

## Capítulo 3

# La arquitectura ilícita del ciberespacio: cibercrimen y ecosistemas de la dark web\*

DOI: <https://doi.org/10.25062/9786287818705.03>

**Carlos Enrique Álvarez Calderón**

Escuela Superior de Guerra "General Rafael Reyes Prieto"

**Resumen:** Este capítulo analiza la arquitectura y el funcionamiento del cibercrimen organizado en la red oscura, las redes sociales y los entornos metaversos enmarcando estos dominios como componentes de un ecosistema criminal transnacional que convergen. A partir de la teoría criminológica, la literatura sobre cibercrimen y el modelo de los ecosistemas criminales, el estudio identifica los facilitadores estructurales, tecnológicos y culturales que sustentan las economías digitales ilícitas. Explora, además, cómo los roles especializados, las infraestructuras de anonimato y las plataformas descentralizadas posibilitan formas modulares y resilientes de organización criminal. El capítulo también introduce el concepto de desviación digital, como precursor cultural del comportamiento cibercriminal, y analiza los delitos emergentes en entornos inmersivos (metacrímenes). Finalmente, ofrece recomendaciones estratégicas para la seguridad nacional colombiana, incluyendo reformas institucionales, actualizaciones legales, marcos de ciberinteligencia y rendición de cuentas de las plataformas, para contrarrestar las amenazas en constante evolución dentro del ecosistema criminal digital. valuar de manera efectiva cómo contribuyen al IS a través de sus dimensiones de análisis.

**Palabras clave:** cibercrimen; ecosistema criminal; metacrímenes; red oscura

---

\* Capítulo de libro resultado del proyecto de investigación "Desafíos y nuevos escenarios de la seguridad multidimensional a nivel nacional, regional y hemisférico en el decenio 2015-2025", del grupo de investigación Centro de Gravedad, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado como A por MinCiencias y registrado con el código COL0104976. Los puntos de vista pertenecen a los autores, y no necesariamente reflejan el pensamiento de las instituciones participantes.

## Carlos Enrique Álvarez Calderón

Candidato a doctor en Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Coaching Ontológico Empresarial, Universidad San Sebastián, Chile. Politólogo y Magíster en Relaciones Internacionales, Pontificia Universidad Javeriana, Colombia. Investigador Asociado MinCiencias y Docente Investigador, Escuela Superior de Guerra "General Rafael Reyes Prieto". Profesional Oficial de Reserva, Fuerza Aeroespacial Colombiana. Asesor y consultor en seguridad y defensa para instituciones de las Fuerzas Militares de Colombia y a nivel internacional.

<https://orcid.org/0000-0003-2401-2789> - Contacto: [carlos.alvarez@esdeg.edu.co](mailto:carlos.alvarez@esdeg.edu.co)

**Citación APA:** Álvarez Calderón, C. E. (2026). La arquitectura ilícita del ciberespacio: cibercrimen y ecosistemas de la dark web. En C. E. Álvarez Calderón (Ed.), *El campo de batalla digital: la defensa nacional en la era algorítmica, Volumen I. (Infraestructuras de la guerra digital: computación, ciberguerra y defensa del ciberespacio)* (pp. 177-236). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818705.03>

## EL CAMPO DE BATALLA DIGITAL: LA DEFENSA NACIONAL EN LA ERA ALGORÍTMICA

### VOLUMEN I. INFRAESTRUCTURAS DE LA GUERRA DIGITAL: COMPUTACIÓN, CIBERGUERRA Y DEFENSA DEL CIBERESPACIO

ISBN IMPRESO (Obra completa): 978-628-7818-65-1

ISBN DIGITAL (Obra completa): 978-628-7818-69-9

ISBN IMPRESO Volumen I: 978-628-7818-66-8

ISBN DIGITAL Volumen I: 978-628-7818-70-5

DOI: <https://doi.org/10.25062/9786287818705>

### Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2026



## Introducción

La *dark web* se ha vuelto un terreno crítico en el campo de la batalla digital, y ha permitido el auge de ecosistemas complejos de ciberdelincuencia organizada. A diferencia de los ciberdelincuentes convencionales, que operan de forma aislada o con poca coordinación, las redes cibercriminales organizadas aprovechan las ventajas tecnológicas de las herramientas de anonimización<sup>1</sup>, las comunicaciones cifradas y los mercados descentralizados para escalar y mantener operaciones ilícitas en jurisdicciones globales (Lusthaus, 2018; Holt & Bossler, 2020). Estos actores constituyen un submundo digital caracterizado no solo por la delincuencia transaccional (por ejemplo, la venta de narcóticos, armas, *malware* y datos robados), sino también por una lógica cada vez más corporativa de prestación de servicios ilícitos, división del trabajo y optimización de beneficios (Graham & Smith, 2024; Alexandrou, 2021).

