

Cibercrimen

Guía para entender y
combatir el delito digital



Miguel Ángel Águila Sánchez



Ra-Ma®

edü
Ediciones de la U

Cibercrimen

Guía para entender y combatir
el delito digital

Miguel Ángel Águila Sánchez



Ra-Ma[®]

edü[®]

Conocimiento a su alcance

Águila Sánchez, Miguel Ángel

Cibercrimen. Guía para entender y combatir el delito digital / Miguel Ángel Águila Sánchez --. Bogotá: Ediciones de la U, 2026

290 p. ; 24 cm

ISBN 978-958-792-982-9 e-ISBN 978-628-7912-34-2 ePUB 978-958-792-983-6

1. Informática 2. Delito informáticos 3. Cibercrimen I. Tít.

621.39 ed. Thema URH

Edición original publicada por © Editorial Ra-ma (España)

Edición autorizada a Ediciones de la U para Colombia

Área: Informática

Primera edición: Bogotá, Colombia, marzo de 2026

ISBN 978-958-792-982-9

© Miguel Ángel Águila Sánchez

© Ra-ma Editorial

Calle Jarama, 3-A (Polígono Industrial Igarsa) 28860 Paracuellos de Jarama

www.ra-ma.es y www.ra-ma.com / E-mail: editorial@ra-ma.com

Madrid, España

© Ediciones de la U - Carrera 27 #27-43 - Tel. (+57) 601 6455049

www.edicionesdelau.com - E-mail: editor@edicionesdelau.com

Bogotá, Colombia

Ediciones de la U es una empresa editorial que, con una visión moderna y estratégica de las tecnologías, desarrolla, promueve, distribuye y comercializa contenidos, herramientas de formación, libros técnicos y profesionales, e-books, e-learning o aprendizaje en línea, realizados por autores con amplia experiencia en las diferentes áreas profesionales e investigativas, para brindar a nuestros usuarios soluciones útiles y prácticas que contribuyan al dominio de sus campos de trabajo y a su mejor desempeño en un mundo global, cambiante y cada vez más competitivo.

Coordinación editorial: Daniela Parra G.

Carátula: Ediciones de la U

Impresión: DGP Editores SAS

Calle 63 #70D-34, Pbx (+57) 601 7217756

Impreso y hecho en Colombia

Printed and made in Colombia

No está permitida la reproducción total o parcial de este libro, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro y otros medios, sin el permiso previo y por escrito de los titulares del Copyright.

A mi familia.

ÍNDICE

ACERCA DEL AUTOR	11
PRÓLOGO	13
INTRODUCCIÓN	16
CAPÍTULO 1. CIBERDELINCUENCIA.....	19
1.1 ¿QUÉ ES LA?.....	20
1.2 LA CONSTANTE EVOLUCIÓN DE LA CIBERDELINCUENCIA.....	21
1.3 CARACTERÍSTICAS DE LA CIBERDELINCUENCIA	26
1.4 PERFIL DEL CIBERDELINCUENTE. EL DELINCUENTE INFORMÁTICO.....	29
1.5 TIPOS DE CIBERATAQUES	39
1.6 PREVENCIÓN CONTRA LOS CIBERATAQUES.....	43
1.7 CASOS IMPORTANTES DE CIBERATAQUES	46
1.8 EVOLUCIÓN DE LOS CIBERDELITOS.....	48
1.9 CIBERDELINCUENTE Y CIBERVÍCTIMA.....	50
1.10 LA PRUEBA PERICIAL EN LOS CIBERDELITOS.....	52
1.11 ESTRATEGIA MUNDIAL CONTRA LA CIBERDELINCUENCIA.....	55
CAPÍTULO 2. CIBERCRIMINALIDAD	58
2.1 CIBERCRIMEN Y CIBERCRIMINALIDAD	59
2.2 DIFERENCIA ENTRE “DELITO INFORMÁTICO” Y “DELITO CIBERNÉTICO”	59
2.3 TIPOS DE CIBERCRIMEN.....	62

2.3.1	La cibercriminalidad económica	62
2.3.2	La cibercriminalidad social	63
2.3.3	La cibercriminalidad política.....	65
2.4	LA AMENAZA DEL CIBERCRIMEN EN LA SOCIEDAD: MEDIDAS PREVENTIVAS.....	71
2.5	LA INVESTIGACIÓN Y PERSECUCIÓN DE LA CIBERCRIMINALIDAD ..	75
2.6	LA IDENTIFICACIÓN Y LA PROBLEMÁTICA PROBATORIA.....	84
2.7	CIBERCRIMINALIDAD EN LAS PRÓXIMAS DÉCADAS.....	87
CAPÍTULO 3. DELITOS INFORMÁTICOS.....		93
3.1	DEFINICIÓN DE DELITOS INFORMÁTICOS.....	93
3.2	LA INFORMÁTICA COMO MEDIO DEL DELITO.....	96
3.3	DELITO INFORMÁTICO: DELINCUENCIA INFORMÁTICA, CRIMINALIDAD INFORMÁTICA, CIBERDELINCUENCIA, CIBERCRIMEN	98
3.4	SUJETOS DE LOS DELITOS INFORMÁTICOS	100
3.5	BIENES JURÍDICOS PROTEGIDOS EN EL DELITO INFORMÁTICO	101
3.6	NUEVAS TECNOLOGÍAS PARA NUEVOS CONCEPTOS DELICTIVOS: CIBERESPACIO, CIBERDELINCUENCIA, CIBERCRIMEN.....	103
3.7	TIPOS DE DELITOS INFORMÁTICOS	106
3.8	DELITO DE ESTAFA O FRAUDE INFORMÁTICO	107
3.8.1	Fraudes cometidos mediante la manipulación de computadoras	107
3.8.2	Falsificaciones informáticas	108
3.9	FRAUDES FINANCIEROS Y ECONÓMICOS.....	108
3.9.1	Fraudes con tarjetas.....	110
3.9.2	Ofertas de trabajo falsas	113
3.9.3	Robo, usurpación o suplantación de identidad.....	114
3.10	SABOTAJE INFORMÁTICO	114
3.11	DELITOS SEXUALES	117
3.12	DELITOS CONTRA LA INTEGRIDAD SEXUAL	121
3.12.1	Prostitución infantil	122
3.12.2	Pornografía infantil	123
3.12.3	Pedofilia.....	126
3.12.4	Grooming	128
3.13	DELITOS DE ACOSO ESCOLAR Y LABORAL.....	130
3.13.1	El acoso escolar o bullying.....	130
3.13.2	El acoso laboral o mobbing.....	132
3.14	ROOTKIT (LA AMENAZA INVISIBLE)	133
CAPÍTULO 4. CIBERDELINCUENCIA ORGANIZADA O SAQUEO INFORMÁTICO.....		134
4.1	EL CIBERESPACIO COMO CAMPO DELICTIVO	135
4.2	CIBERCRIMEN	137
4.2.1	Ingresos económicos de forma fraudulenta.....	139

