual ha realizado estudios para hacer frente a esta nueva forma de criminalidad, lo cual ha permitido identificar los delitos informáticos con la finalidad de enfrentarlos y proteger así los bienes jurídicos que afectan, como la intimidad, economía y propiedad intelectual.

Quienes operan en el sistema penal, no pueden permanecer al margen de las exigencias que imponen las características del Estado en que se desempeñan. Ello, obviamente incluye los desafíos sobre el desarrollo de la ciencia y las nuevas tecnologías. Por consiguiente, tampoco pueden mantenerse ajenos a las funciones que el derecho penal asume y que considerará en un momento histórico concreto y en un ordenamiento jurídico determinado.

En el ciberespacio se entrelaza la oportunidad encontrada por el ciberdelincuente, el contexto favorable creado por el ciberespacio y su accionar frecuente, buscando optimizar ese contexto favorable y sacar el mayor provecho posible.

El origen de la ciberdelincuencia se encuentra inexorablemente atado al fenómeno de la globalización, en la medida que con ella se ha maximizado el uso de redes de informática, sistemas y las TIC. El fenómeno informático es una realidad incuestionable y parece que también irreversible. Por lo tanto, el problema se traduce en buscar fórmulas efectivas de control, respecto a las cuales el derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismos sociales para el mantenimiento de un orden social.

BIBLIOGRAFÍA

AGUSTINA SANLLEHÍ, J. R. **La arquitectura digital de internet como factor criminógeno.** En: **IEJCS. Art. 4 Número 3**, 2009.

ALSHALAN, A. **Miedo al cibercrimen y victimización: análisis de una encuesta nacional**. España: Editorial Siglo XXI, 2006.

BAKER, W.; et. al. **Informe de investigaciones de incumplimiento de datos 2010. Un estudio realizado por el equipo de Verizon Risk en cooperación con los Servicios Secretos de los Estados Unidos.** Disponible en: https://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf

BOCIJ, P. **Víctimas del ciberstalking: un estudio exploratorio del acoso perpetrado a través de internet**. México: UNAM, 2003.

BOSSLER, A. M.; HOLT, T. J. **Actividades en línea, tutela e infección por malware**. En: **IJCC. Volumen 3. Número 1**, 2009.

BOSSLER, A. M.; HOLT, T. J. **El efecto del autocontrol sobre la victimización en el ciberespacio.** En: **Diario de investigación sobre crimen y delincuencia. Volumen 47. Número 3.** Maryland, Estados Unidos: 2010.

BOSSLER, A. M.; HOLT, T. J. **Examen de la aplicabilidad de la teoría de actividades rutinarias de estilo de vida para la victimización por delito cibernético.** España: Editorial Dykinson, 2009.

BOTTOMS, A. E.; WILES, P. **Criminología ambiental**. En: MAGUIRE, M.; GAN, R.; REINER, R. **Manual de criminología.** México: UNAM, 1999.

CASANOVAS, P. **Internet y pluralismo jurídico: formas emergentes de regulación.** Granada, España: Editorial Comares, 2003.

CHAWKI, M.; ABDEL WHAB, M. **Robo de identidad en el ciberespacio: problemas y soluciones**. En: **LE. Volumen 11, Número 1,** 2006.

CHOI, K. **Victimización por delitos informáticos y teoría integrada: una evaluación empírica.** En: **Revista latinoamericana de estudios de seguridad.** Ecuador: 2008.

CHUA, C. E. H.; WAREHAM, J. **Lucha contra el fraude de las subastas en internet. Una computación de evaluación y propuesta.** México: UNAM, 2004.

CLARKE, R. V. **Productos: comprender, anticipar y reducir la demanda de productos robados.** En: **Serie de investigación policial, publicaciones de investigación de la Oficina Central Británica.** Londres, Inglaterra: 1999.

CLOUCH, J. **Principio del cibercrimen.** España: Editorial Marcial Pons, 2005.

COHEN, L.; FELSON, M. **Cambio social y tendencias de la tasa de delincuencia: un enfoque de actividad rutinaria.** En: **Revista de derecho penal y criminología. Número 20.** Granada, España: 2018.

CORCOY BIDASOLO, M; JOSHI, U. **Delitos contra el patrimonio cometidos por medios informáticos. Revista RJC. No. 3.** Barcelona, España: 1998.

DE LA CUESTA ARZAMENDI, J. L. **Derecho penal informático.** España: 2010.