La arquitectura de la *dark web*, en particular de las plataformas que operan a través del rutador Onion (Tor) e I2P, ha permitido la ocultación de identidades, geolocalizaciones y huellas digitales, lo que la convierte en un terreno fértil para mercados criminales como Silk Road, AlphaBay, Dream Market e Hydra (Ozkaya & Islam, 2019; Nearchou, 2023). Estas plataformas no solo facilitan las transacciones lícitas e ilícitas, sino que también replican los mecanismos de confianza del legítimo y popular comercio electrónico, como las calificaciones de los proveedores, los servicios de depósito en garantía y la resolución de disputas, lo que refuerza la retención de usuarios y la continuidad operativa (Watters, 2024; Holt et al., 2022). Por ende, la convergencia del anonimato, alcance transnacional y alta rentabilidad

---

<sup>1</sup> La "anonimización" es un proceso que transforma datos personales de manera que ya no se pueda identificar a las personas a las que se refieren. Esto se logra eliminando o modificando los datos identificables para obtener información anónima. La anonimización es crucial para proteger la privacidad de los individuos y cumplir con la normativa de protección de datos.

permiten que las empresas criminales prosperen pese a la intensificación de las intervenciones policiales y el cierre de mercados (Jenkinson, 2022; Viano, 2017).

Cabe señalar que la ciberdelincuencia organizada en la *dark web* no es tan solo un fenómeno económico: es también una configuración sociotécnica que difumina las fronteras entre la desviación, delincuencia y las subculturas digitales. Si bien este capítulo se centra en el análisis de las organizaciones cibercriminales y las infraestructuras de la *dark web*, es importante reconocer el papel de la desviación digital como entorno propicio. Las comunidades digitales desviadas (incluidos los foros de *hackers*, redes de piratería y culturas del *troleo*), suelen servir de incubadoras de conductas delictivas al normalizar prácticas ilícitas y proporcionar formación técnica entre iguales (Graham & Smith, 2024; Noble et al., 2017). Estos elementos subculturales, aunque no son delictivos *per se*, reducen las barreras a la ciberdelincuencia y refuerzan identidades arraigadas en ideologías antisistémicas o libertarias (Holt et al., 2022; Kremling & Sharp Parker, 2017).

Lo anterior plantea la pregunta central de investigación de este capítulo del libro: ¿Cómo operan y evolucionan las redes cibercriminales organizadas dentro de los ecosistemas de la web oscura, y cuáles son las dinámicas estructurales, tecnológicas y criminológicas que sustentan estas economías ilícitas? Es imperativo abordar ese interrogante desde los estudios en seguridad y defensa, con el propósito de desarrollar contramedidas eficaces que vayan más allá de la mitigación técnica y abarquen dimensiones legales, culturales y estratégicas.

La relevancia teórica y política de este campo de estudio se ve subrayada por los desafíos que el cibercrimen organizado plantea a los sistemas legales, a las agencias de inteligencia y a las arquitecturas de ciberseguridad. Los modelos tradicionales de control de la delincuencia organizada son cada vez más inadecuados en el ciberespacio, debido a su naturaleza fluida, sin fronteras y cifrada (Clough, 2015; Donalds et al., 2022). Para responder a eso, Estados y organizaciones internacionales han desarrollado instrumentos jurídicos transnacionales (por ejemplo, el Convenio de Budapest), así como respuestas tácticas que incluyen la informática forense digital, la OSINT<sup>2</sup> y las estrategias de ciberinfiltración (Holt & Bossler, 2020; Bandler & Merzon, 2020; Akhgar et al., 2021). Sin embargo, la ecología de la red oscura, en rápida evolución, continúa superando a los marcos regulatorios y de aplicación de la ley.

---

<sup>2</sup> Open Source INTelligence (Inteligencia de Fuentes Abiertas), es una disciplina que se enfoca en recolectar, analizar e interpretar información de fuentes públicas y accesibles legalmente.