4.2.2	Fraude en comercio electrónico	139
4.2.3	El carding	140
4.2.4	Ventas en portales de anuncios clasificados	142
4.2.5	Crime as a service	143
4.2.6	La infraestructura de mulas	144
4.2.7	Los timos en la Red	144
4.2.8	La piratería informática	145
4.2.9	Blanqueo de capitales	150
4.2.10	Causas y consecuencias del blanqueo de capitales	153
4.2.11	Técnicas de blanqueo de capitales	156
4.2.12	Mecanismos de detección del blanqueo de capitales	160
4.3	CIBERTERRORISMO	160
4.3.1	Comunicación y propaganda	162
4.3.2	Financiación de los grupos terroristas	169
4.3.3	La captación de los seguidores o súbditos	169
4.3.4	Adoctrinamiento	170
4.3.5	El uso de Internet y su radicalización en la Red	171
4.4	CIBERGUERRA	172
4.4.1	¿Qué es ciberguerra?	173
4.4.2	El sistema informático en la ciberguerra actual	174
4.4.3	Ciberespacio: territorio sin fronteras	175
4.4.4	El conflicto Israel-Hamas	177
4.4.5	El conflicto Rusia-Ucrania	179
CAPÍTULO 5. HACKERS.....		182
5.1	LA APARICIÓN DEL HACKER, JÁQUER O JACKER	183
5.2	LAS HERRAMIENTAS DEL HACKER	184
5.3	LA ENSEÑANZA HACKER	187
5.4	¿QUIENES SON LOS CRACKERS?	192
5.5	LA OCULTACIÓN DE MENSAJES: LA CRIPTOGRAFÍA	194
5.6	EL SOFTWARE LIBRE	197
5.7	CIBERSOCIEDAD Y CIBERGRUPOS DE HACKERS	198
5.8	ORIGEN Y PRECEDENTES DE LOS HACKERS	200
5.9	LA CIBERSOCIEDAD ACTUAL Y DE FUTURO	202
5.10	CRÓNICAS DE HACKERS Y CRACKERS	202
5.10.1	El caso del Phreaker ciego	203
5.10.2	El robo del banco	203
5.11	LA SEGURIDAD EN INTERNET Y LA AMENAZA DE LOS VIRUS INFORMÁTICOS	204
5.12	LAS AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS Y DE LOS DATOS	209
5.13	LA IMPORTANCIA DE UNA DEFENSA CIBERNÉTICA PROACTIVA CONTRA LOS CIBERATAQUES	214
5.13.1	Ataques contra la integridad	214
5.13.2	Ataques contra la disponibilidad	214

5.13.3 Ataques contra la privacidad	215
5.14 SEGURIDAD EN SISTEMAS.....	215
5.15 SEGURIDAD EN REDES	216
5.16 SEGURIDAD EN APLICACIONES WEB Y WEBSERVERS	219
CAPÍTULO 6. REDES SOCIALES.....	223
6.1 ATRAPADOS EN LA TELA DE ARAÑA.....	223
6.2 LA TECNOCRACIA O EL MUNDO DE LA INCOMUNICACIÓN TRADICIONAL	225
6.3 EL FENÓMENO DE LAS REDES SOCIALES EN LA SOCIEDAD	226
6.4 LOS PERFILES DE LOS ADOLESCENTES EN LAS REDES SOCIALES..	229
6.5 EL COMPONENTE RELACIONAL, DE ENTRETENIMIENTO Y DE OCIO DE LAS REDES SOCIALES	232
6.6 EL RIESGO DEL USO ABUSIVO DE LAS REDES SOCIALES	234
6.7 LAS REDES SOCIALES COMO MEDIO DE DIFUSIÓN	237
6.8 EL USO DE LAS REDES SOCIALES: PRIVACIDAD Y SEGURIDAD	241
6.9 TENDENCIAS EN LAS REDES SOCIALES.....	244
6.9.1 Mayor personalización y algoritmos inteligentes.....	245
6.9.2 Inteligencia Artificial (IA) y chatbots.....	246
6.9.3 Realidad Virtual (RV) y redes sociales inmersivas	247
6.9.4 Mayor enfoque en la autenticidad y la transparencia.....	247
6.9.5 Contenido generado por los usuarios	247
6.9.6 Redes sociales de nicho.....	247
6.10 EL AUQUE DE LA UTILIZACIÓN Y EXPANSIÓN DEL TIKTOK.....	248
6.11 LAS REDES SOCIALES EN LA ACTUALIDAD Y SU IMPACTO SOCIOCULTURAL: BENEFICIOS Y PERJUICIOS DEL USO DE LAS REDES SOCIALES.....	249
6.12 REDES SOCIALES Y PERSPECTIVAS DE FUTURO.....	250
CAPÍTULO 7. LEGISLACIÓN	251
7.1 EL CODIGO PENAL ESPAÑOL Y LA CIBERDELINCUENCIA.....	252
7.2 DELITOS RECOGIDOS Y TIPIFICADOS EN EL CÓDIGO PENAL ESPAÑOL.....	253
7.2.1 Delitos relacionados con el contenido.....	253
7.2.2 Descubrimiento y revelación de secretos	254
7.2.3 Estafa informática	255
7.2.4 De las defraudaciones de fluido eléctrico y análogas.....	256
7.2.5 Daños informáticos	256
7.2.6 De los delitos relativos a la propiedad intelectual.....	256
7.3 LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA.....	257
GLOSARIO.....	263
BIBLIOGRAFÍA.....	271



ACERCA DEL AUTOR

Miguel Ángel Águila Sánchez

Doctor en Análisis y Prevención del Terrorismo y Licenciado en Ciencias del Trabajo por la Universidad Rey Juan Carlos (Madrid). Ha sido Profesor Adjunto Doctor en la Facultad de Criminología, Grado de Criminología y en el Grado de Psicología en la Universidad Internacional Isabel I de Castilla (Burgos). Asimismo, Profesor Doctor del Departamento de Derecho Público I y Ciencia Política, Grado de Criminología y Doble Grado de Criminología y Derecho, en la Universidad Rey Juan Carlos, Campus de Vicálvaro y Alcorcón (Madrid). Y profesor en la Academia del Cuerpo Nacional de Policía (Madrid) en el Seminario “Policía de Barrio”.

Ha pertenecido al Ministerio del Interior desempeñando el cargo de Subinspector como: Jefe de Sección, Nivel 22, Dirección General de la Policía, División Económica y Técnica, Área de Gestión Financiera y Presupuestaria, Sección de Contabilidad Presupuestaria (Madrid). Jefe de Turno en la Inspección de Guardia en la Comisaría de Policía Nacional de Buenavista (Madrid). **Jefe de Sección de Estudios en la Academia Especial de Policía Nacional.**

Es autor de diversas publicaciones: “Crónicas, relatos e historias de la Mafia y sus capos”, Editorial Punto Rojo, Sevilla.