EMIGH, A. **Robo de identidad online: tecnología de phishing, puntos de reloj y contramedidas. Reporte sobre tecnología de robo de identidad online y contramedidas.** México: UNAM, 2005.

FARRELL, G.; PEASE, K. **Criminología y seguridad**. En: Grill, M. **Manual de seguridad**. México: UNAM, 2005.

FELSON, M. **Crimen, oportunidad y vida diaria**. Madrid, España: Editorial Dykinson, 2015.

FERNÁNDEZ TERUELO, J. G. **Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de red.** En: **Revista de derecho penal constitucional. Número 19**, 2007.

GARLAND, D. **La cultura del control. Crimen y orden social en la sociedad contemporánea.** Barcelona, España: Editorial Gedisa, 2005.

GARRIDO, V; STANGELAND, P.; REDONDO, S. **Principios de criminología.** Valencia, España: Editorial Tirant lo Blanch, 2006.

GORDON, S.; CHESS, D. M. **Donde hay humo hay espejos: la verad sobre los caballos trojanos en internet.** En: **Revista Electrónica de Derecho Penal y Criminología,** 1998.

GRABOSKY, P. **Criminalidad virtual: vino viejo en nuevas botellas.** En: **Revista de ciencia política. Vol. 27. Número 2.** Santiago, Chile: 2007.

GUTIÉRREZ FRANCÉS, M. L. **En torno a los fraudes informáticos en el derecho español.** En: **Revista AIA. Número 11.** España: 1994.

HOAR, S. B. **Tendencias en cibercrimen: el lado oscuro del internet.** En: **Justicia criminal. Volumen 20. Número 3.** 2005.

HUGHES, L. A.; DELONE, G. J. **Virus, gusanos y caballos troyanos: ¿crímenes graves, molestos o ambos?** En: **SSCR. Volumen 25. Número 1.** 2007.

HUTCHINGS, A.; HAYES, H. **Teoría de la actividad rutinaria y victimización por phishing: ¿quién es atrapado en la "red"?** México: UNAM, 2009.

ISLA CORTÉS, J. I. M. **Seguridad en redes informáticas.** México: UNAM, 2005.

JAISHANKAR, K. **Cibercriminología. Explorando los crímenes de internet y el comportamiento criminal.** España: Editorial Reus, 2011.

JAISHANKAR, K. **Crímenes relacionados con la identidad en el ciberespacio: examinando el phishing y su impacto.** En: **IJCC: volumen 2.** 2008.

JEWKES, Y. **Cibercrimen.** España: Editorial Bosch, 2006.

MACIÁ FERNÁNDEZ, G. **Ataques de denegación de servicio a baja tasa contra servidores.** España: Universidad de Granada, 2007.

MAÍLLO, A. **Introducción a la criminología.** Madrid, España: Editorial Dykinson, 2009.

MARCUM, C. D. **Teoría de la victimización de adolescentes online y construcciones de actividades de rutina.** Madrid, España: Editorial Dykinson, 2011.

MCQUADE, S. C. **Cibercrimen.** En: MAGUIRE, M.; GAN, R.; REINER, R. **Manual de criminología.** México: UNAM, 1999.

MEDINA ARIZA, J. J. **El control social del delito a través de la prevención situacional.** En: **Revista de Derecho Penal Constitucional. Número 2.** 1998.

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: **Revista electrónica de ciencia penal y criminología. Número 13-07.** España: 2011.

MORALES GARCÍA, O. **Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del consejo de europa sobre cyber-crime.** En: **CDJ. Número 9.** España: 2002.

MORÓN LERMA, E. **Derecho penal y nuevas tecnologías. Panorama actual y perspectivas futuras.** En: CASANOVAS, P. **Internet y pluralismo jurídico: formas emergentes de regulación.** Granada, España: Editorial Comares, 2003.

MYERS, S. **Introducción al phishing.** En: JOKOBSON, M.; MYERS, S. **Phishing y contramedidas: entendiendo el creciendo problema del robo de identidad electrónico.** México: Editorial Aranzadi, 2006.

NGO, F.; PATERNOSTER, R. **Victimización por delito cibernético: un examen de los factores de nivel individual y situacional.** En: **IJCC. Volumen 5. Número 1.** 2011.

OLLMAN, G. **La guía del phishing: entendiendo y previniendo los ataques de phishing. Informe técnico NGSS.** España: 2009.