En consecuencia, el presente capítulo se propone analizar los elementos estructurales, tecnológicos y criminógenos de la ciberdelincuencia organizada en la red oscura situando dichos fenómenos en contextos sociológicos y criminológicos más amplios. El documento comienza describiendo la dinámica operativa de los grupos cibercriminales, para explorar posteriormente la arquitectura y la gobernanza de los mercados ilícitos y, finalmente, analizar los facilitadores criminógenos y los desafíos para la aplicación de la ley. La desviación digital se examinará como una capa contextual secundaria que configura el entorno cultural y psicológico de este ecosistema.

## La ciberdelincuencia organizada en la era digital

El cibercrimen se ha convertido en un fenómeno global donde actores ilícitos utilizan tecnologías en red para cometer delitos a escala transnacional. En ese contexto, el cibercrimen se solapa con el crimen organizado tradicional, pero opera a través de plataformas digitales, como los mercados, productos y servicios ilícitos de la web oscura, el *ransomware* y el fraude en línea. El alcance de la ciberdelincuencia organizada ahora incluye mercados delictivos (por ejemplo, de drogas o datos), ofertas de delincuencia como servicio (CaaS), e incluso, operaciones cibernéticas habilitadas por Estados mafiosos y cleptocráticos. Como observa Viano (2017), estos avances se deben a la convergencia de oportunidades de bajo riesgo y alta rentabilidad en el ciberespacio para el crimen organizado, ya que Internet facilita el tráfico global y el movimiento de dinero. Asimismo, actores criminales patrocinados por algunos Estados han perseguido objetivos estratégicos y financieros mediante la perpetración de ciberdelitos.

### Definición de cibercrimen y de ciberdelincuencia organizada

En principio, el cibercrimen podría conceptualizarse como los delitos perpetrados a través de redes informáticas o sistemas digitales atacando la infraestructura digital o utilizándola como medio para facilitar las actividades ilícitas. Empero, las definiciones de "cibercrimen" y "ciberdelincuencia organizada" han cambiado en las últimas dos décadas, a medida que la evolución de las tecnologías digitales ha transformado la naturaleza del comportamiento delictivo. Si bien no existe una definición universalmente consensuada, académicos, organismos internacionales e

instituciones jurídicas han proporcionado múltiples marcos que intentan delinear estos fenómenos en términos tanto conceptuales como operativos.

Según Payne (2020), las definiciones con relación al “cibercrimen” son importantes por al menos siete razones que se superponen: 1) la forma como las personas definen el cibercrimen determinará las estimaciones sobre su alcance; 2) las definiciones de cibercrimen influirán en las consecuencias (o respuestas individuales) a comportamientos específicos; 3) las definiciones de cibercrimen tienen implicaciones en la forma como los criminólogos intentan explicar los delitos cibernéticos; 4) las definiciones guiarán las estrategias de intervención utilizadas para responder a ciertos tipos de comportamiento; 5) las definiciones guiarán las estrategias de prevención utilizadas para prevenir ciertos tipos de comportamientos cibercriminales; 6) las definiciones determinarán también las metodologías de investigación utilizadas para estudiar el comportamiento cibercriminal, y 7) en consecuencia con lo anterior, las definiciones determinarán cómo los académicos enseñan sobre el comportamiento.

En términos académicos las definiciones de cibercrimen tienen ramificaciones en la aplicación de las teorías criminológicas. Siguiendo una perspectiva durkheimiana, por ejemplo, algunos podrían definir el cibercrimen como un comportamiento normal. Desde esa perspectiva, el cibercrimen podría considerarse un fenómeno que cumple al menos cuatro funciones: 1) podría advertir sobre problemas específicos que deben abordarse (el aumento de los fraudes en internet dio lugar a nuevas formas de hacer más seguras las compras en línea); 2) podría, de hecho, impulsar el cambio social (el *hacktivismo* podría ser un ejemplo); 3) podría promover la integración comunitaria, y 4) las definiciones de cibercrimen ofrecen ejemplos de cuáles comportamientos se consideran aceptables, y cuáles, inaceptables. Las definiciones de cibercrimen también impulsan (o al menos se relacionan con eso) las estrategias de investigación. Desde la perspectiva de Payne (2020), quienes definen el cibercrimen con una orientación más social, por ejemplo, podrían ser más propensos a utilizar estrategias de investigación en ciencias sociales para estudiar este fenómeno; mientras, quienes definen el cibercrimen desde una perspectiva más tecnológica probablemente utilizarían otras estrategias.