- Coautor de “En torno al 23-F”, editado por La Albolafia, Revista de Humanidades y Cultura, Revista científica de periodicidad cuatrimestral, número 19, Madrid.
- Autor de “Criminalística e investigación”, Facultad de Criminología, Grado de Criminología, Cursos 2016-2018, Universidad Internacional Isabel I de Castilla (Burgos).
- Autor de “Psicología del terrorismo”, Facultad de Ciencias de la Salud, Grado de Psicología, Cursos 2016-2018, Universidad Internacional Isabel I de Castilla (Burgos).
- Autor de “Diáspora islamista –origen, causas y consecuencias–”, Editorial Círculo Rojo, Almería.
- Autor de “Retrato de un hombre gris”, Editorial Círculo Rojo, Almería.
- Autor de “Tipos y Formas de Delincuencia”, Editorial Universitas, Madrid.
- Coautor de “La incorporación de la mujer a las Fuerzas Armadas -Historia, Testimonios y Fuentes de información-”, editado por la Universidad Rey Juan Carlos, Estudios Estratégicos del Ministerio de Defensa y el Instituto de la Mujer del Ministerio de Sanidad, Política Social e Igualdad, Madrid.
- Autor de “Las treguas de ETA desde una perspectiva comparada”, Editorial Visión Libros, Madrid.

Y, participado en diversas ponencias: “La vulnerabilidad energética como riesgo para la seguridad”, Universidad Rey Juan Carlos, Facultad de Ciencias de la Comunicación, Campus de Fuenlabrada (Madrid). Ponencia “Terrorismo y Seguridad Energética”.

“La comunicación de la defensa y los conflictos armados”, Universidad Rey Juan Carlos, Facultad de Ciencias de la Comunicación, Campus de Fuenlabrada (Madrid). Ponencia “Los Comunicados de la Policía y los Medios de Comunicación”.



PRÓLOGO

La tecnología, en esencia, constituye un conjunto de herramientas y conocimientos que el ser humano ha ido incorporando a su actividad diaria para resolver problemas y satisfacer las necesidades que le iban surgiendo adaptando sus recursos para un mayor bienestar.

La tecnología a lo largo de la historia ha ido transformando la sociedad, mejorando la productividad y eficiencia en el desarrollo de los problemas planteados, y surgiendo nuevos cambios en la interacción social de las personas. Su uso representa una mejora de la calidad de vida, facilitando múltiples tareas en todos los ámbitos de la vida social, laboral, cultural, científica, deportiva, etc.

La relación entre el ser humano y la tecnología es intrínseca y evolutiva, al utilizar las herramientas para adaptar y transformar su entorno. Es fundamental que su utilización sirva para avanzar y facilitar las condiciones del ser humano y un mayor bienestar social, por lo que resulta imprescindible que su uso sea para el desarrollo integral de las personas, pero no para su aislamiento del resto de la sociedad.

Atrás quedan en el pasado innovaciones técnicas que han supuesto un gran desarrollo para la humanidad como la aparición de la imprenta (1440), el teléfono (1876), la bombilla incandescente (1879), la radio (1897), o la televisión (1927), son fechas aproximadas, que se presumen como las iniciadoras de su aparición y desarrollo, aunque pueden existir diversas interpretaciones al respecto.

Entre los avances tecnológicos más significativos y cercanos a la actualidad, podemos referenciar los siguientes:

- **Sistemas Operativos.** Consiste en un *software* fundamental que actúa como intermediario entre el *hardware* de un dispositivo y las aplicaciones que se ejecutan en él. Cuando se enciende el ordenador, el sistema operativo se encarga de ver las ventanas, gestionar tus archivos, instalar software, etc. Algunos son Mac OS de Apple, Windows de Microsoft y Android para Smartphone.
- **Microprocesador.** Conocido como CPU, es el circuito integrado central de un sistema informático, que ejecuta las instrucciones de los programas y realizar cálculos. Puede afirmarse que es el cerebro de la computadora.
- **Computadora personal.** A partir de esta fecha comienza su comercialización aunque su revolución comienza en 1975, que aunque no poseían teclado ni pantalla, sí marcó un hito en la popularización del uso de los microprocesadores y lenguajes de programación como BASIC para uso personal.
- **Correo electrónico.** Es un sistema que permite enviar mensajes entre diferentes computadoras a la red, introduciendo el uso del símbolo @ para identificar la dirección del destinatario.
- **Internet.** En este año se presentó ARPANET demostrando que el sistema era operativo creando una red de 40 puntos conectados en diferentes localizaciones.
- **Computadora portátil.** Supondrá una innovación y un gran beneficio para el trabajo de científicos, militares, empresarios y otras profesiones, al poder contar con la información que contenían pudiendo trasladarla de un sitio a otro.
- **Navegadores de Internet.** El primer navegador que se difundió por la red fue el *Mosaic*, después se transformaría en el *Netscape*, que dominaría el mercado hasta la llegada de Microsoft con la aparición de Internet Explorer en 1996.
- **Bluetooth.** Fue desarrollada por la empresa sueca Ericsson como alternativa inalámbrica a los cables para conectar dispositivos electrónicos, permitiendo la comunicación entre dispositivos fijos y móviles a corta distancia a través de una frecuencia de radio de onda corta.
- **Memoria USB.** Se creó en 1996, pero no disfrutaría de una amplia aceptación por sus limitaciones de corriente. Tendrá su aparición en el mercado con el lanzamiento USB 1.1 en 1998.

- **Big Data.** Se refiere a la capacidad de almacenamiento y procesamiento de grandes volúmenes de datos, a menudo en tiempo real, superando las capacidades de los sistemas tradicionales.
- **Wi-Fi.** Permite la conexión de dispositivos, intercambiando información entre sí. Creando una red. La conexión se realiza a Internet a través de un *router* inalámbrico. Al acceder al Wi Fi, se conecta a un router inalámbrico permitiendo a sus dispositivos compatibles con Wi-Fi que se conecten a Internet.
- **Redes sociales.** Son las plataformas digitales que facilitan la conexión, comunicación e intercambio de contenido entre los usuarios.
- **YouTube.** Otra plataforma *online* donde los usuarios pueden subir, ver, compartir o comentar vídeos. Es una red social de vídeos donde se pueden encontrar todo tipo de contenido.

Esta relación, obviamente no es completa, representa una mínima parte de los avances tecnológicos y los constantes desarrollos informáticos que se suceden de forma simultánea y con una rapidez difícil de sincronizar. El mundo tecnológico y, en consecuencia, el espacio virtual, está comenzando un camino con perspectivas infinitas donde no se vislumbra sus límites, ni las consecuencias que puedan reportar dichas innovaciones en el devenir de los casos.

El ser humano debe ser consciente de que la tecnología y sus avances deben estar al servicio de la humanidad y no caer en la tentación o en el error de que sea el hombre quien dependa de la tecnología.

Toda innovación tecnológica representa un gran avance, siempre y cuando, esté bajo el dominio y el control del ser humano.

INTRODUCCIÓN

Con la aparición de Internet en 1969, estableciéndose la primera de conexión de computadoras, va a experimentar un crecimiento exponencial en la década de 1990 en el hemisferio occidental y un mayor crecimiento a nivel mundial en la primera década del siglo XXI alcanzando a la tercera parte de la población mundial. Esa primera conexión tiene lugar entre las universidades de UCLA y Stanford, a través de una línea telefónica conmutada. Con la primera conexión se construyó el mito de que se había realizado con el fin de evitar posibles ataques nucleares, extremo este que continúa en la clase popular, aunque también su finalidad era evitar los continuos fallos que se producían en la red.