ORTIZ DE URBINA GIMENO, I. **Memento práctico penal y económico de la empresa 2011-2012.** Madrid, España: Editorial Francis Lefebvre, 2011.

PINGUELO, F. M.; MULLER, B. W. **Crímenes virtuales, daños reales: un primer sobre los delitos cibernéticos en estados unidos y los esfuerzos para combatir los cibercriminales.** En: **VJLT. Volúmen 16. Número 1.** 2011.

PITTARO, M. L. **El acoso cibernético: un análisis sobre el acoso y la intimidación en línea. Revista de victimología.** Madrid, España: 2007.

POULLET, Y. **Hacia nuevos principios de protección de datos en un nuevo entorno tic.** En: **Revista de internet, derecho y política. Número 5.** España. 2007.

PRATT, T. C.; HOLTFRETER, K; REISIG, N. D. **Actividad rutinaria en línea y fraude en internet: extendiendo la generalidad de la teoría de la actividad rutinaria.** En: **Diario de Investigación sobre Crimen y Delincuencia. Volumen 47. Número 3.** Maryland, Estados Unidos: 2010.

QUINTERO OLIVARES, G. **Internet y derecho penal. Imputación de los delitos y determinación de la competencia.** En: **La ley penal: revista de derecho penal. Número 37. Año IV.** España: 2007.

RATCHFORD, B. T.; TALUKADAR, D.; LEE, M. **Un modelo de elección del consumidor de internet como fuente de información.** España: Editorial Bosch, 2001.

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. Número 6.** España: 2008.

REYNS, B. **Ser perseguido en línea alcance y naturaleza de la victimización del ciberstalking de un estilo de vida.** Barcelona, España: Editorial Ariel, 2010.

ROMEO CASABONA, C. M. **El cibercrimen: nuevos retos jurídicos-penales, nuevas respuestas político-criminales.** Granada, España: Editorial Comares, 2006

ROMEO CASABONA, C. M. **Los delitos de daños en el ámbito informático**. En: **CPC. Número 43.** España: 1991.

ROSENZWEIG, R. **Magos, burócratas, guerreros y hackers: escribiendo la historia de internet.** En: **AHR. Volumen 103. Número 5.** 1998.

SERRANO MAÍLLO, A. **Oportunidad y delito.** Madrid, España: Editorial Dykinson, 2009.

SIEBER, U. **Tecnología de la información y reforma de la ley penal.** México: UNAM, 1985.

SINROD, E. J.; REILLY, W. P. **Los delitos cibernéticos: un enfoque práctico para la aplicación de las leyes federales sobre delitos informáticos.** España: Editorial Dykinson, 2000.

STADLER, W. A. **Fraude en internet.** En: FISHER, B. S.; LAB, S. P. **Enciclopedia de victimología y prevención del crimen.** California, Estados Unidos: Publicaciones Sage, 2010.

STAJANO, F.; WILSON, P. **Comprendiendo a las víctimas de fraude: siete principios para la seguridad de sistemas.** España: Editorial Dykinson, 2011.

WALL, D. CIBERCRIMEN: **la transformación del crimen en la era de la información.** Madrid, España: Alianza Editorial, 2007.

WALL, D. S. **¿Qué son los cibercrímenes?** México: UNAM, 2005.

WILLIAMS, P. **Crimen organizado y cibercrimen: sinergias, tendencias y respuestas.** España: Editorial Académica Española, 2001.

YAR, M. **Cibercrimen y sociedad.** España: Editorial Reus, 2006.

YAR, M. **La novedad del ciberdelito: una evaluación a la luz de la teoría de la actividad rutinaria.** En: **Revista Electrónica de Derecho Penal y Criminología.** España: 2005.

YBARRA, M. L.; MITCHELL, K. **Exposición a la pornografía de internet en niños y adolescentes: una encuesta nacional.** En: **CpB. Volumen 8. Número 5.** 2005.

YEARGAIN, J. W.; SETTOON, R. P.; MCKAY, S. E. **Acto de spam 2003: como spamear legalmente.** En: **JSeC. Volumen 2. Número 1.** 2004.

YUCEDAL, B. **Victimización en el ciberespacio: una aplicación de las teorías de exposición a la actividad rutinaria y al estilo de vida.** En: **Revista Electrónica de Ciencia Penal y Criminología.** España: 2010.