Ahora bien, una simple revisión de la investigación sobre cibercrimen en el ámbito de la justicia penal confirma que el término no ha existido durante mucho tiempo. Antes de su introducción se utilizaba la frase “delito informático”, y es a Parker (1976) a quien se le atribuye el desarrollo de una de las primeras taxonomías sobre delitos informáticos. La taxonomía de Parker (1976) define los delitos informáticos como aquellos en los que un computador es: 1) el objeto del delito,

2) el entorno donde se comete el delito, 3) el instrumento para cometerlo, y 4) el símbolo del delito (por ejemplo, cuando las personas afirman engañosamente que utilizan recursos informáticos para fundamentar decisiones que conducen a una conducta delictiva). Más tarde, Hollinger y Lanza-Kaduce (1988) desarrollaron uno de los primeros trabajos de criminología sobre el tema centrándose en cómo se llegó a penalizar el delito informático. Luego, la Convención de Budapest sobre Ciberdelincuencia, firmada en 2001, caracterizó estos delitos de una manera que se asemejaba vagamente a la taxonomía de Parker (1976).

Tras la aparición del término "delito informático" los investigadores interesados en estas conductas empezaron a introducir otros términos, tales como: el "delito digital", consistente en "cualquier actividad delictiva que implique el uso de computadores y redes o cualquier otro dispositivo digital" (Sabell et al., 2012, p. 558); el "delito electrónico", caracterizado como "un acto ilegal que se lleva a cabo utilizando una computadora o medios electrónicos" (Kardya & Mitrou, 2007, p. 2); el "delito en internet", definido por el Centro de Quejas de Delitos en Internet como cualquier actividad ilegal que involucre uno o más componentes de internet, como sitios web, salas de chat o correo electrónico; el "delito en la red", el cual se ha descrito como "no solo [...] una forma de interceptación de datos, sino que también implica la intrusión en redes para obtener acceso no autorizado a los datos, o incluso modificarlos, destruirlos, hacer un uso no autorizado de los recursos de la red, etc." (Wang, 2012, p. 1); el "tecnocrimen", que incluye una amplia gama de delitos cometidos en el sistema tecnológico (Friedrichs, 2009), y el "delito virtual", referido a los delitos cometidos en entornos de realidad virtual o juegos virtuales (Lastowka & Hunter, 2004).

Pero ninguno de estos términos ha tenido la misma difusión que el "cibercrimen", aunque sigue siendo un término relativamente nuevo. En este orden de ideas, y según el Convenio del Consejo de Europa sobre Ciberdelincuencia, considerado ampliamente el primer tratado internacional que aborda los delitos cometidos a través de internet y otras redes informáticas, el "cibercrimen" se define como los "delitos contra datos y sistemas informáticos, delitos informáticos, delitos de contenido y delitos contra los derechos de autor" (Krone, 2005, p.1). Wall (2007) ofrece una perspectiva más analítica afirmando que "los ciberdelitos son actividades delictivas o dañinas que son informativas, globales y están interconectadas, y deben distinguirse de los delitos que simplemente utilizan computadoras" (p. 4).

Una definición tecnológica propuesta por Clough (2012) considera el cibercrimen como "el uso de tecnología digital para la comisión o facilitación de delitos" (p. 364). Dicha perspectiva enfatiza la naturaleza instrumental del cibercrimen, al

distinguir entre la intención del delincuente y el medio de ejecución. Por su parte, Interpol añade una dimensión práctica al definir el ciberdelito como un “área delictiva en rápido crecimiento” que aprovecha “la velocidad, la comodidad y el anonimato de internet” para una amplia gama de delitos que “no conocen fronteras, ni físicas ni virtuales” (Ozkaya & Islam, 2019, p. 6). Por eso, el cibercrimen se entiende mejor como un fenómeno multidimensional que incorpora perspectivas jurídicas, tecnológicas, criminológicas y sociológicas. Abarca conductas que van desde la filtración de datos y fraude financiero hasta el ciberacoso y actividades relacionadas con el terrorismo, con una escala e impacto amplificados por la interconectividad global. El autor de este capítulo lo define como las actividades ilegales realizadas mediante sistemas informáticos, dispositivos digitales o redes, ya sea como medio o como objetivo del delito.