Internet sirve como enlace de redes pequeñas dándolas una mayor cobertura al incluirlas en una red global, lo que facilita utilizar un lenguaje común o protocolo conocido como TCP/IP (*Transmission Control Protocol/Internet Protocol*, Protocolo de control de transmisión/Protocolo de Internet), constituyendo y dando lugar a Internet como la “Red de redes”.

Consecuencia de ello la sociedad humana va a experimentar una transformación con la implantación de las tecnologías digitales que supondrán un cambio total en todos sus aspectos. Este cambio afectará de forma directa a comportamientos que se han ido sucediendo a lo largo de la historia y que de alguna forma eran considerados como métodos de trabajo incuestionables e irremplazables. El mundo del papel como método primario como transmisión de órdenes, emplazamientos, conocimiento de actuaciones o simplemente como medio de comunicación, quedará obsoleto y ambiguo fuera de todo contexto de relación tanto en el ámbito laboral, académico, social y de cualquier estamento de relación entre las personas. La aparición de nuevos métodos tecnológicos hará que poco a poco esos anteriores recursos vayan siendo arrinconados en el olvido y que su desaparición sea cuestión de tiempo.

La era digital ha llegado para quedarse y su aparición implica un mayor conocimiento constante de los avances que se suceden con una velocidad inusitada. Esta constante innovación no solo responde a las necesidades que se siguen produciendo sino que la digitalización implica de un esfuerzo de seguimiento que, en gran parte de ese avance hace que su progresiva actualización vaya por delante de lo que el ser humano, en su concepto general, pueda absorber y asimilar tal cantidad de información.

El uso de Internet ha experimentado un gran crecimiento. A principios del siglo XXI el número de usuarios pasó a tener cerca de 2.000 millones y una cuarta parte de la población mundial tenía conexión a computadoras. Su uso se encuentra extendido en todos los ámbitos de la sociedad. En el mundo laboral a través del *Teletrabajo* va a suponer una mayor colaboración y rapidez en sus tareas, además de representar un menor coste y mayor agilización en su intercambio de ideas y de información que dan como resultado un mayor beneficio. A nivel *académico*, su información resulta infinita ya que ofrece un espectro de divulgación de información que en tiempos pasados era inimaginable poder abarcar en un estado físico para poder ser consultado y almacenado. Atrás quedan las enciclopedias y las bibliotecas tradicionales donde el mundo del papel abarcaba grandes espacios donde dormían los volúmenes en espera de ser capturados por cualquier lector ávido de información y cultura. Como medio *social* de comunicación entre personas hace que la presencia social, en la relación, no sea imprescindible para poder mantener una conversación en directo, tanto física como temporal, redundando en una mayor celeridad en la comunicación e intercambio de ideas o pareceres, lo que refleja que la evolución del individuo no va a necesitar de la presencia de un congénere de forma presencial sino que se podrá efectuar de manera virtual. Así como los logros de la digitalización han traído nuevos desafíos y avances que han facilitado mejoras en la sociedad, no solo a nivel individual sino globalmente, también es necesario resaltar que lo mismo que ocurre con el campo de la criminalidad, este avance ha supuesto un retroceso en la armonización de las relaciones interpersonales, haciendo del individuo un ser cada vez más aislado y separado de la colectividad encerrado en un mundo virtual que, en ocasiones, le aleja de la realidad social.

La libertad encubierta que posee el delincuente cibernético hace que este explore multitud de campos que la red le proporciona buscando nuevos retos para sus inclinaciones delictivas, amparadas en el anonimato y que le dan inmediatez a todos sus deseos criminológicos, como ciberterrorismo, ciberamenazas, ciberacoso, sexting, etc., ya que el abanico resulta infinito a la vez que se compone de un gran entramado para su persecución y localización, y su posterior, detención.

La expansión y crecimiento de Internet como medio de comunicación ha supuesto un intercambio masivo de información masiva que adquiere una

trascendencia social que tiene lugar en tiempo real y que va a abarcar a todo tipo de actividades de todo tipo, desde el acto lúdico, como los de carácter político, económico, cultural, social, etc., y por supuesto, tendrá un espacio reservado y de gran proyección para el ámbito delictivo o criminal.¹

La aparición tecnológica hace que el contexto de la criminalidad no tenga por qué coincidir el hecho delictivo con la presencia física del delincuente y su víctima, al igual que ocurre con el tiempo para su realización. La figura del individuo que ejecuta el acto criminal sigue presente en la casuística del delito como factor fundamental para la realización del hecho punible pero no así para su entorno espacio-temporal, donde el espacio puede tener su configuración sin presencia física de la víctima, y donde el espacio temporal, no necesariamente es en el momento en que el autor lleva a cabo el mismo, por lo que el espacio geográfico resulta intrascendente al mismo que resulta intemporal.²

Todo avance de la ciencia implica un mayor desarrollo de todos los ámbitos en la sociedad. El ser humano a través de la historia ha ido progresando en conocimiento ampliando su campo intelectual que con el transcurso del tiempo se ha ido adaptando a las necesidades que su entorno le iba exigiendo. El mundo laboral, académico, sanidad, social, armamentístico, climatológico, comunicativo, y de otras órdenes interrelacionados, han aprovechado los avances que la tecnología les ha ido aportando a sus metodologías facilitando sus doctrinas y sus métodos de aplicación redundando en un mayor beneficio y simplificación de sus tareas repercutiendo en beneficio de la sociedad. Pero como todo avance también aparecen sus inconvenientes, el mundo de la criminalidad aprovechara estos recursos para adentrarse en el mundo tecnológico, el cual, además de facilitarle sus múltiples campos delincuenciales, le va a aportar una mayor rapidez en sus acciones delictivas dotándolas de una invisibilidad que la proporciona el anonimato en las múltiples facetas que abarca su conducta criminal.

Aquí comienza una nueva escala del crimen organizado donde sus acciones delictivas se van a ver multiplicadas exponencialmente y, donde sus autores, van a poseer de un tiempo necesario para que muchos de sus delitos tarden en aparecer para su persecución e incluso muchos de ellos quedar en el anonimato de las redes sociales, dando lugar a lo que comienza a extenderse, y entenderse, como ciberdelincuencia.

1 Cfr., ÁGUILA SÁNCHEZ, Miguel Ángel, Tipos y Formas de delincuencia, Editorial Universitas, Madrid, 2013, p. 263.

2 Ibídem., p. 264.

CIBERDELINCUENCIA

La sociedad al igual que ocurre con el mundo laboral está en constante transformación añadiendo cada vez más una compleja radiografía social difícil de delimitar en su configuración. Los intentos por clasificar y controlar el amplio espectro delictivo que se viene sucediendo con el paso del tiempo hacen que la delincuencia, pueda transgredir e ir por delante de la normativa jurídica, al sobrepasar a esta con delitos que surgen con modalidades que eran inimaginables en tiempos recientes.

El cambio en el concepto laboral que se viene produciendo y normalizando, en la actualidad, hacia el denominado teletrabajo hace que los modelos desarrollados a lo largo de la historia se vean superados por su rápido avance y no puedan garantizar una seguridad a sus partidarios.

La ciberdelincuencia al igual que ocurre con el mundo digital y el uso de Internet han ido evolucionando y surgiendo nuevos avances tecnológicos, los delincuentes han adaptado su metodología asediando de TIC (Tecnologías de Información y Comunicación) a los equipos de seguridad a poder introducirse en las organizaciones encontrando las debilidades que encuentran en sus sistemas.

El delito en sentido genérico es inherente con el ser humano. Desde los tiempos más remotos de la humanidad el hombre ha establecido una serie de conductas y normas que reglamentaban el comportamiento del individuo con el resto de la sociedad. Estas normas o preceptos, o si se prefiere de bandos, llevaban a la sociedad a mantenerse dentro de unos límites de convivencia que permitían el normal desarrollo de la vida en comunidad. Pero dentro de esa unión siempre han existido individuos que han transgredido esas cláusulas de convivencia y han adoptado una conducta antisocial desobedeciendo el ordenamiento establecido por esa sociedad, donde el sujeto lejos de seguir con los principios básicos de sus ciudadanos establecidos en un orden social, causan un perjuicio al resto de la ciudadanía enfrentándose a su estructura social.

1.1 ¿QUÉ ES LA?

El término “ciberdelincuencia” tiene múltiples acepciones según los contextos en los que aparece. No obstante, la palabra “ciberdelincuencia” tiene múltiples interpretaciones que han sido recogidas por numerosos tratadistas, si bien, no hay una definición concisa. Una de estas definiciones se encuentra recogida en el Diccionario de la Real Academia Española (RAE) donde se cita que “ciberdelincuencia” es toda: “Actividad delictiva que se lleva a cabo a través de Internet”.³

La “ciberdelincuencia” podría ser entendida como cualquier forma de criminalidad que tiene lugar en el ámbito de interacción social determinada por el uso de las Tecnologías de la Información y la Comunicación (TIC). La sociedad ha sufrido una gran transformación al pasar de una etapa industrial a otra postindustrial, que han ejercido una influencia en todos los ámbitos de la estructura social. El desarrollo de las tecnologías va a suscitar un cambio cualitativo en el concepto de riqueza, no solo a nivel individual sino que será transnacional, donde las naciones con grandes inversiones en tecnología alcanzarán grandes cotas de riqueza económica, a la vez que van a experimentar un progreso exponencial en su desarrollo, no solo económico, sino en lo social. El cambio va a suponer un nuevo concepto de sociedad donde los valores instaurados van a relegar a un segundo plano todo lo que en la etapa industrial supuso un gran hito revolucionario quedara desbancado por una vertiginosa carrera industrial por organizaciones dedicadas el sector tecnológico donde las últimas novedades tienen un tiempo limitado.

Esta vertiginosa transformación de la sociedad que denominaríamos industrial va a sufrir un cambio exponencial donde su sociedad se va a ver inmersa en todos los aspectos de su día a día, tanto en el ámbito doméstico como en el laboral, abarcando a todos los estamentos de la sociedad y, en consecuencia, de las naciones. Es aquí donde hace acto de presencia lo que venimos denominando “ciberdelincuencia”, al estar interconectados todos los estamentos de la sociedad, desde el ámbito familiar, educativo, empresarial o el propio Estado, haciendo acto de presencia el ciberdelincuente.

La transformación analógica-digital da lugar a mayores oportunidades y cambios en las estructuras socioeconómicas, empresariales, organizaciones nacionales e internacionales, y en todos los ámbitos culturales, sociales, políticos y de relación del individuo. La nueva tecnología va a facilitar el acercamiento y el crecimiento de todos los sectores, desde un prisma personal hasta el colectivo, pasando y estableciéndose en todos los estamentos, tanto privados como públicos.

3 Diccionario de la Real Academia Española (RAE), 23ª edición, de octubre de 2014. Disponible en <https://www.rae.es/obras-academicas/diccionarios/diccionario-de-la-lengua-espanola>.

El ciberdelincuente al igual que sucede con la criminalidad genérica, puede realizar los ciberdelitos, tanto de forma individual, grupal o como grupos organizados. Una característica de la ciberdelincuencia, que la diferencia de cualquier otra actividad delictiva, radica en el anonimato y la dificultad que supone el rastreo de estos ciberdelinquentes debido en gran parte a la globalización digital que ha tenido lugar en las últimas décadas, constituyendo una red de conexiones de dimensiones infinitas lo que procura un difícil seguimiento para la localización del autor del hecho delictivo dotándole de un anonimato que le permite actuar con gran rapidez y desaparecer de un primer plano.

Dentro de los objetivos de los ciberdelinquentes consisten en dañar los sistemas informáticos de personas o de entidades privadas o públicas, para poder acceder a sus sistemas informáticos y hacer un uso fraudulento de sus datos personales con la finalidad de obtener un beneficio que puede abarcar desde una suplantación de la personalidad, ciberamenazas, extorsiones, económico, etc.

La globalización ha traído un constante intercambio de información que se recoge en las redes y que gran parte de esa información queda de forma permanente en el espacio digital, lo que permite a los ciberdelinquentes un constante rastreo del campo digital en busca de víctimas que en ocasiones son conscientes de haber sido objeto de un delito transcurrido un tiempo de su ejecución. Lo que facilita a su transgresor un beneficio real y en el acto, facilitando su enriquecimiento, a la vez que permite disponer de un periodo de escape para su desaparición y dificultando su persecución.

1.2 LA CONSTANTE EVOLUCIÓN DE LA CIBERDELINCUENCIA

La aparición del fenómeno de Internet ha supuesto una revolución tecnológica de incalculable alcance donde el concepto de sociedad en su amplio concepto ha experimentado un cambio sustancial en todos los órdenes de su comportamiento y hábitos de la vida cotidiana. Desde que en 1969 hiciera acto de presencia la “Red de redes” los sistemas informáticos han pasado a ocupar un papel primordial en todos los campos y registros de la sociedad. En la actualidad, todas las organizaciones tanto públicas como privadas, y el propio individuo como ser singular, han pasado a tener una dependencia total de los sistemas informáticos que se apoderan de los procesos de toda índole como los políticos, económicos, deportivos, culturales, sociales, donde se interrelacionan haciendo una gran tela de araña donde se ubica toda una información que trasciende de manera global, no solo desde una perspectiva del individuo como ser único y aislado sino como una parte del mundo global. Esto supone un gran avance en cuanto a las posibilidades de facilitar una serie de actos que redundan en beneficio de la persona, economizando tiempo y espacio para resolver

asuntos de carácter personal, administrativo, laboral o de cualquier otra índole, pero también ocurre esta innovación que nos facilita múltiples labores, hace que aparezca otra modalidad encauzada hacia la criminalidad, a la cual, le facilita y amplía su espectro delictivo dejando atrás la considerada delincuencia tradicional.

Con este desarrollo exponencial de Internet, comienzan a surgir nuevos términos hasta entonces no conocidos como ciberdelincuencia, cibercrimen, ciberterrorismo, ciberamenazas, ciberacoso, y otros similares todos ellos vinculados al desarrollo tecnológico que comienza a invadir el espacio cibernético dejando atrás aspectos y actitudes ya consideradas anticuadas y obsoletas dentro del campo delincencial.

La evolución como forma de transformación implica una serie de cambios que tiene lugar en una actividad determinada. En el campo criminal el avance tecnológico, además de representar una innovación delictiva, agiganta otro modelo más efectivo y de mayor profundidad. El ciberespacio facilita para las tareas delictivas una mayor facilidad en su ejecución, al contar menos riesgos u obstáculos por parte de la víctima para realizar el acto punible; no precisan de notables recursos para ejecutar su acción; no precisan de la presencia física del perjudicado toda vez que se puede llevar a cabo por medio del ciberespacio y, por último, un hecho relevante y primordial, la impunidad de sus delitos al no contar algunos Estados con una legislación que contemple y recoja la tipificación de dichos actos, quedando en la impunidad al contener lagunas dentro de su campo jurídico que no puedan sancionar las conductas criminales.⁴

La comisión de estos actos delictivos basados en el ciberespacio suele acontecer basándose en una relación cuadrangular. Si nos basáramos en la actividad delictiva tradicional tendríamos esa misma relación en cuanto a los requisitos para su ejecución: el sujeto activo o delincuente, el pasivo o víctima, el espacio de su ejecución y la temporalidad para ser llevado a cabo la acción criminal. En el caso del ciberdelito, igualmente, está el *sujeto activo* que es el encargado de insertar en la red la acción destructiva o dañosa, a través de los sistemas informáticos. Los *coadyuvantes*, o los facilitadores, carentes de intencionalidad, que propulsan la ejecución al ser el proveedor de los servicios de Internet, al conectar al usuario a través de la línea telefónica a Internet. *El servidor de web* donde se aloja en un disco duro la información destructiva. Y, por último, el *sujeto pasivo* -la víctima-, donde en ocasiones esa acción delictiva o dañina puede resultar desconocida carente de una decisión determinada movida por el ánimo de causar un mal a la víctima y un

4 Cfr., SUBIJANA ZUNZUNEGUI, Ignacio José, El ciberterrorismo: una perspectiva legal y judicial, Eguzkilore, número 22, San Sebastián, 2008, p. 171.

beneficio al autor criminal, pero sin conexión ni animadversión conocida, al tratarse de una acción virtual, es decir, a través del ciberespacio.⁵

Esta innovación tecnológica provocará un nuevo contexto en la existencia del concepto de la oportunidad criminal donde deja de ser necesaria la presencia del delincuente y de la víctima en un tiempo real y un espacio común. La figura del criminal sigue presente en la casuística del delito siendo necesaria su participación para el acto delictivo, pero no ocurre lo mismo con el entorno espacial o temporal, los cuales pueden ser ubicados fuera del espacio del autor y, en tiempo no presente. Es decir, que la víctima percibe el hecho delictivo en un espacio geográfico distinto al causante del hecho punible y de forma intemporal.⁶

La ciberdelincuencia se fundamenta en los avances tecnológicos pero sus raíces proceden de la delincuencia tradicional. Los delitos actuales no difieren en su esencia de los practicados en tiempos pretéritos, sus figuras delictivas siguen siendo las mismas, si bien se ven actualizadas con la aparición de las nuevas tecnologías informáticas que hacen que su forma de ejecución difiera en ciertos aspectos a la hora de la consumación del acto criminal. Dos aspectos que diferencian el modelo tradicional y el tecnológico radican en la necesidad del espacio y tiempo para su consumación.⁷

En consecuencia, para hacer realidad el hecho punible y, ante la falta de necesidad de la unión del espacio y tiempo para su ejecución, se hace precisa la aparición de un nuevo ciberespacio denominado *espacio virtual*. Espacio donde se intercambian informaciones siendo necesaria la ubicación de un espacio terrestre donde tenga lugar la ubicación de los terminales informáticos donde se reciba la información emitida por el agente a fin de ser recibida por la presunta víctima y donde a través de este espacio virtual tiene lugar la conexión del espacio-tiempo. También esta premisa de su ubicación en un espacio terrestre fijo y, con las innovaciones posteriores, han dejado de ser imprescindibles al poder seguir recibiendo la información tanto el emisor como el receptor en movimiento a través de la denominada: *telefonía móvil*.⁸

El hecho de que el desplazamiento espacial no sea necesario y que su coste pueda verse minorado, no implica que no tenga una importancia temporal para

5 Ibidem., p. 171.

6 Op. cit., ÁGUILA SÁNCHEZ, Miguel Ángel, p. 264.

7 Ibidem., p. 264.

8 Ibidem., p. 264.

su ejecución en el ciberespacio.⁹ El coste estará en función del delito de que se trate. En los supuestos económicos, tanto su desarrollo como su ejecución, exige la presencia de los *hackers* en busca de las vulnerabilidades que pueda ofrecer el sistema informático objeto de su manipulación. Y, en esa selección de la víctima por parte del agresor radica la elección de la creación del *software* pertinente para que sea la propia víctima la que al interaccionar sea “expoliada”.¹⁰

Lo realmente característico del ciberespacio radica en dos causas fundamentales: la *primera*, en que al no ser necesario el desplazamiento para la acción delictiva hace que conlleve un incremento en el número potencial de víctimas al poder hacer una mejor selección a la hora de decidir su mejor objetivo. Y, la *segunda*, porque supone una reducción del coste espacio-temporal. Aunque esto no implica que no exista un precio temporal, el cual, estará supeditado al tipo del acto punible que se trate de realizar.¹¹

Los ciberdelitos han pasado a ser dentro del panorama social actual una fuente de enriquecimiento presente, no solo a nivel individual del delincuente, ocasional o habitual, sino que ha representado un campo productivo de múltiples facetas para grupos u organizaciones criminales. La aparición de las nuevas tecnologías en el siglo XX va de alguna manera a arrinconar o dejar en un segundo plano a la delincuencia tradicional.

Estos ciberdelitos comienzan su andadura en 1834, donde dos ciberdelincuentes consiguen piratear el sistema del telégrafo francés consiguiendo información del mercado financiero, lo que es considerado como el primer ciberataque registrado en el mundo.

Los primeros vestigios de los ciberdelitos podrían ser considerados en una primera etapa entre las décadas de 1940 y 1960, donde sus primeras conexiones a través de los ordenadores conectados entre distintos organismos eran considerados de una cierta seguridad en la creencia de que tanto los sistemas como los datos que pudieran ser recogidos en los mismos gozaban de mecanismos que eran inaccesibles a terceros. Sin embargo, surgirán ejemplos en este periodo donde se tiene constancia de diversos sucesos que servirán de aviso que la Red puede ser reconducida por terceras personas hacia un fin delictivo a través de su infiltración en las bases de datos de otros interlocutores. Un primer *hacker* ético, es el realizado por Rene Carmille,

9 Cfr., MIRÓ LLINARES, Fernando, El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Derecho Penal y Criminología, Editorial Marcial Pons, Madrid, 2012, pp. 171-172.

10 Op. cit., ÁGUILA SÁNCHEZ, Miguel Ángel, p. 265.

11 Cfr., MERLOS, Alfonso, Terror.com. Irak, Europa y los nuevos frentes de la Yihad, Ediciones Universidad de Navarra (EUNSA), Navarra, 2008, p. 150.

miembro de la Resistencia Francesa durante la ocupación nazi en la Segunda Guerra Mundial, experto en computadoras de tarjetas perforadas que el gobierno de Vichy (Francia) usa para el procesamiento de información, y donde detecta que los nazis utilizan *punch* –máquinas de cartas para procesar y rastrear a los judíos voluntarios para permitirles usar el suyo, y posteriormente, piratearlos para eliminar su plan–.¹²

En las dos décadas siguientes 1970-1980,¹³ en esta segunda etapa, las computadoras se convertirán en el gran objetivo a ser manipuladas con la intencionalidad de extraer la información necesaria para utilizar sus datos para lucrarse mediante su desviación de su contenido en beneficio particular, tanto a nivel individual como grupal u organizativo. Con su expansión y con el crecimiento exponencial que surgía en los sistemas informáticos las lagunas penales cada vez más notorias dejan a las víctimas sin un amparo legal y, mucho menos, una satisfacción al agravio sufrido.

La rapidez en los sistemas informáticos unido en estos primeros periodos de clandestinidad, desde el prisma de su persecución, hace que los ciberdelitos crezcan no siendo amparados por una legislación que se veía desbordada para su tipificación ante la novedad y aparición de un modelo delictivo carente de los recursos necesarios para ir al ritmo que las organizaciones criminales contaban al invertir grandes sumas de capital en su implantación de medios informáticos. Una de las primeras manifestaciones de la delincuencia informática tendrá su base en el sistema económico, dando lugar al fraude informático, manipulación de datos y, otra serie de actividades basadas en el sabotaje industrial.

En la segunda etapa de estas décadas citadas, el aumento y adquisición por parte de la población de forma generalizada, va a suponer el surgimiento de la piratería del *software*, incidiendo de forma notoria en infracciones contra la propiedad intelectual y extendiéndose a la década de 1990, donde tendrá su impacto de forma directa en el mundo audiovisual.¹⁴

La tercera etapa en la década de 1990, tiene lugar la gran expansión de los ordenadores ocupando un papel predominante en el mundo de la comunicación. Los hogares, oficinas, centros oficiales y todo un entramado comercial, van a acaparar este medio tecnológico haciendo desaparecer toda documentación y su sistema de archivo tradicional. La información comienza a ser globalizada y los constantes avances

12 Cfr., Historia del cibercrimen, Observatorio Guatemalteco de Delitos Informáticos (OGDI). Disponible en: <https://ogdi.org/historia-del-cibercrimen> (2016-2024).

13 Cfr., CORDERO RUIZ, Nuria Fernanda, La Ciberdelincuencia. The Cybercrime, Alcalá de Henares (Madrid), 2021, p. 6.

14 Cfr., HERNÁNDEZ DÍAZ, Leyre, El delito informático, Eguzkilore, número 23, San Sebastián, 2009, pp. 229-230.

tecnológicos tendrán un sinfín de adeptos y consumidores que irán incorporándose a un nuevo tipo de comunicación.

La información personal se encuentra en el ciberespacio donde todo dato que se cuelga en la Red automáticamente es absorbido en tiempo real desde cualquier lugar del mundo.¹⁵

En el siglo XXI los avances tecnológicos continúan expandiendo su campo de acción encontrándose en todos los estamentos oficiales almacenando toda su información y convirtiéndose en un foco de atracción para organizaciones criminales que contemplan un panorama delictivo de forma inmediata y de grandes recursos para incrementar su riqueza económica.

1.3 CARACTERÍSTICAS DE LA CIBERDELINCUENCIA

La globalización ha traído una revolución en el mundo de la comunicación sin precedentes en lo relativo a conceptos tanto genéricos como específicos, como son la economía, la seguridad, el ocio, la comunicación social, el mundo laboral, y otra serie de procedimientos que encuentran su acomodo en el ciberespacio, convirtiéndose en una fuente de almacenamiento y distribución que no tiene límites.



15 Op. cit., CORDERO RUIZ, Nuria Fernanda, p 7.

La Red va a suponer para la población un gran avance en cuanto a su forma de adquirir información de forma instantánea, ahorrándole un tiempo para obtener su contenido. Pero igualmente surgirá un mundo paralelo al margen de la legalidad haciendo acto de presencia grupos y organizaciones criminales basadas en la ciberdelincuencia, cibercrimen o el ciberterrorismo.¹⁶

El uso de los TIC (Tecnologías de la Información y las Comunicaciones) hace que la seguridad en el tratamiento de nuestros datos provoque gran incertidumbre en cuanto a la seguridad. Debido a ese flujo de información que transcurre por la Red los estados han tratado de establecer unos sistemas de seguridad que puedan servir de barrera ante ataques exteriores. El concepto de cibercrimen es difícil de tipificar y de dar una definición que cubra el espectro delictivo que abarca ya que a través de la Red su abanico es infinito, desde el delito económico, pasando por ciberamenazas, coacciones, robo de datos, acoso, pornografía infantil, suplantación de identidad, *cyberbullying*, *grooming*, *phishing*, etc., por lo que se hace preciso implantar unos sistemas de seguridad que contrarresten estas modalidades delictivas.

Existen diversas interpretaciones sobre que debe entenderse por delito informático entendiendo este en un primer momento como: “un acto delictivo que se comete a través de la informática teniendo como objetivo una computadora, o la utilización de esta, de una red de computadoras o de cualquier dispositivo en red”. En consecuencia, y ante la aparición y extensión de Internet estas acciones comenzaron a generalizarse en el espacio virtual dando lugar a la denominación del cibercrimen.

En consecuencia, y en base a las definiciones expuestas por numerosos tratadistas expertos en el tema se podría afirmar que: “el cibercrimen es toda acción delictiva realizada a través de un equipo informático o de Internet, con la finalidad de causar un daño a terceros o de obtener un beneficio propio utilizando el ciberespacio”.

Dentro de las características de la ciberdelincuencia al tratarse de delitos que pueden ser cometidos desde cualquier lugar físico del planeta y sin necesidad de asociación para ejecutar sus acciones delictivas con otro organismo o persona, lo que origina una mayor dificultad para su localización creando una mayor incertidumbre motivo por el cual se precisa un plan general de ciberseguridad que resguarde nuestra información y base de datos de ataques externos.

16 Op. cit., ÁGUILA SÁNCHEZ, Miguel Ángel, p. 279.

Entre las características de las nuevas tecnologías podríamos citar las siguientes:

1. Carencia de barreras geográficas. Los ciberdelincuentes poseen un campo de actuación global para sus actuaciones delictivas dotándoles de múltiples posibilidades para llevar a cabo incluso varias tareas simultáneas lo que le permite un mayor beneficio y una mayor dificultad para su rastreo.
2. Inmediata. Esta es de una celeridad que se produce en el mismo instante en que se está ejecutando la acción criminal, es por tanto, de una rapidez instantánea lo que facilita al autor del acto delictivo unos beneficios en el momento en que lleva a cabo el ciberdelito.¹⁷
3. Anonimato. El sistema jurídico actual se encuentra con múltiples dificultades para combatir estos delitos que tienen lugar a través de Internet. La gran cantidad de actos cometidos en la Red y, el gran número de organizaciones criminales que operan en el ciberespacio, unido a la celeridad de sus actuaciones representan un obstáculo para su persecución por lo que muchas de ellas quedan sin poder ser controladas.

Los ordenadores tienen asignado una dirección IP (*Internet Protocol*) por lo que su seguimiento resulta complejo pudiendo detectar su dinamismo. Sin embargo, el problema surge cuando esos protocolos son manipulados no garantizando la autoría de la acción. El anonimato viene motivado precisamente porque no requiere de un espacio concreto para su realización sino que se puede realizar de forma universal, es decir, no precisa de una cercanía entre el delincuente y la víctima.¹⁸

4. Universalidad del espacio. En el delito tradicional resultaba necesaria la cercanía para la comunicación entre emisor y receptor. En la actualidad, el ciberespacio elimina esta característica y dota al ciberdelincuente de la posibilidad de realizar el hecho punible sin tener que llevarlo a cabo en un espacio común lo que facilita evitar una serie de obstáculos en su ejecución, pudiendo incluso ser intemporal.¹⁹

17 Op. cit., CORDERO RUIZ, Nuria Fernanda, p. 11.

18 Op. cit., ÁGUILA SÁNCHEZ, Miguel Ángel, p. 280.

19 Ibídem., p. 280.

5. Reproducción masiva. Los múltiples contenidos que alberga Internet hacen que su expansión no tenga límites y sean una fuente de consulta por parte de organizaciones criminales para sus actividades delictuales.²⁰
6. Dificultad para su persecución. El entramado del ciberespacio hace que la dificultad para el seguimiento de los ciberdelinquentes resulte de una complejidad extraordinaria lo que facilita su rápida desaparición una vez realizadas sus acciones delictivas en esa tela de araña que constituye el espacio en la Red.
7. Propagación de noticias falsas o *fake news*. Los países tratan de articular estrategias que puedan combatir de forma eficaz la desinformación que circula a través de Internet intentando manipular a la opinión pública a través de bulos o de información adulterada constituyendo una amenaza global para los estados y suponiendo grave perjuicio para la libertad de los ciudadanos, lo que conlleva un riesgo para las democracias, ya que puede crear un clima de inestabilidad en la sociedad al difundirse noticias falsas que puedan desestabilizar el normal funcionamiento de la población.

1.4 PERFIL DEL CIBERDELINCUENTE. EL DELINCUENTE INFORMÁTICO

La Criminología según nuestra Real Academia Española es: “La ciencia que estudia las causas y circunstancias de los distintos delitos, la personalidad de los delinquentes y el tratamiento adecuado para su represión”.²¹

El delincuente tradicional se ha caracterizado por poseer una habilidad determinada para la comisión de su actividad delictiva en función de las características y de su *modus operandi*. Así, a lo largo de la historia delincuencia, y todavía en tiempos presentes podemos apreciar diversas modalidades relajadas por delinquentes habituales como: robos, hurtos, estafas, amenazas, coacciones, de la trata de seres humanos, agresiones sexuales, acoso sexual, calumnia, injurias, lesiones, homicidios, asesinatos, extorsión, etc., y un sinnúmero de conductas que han precisado, en algunos de sus casos, de una maestría para su realización. Sin embargo, el perfil del ciberdelincuente requiere en principio de una preparación más cuidada desde un prisma de su especialización. En principio es necesario poseer un mínimo nivel de conocimiento del sistema informático en cuanto a su utilización. En cuanto a su grado de conocimiento sus actividades o hechos delictivos podrán abarcar un

20 Op.cit., CORDERO RUIZ, Nuria Fernanda, p. 13.

21 Diccionario de la Real Academia Española (RAE), 23ª edición, de octubre de 2014. Disponible en <https://www.rae.es/obras-academicas/diccionarios/diccionario-de-la-lengua-espanola>.

campo cibernético más amplio desde el robo de identidad, la infección del *malware*, el *phishing*, la extorsión, las estafas, el acoso, etc.

Tratar de establecer un perfil criminal concreto del ciberdelincuente resultaría posiblemente algo inexacto e incompleto debido al múltiple espacio que abarca Internet y sus innumerables campos delictivos que pueden ser objeto de un mismo perfil del delincuente informático dada su heterogeneidad. Sin embargo, lo que resulta necesario es que por parte del sujeto activo del hecho punible tenga unos mínimos conocimientos de la informática. En base a estos conocimientos se estaría en poder establecer una categorización de los usuarios del medio. Por un lado, los que se podrían denominar especialistas que estarían interesados en profundizar en el sistema en busca de la información que necesita para realizar su acción delictiva, requiriendo un gran conocimiento informático para acceder a los datos que precisa para perpetrar el delito. Mientras que, en un segundo plano, no se trata de un fin en sí mismo, sino que su meta es conseguir el objetivo que persigue.²²

Por lo que se viene manifestando al delincuente cibernético, el procesamiento electrónico de datos le acrecienta las posibilidades de éxito en su actuación ilícita convirtiendo esos conocimientos en un factor criminógeno para llevar a cabo su actuación.²³

La informática ha ido evolucionando de forma exponencial convirtiéndose en un elemento indispensable para cualquier tipo de actividad. En principio, el delincuente informático, era en su gran mayoría jóvenes que eran atraídos por un mundo virtual que les ofrecía un panorama de actuaciones hasta ahora desconocidas. Su utilización era un modo de aparecer entre sus colegas como alguien con unos conocimientos que destacaba del resto de sus compañeros. En el mundo laboral y cuando las empresas comenzaron a estandarizar su uso como método de trabajo para sus planteamientos el abanico de posibilidades de su utilización fue incrementándose dejando de ser un objeto lúdico convirtiéndose en una herramienta de infinitas vertientes.

Sin embargo, su utilización no siempre va a estar destinada con fines lícitos, sino que aparece el delincuente informático cuyo propósito, al igual que ocurriera con el delincuente tradicional, basara su experiencia y conocimiento en la búsqueda del enriquecimiento personal. En un principio, de forma más limitada, para posteriormente y, de acuerdo con su conocimiento y posibilidades de obtener medios más sofisticados, ampliar su campo de acción delictiva contra empresas,

22 Cfr., CÁMARA ARROYO, Sergio, Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente, Derecho y Cambio Social, nº 60, abril-junio 2020, pp. 486-487.

23 Cfr., DE LA CUESTA ARZAMENDI, José Luis y PÉREZ MACHÍO, Ana Isabel, Parte II, Aspectos Criminológicos y Victimológicos, Ciberdelinquentes y cibervíctimas, Capítulo 3, p. 100.