Mientras que el cibercrimen se refiere a la naturaleza del delito y a sus medios, la “ciberdelincuencia organizada” describe la estructura y la coordinación de dichas actividades. La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo) ofrece una definición amplia describiendo a un “grupo delictivo organizado” como un “grupo estructurado de tres o más personas, que existe durante un tiempo y actúa concertadamente con el fin de cometer delitos graves (...) para obtener un beneficio económico o material” (UNODC, 2004, art. 2a). Al aplicarlo al contexto digital, Lavorgna (2018) identifica tres características del crimen organizado convencional que se traducen, a su juicio, en la ciberdelincuencia organizada: 1) un conjunto de actividades delictivas, tanto sofisticadas como continuas, a menudo mantenidas mediante corrupción u ofuscación técnica; 2) una organización estructurada con una jerarquía y división del trabajo definidas, y 3) una infiltración sistémica en las esferas económicas o políticas.

La Oficina de las Naciones Unidas contra la Droga y el Delito (en inglés, UNODC, por las iniciales de United Nations Office on Drugs and Crime) establece que por “ciberdelincuencia organizada” se entiende “un delito cibernético [...] que sea: a) cometido por un grupo delictivo organizado, según se define en el artículo 2 [...] de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, [...]; o b) que implique un delito tipificado con arreglo al artículo 5 de la Convención, que abarca la penalización de la participación en un grupo delictivo organizado” (UNODC, 2022, p. 8). A su vez, Graham y Smith (2024) señalan que los grupos de ciberdelincuencia organizada son “organizaciones jerárquicas y estructuradas que realizan actividades delictivas sofisticadas en las que sus miembros desarrollan su propia cultura interna y una reputación de criminales” (p. 135). Estos grupos pueden surgir completamente en el ciberespacio (por ejemplo, colectivos

de *hackers*), o tener su origen en organizaciones tradicionales del crimen organizado que expanden sus operaciones en línea (por ejemplo, grupos mafiosos que realizan ataques de *ransomware* o trafican con contrabando digital). Neto (2017) clasifica, además, a las redes cibercriminales organizadas en tres diferentes tipos: 1) redes híbridas (grupos criminales tradicionales que usan la tecnología para mejorar sus operaciones); 2) redes cibercriminales puras (colectivos descentralizados nacidos en línea que rara vez se reúnen en el mundo físico), y 3) redes con motivaciones ideológicas (como grupos ciberterroristas y hacktivistas, que aprovechan sus habilidades técnicas para alcanzar fines políticos).

Al respecto, lo que distinguiría la ciberdelincuencia organizada de los delitos cibernéticos individuales o poco coordinados sería su escala, continuidad y capacidad para causar daños. Estos grupos suelen participar en empresas delictivas complejas, como el *ransomware* en forma de servicio (RaaS), distribución de *malware*, fraude con tarjetas de crédito, redes de explotación sexual infantil y ciberespionaje. La aparición de los mercados digitales y el modelo de delincuencia como servicio (CaaS) permite a estos grupos externalizar componentes clave (creación de *malware*, blanqueo de capitales o ataques DDoS), lo que mejora tanto la eficiencia como el anonimato. Otra característica de la ciberdelincuencia organizada es su capacidad para trascender fronteras geográficas manteniendo la cohesión funcional, ya que, a diferencia de las bandas callejeras o las mafias, las organizaciones cibercriminales pueden estar formadas por miembros de distintos continentes, comunicarse mediante plataformas cifradas y, a menudo, operar en diferentes zonas horarias (Graham & Smith, 2024).

En resumen, ni el fenómeno del cibercrimen ni la ciberdelincuencia organizada son construcciones jurídicas estáticas, sino fenómenos sociotécnicos dinámicos moldeados por la evolución de las tecnologías y las fuerzas económicas globales, así como las de los entornos criminógenos en línea. Definir el cibercrimen implica reconocer su complejidad y multiplicidad, desde los ataques puramente digitales hasta el fraude cibernético. Definir la ciberdelincuencia organizada requiere prestar atención a la estructura, intención, coordinación y persistencia de los delitos, con crecientes implicaciones para las fuerzas del orden transnacionales y para las políticas de ciberseguridad.

## Evolución histórica del cibercrimen

La historia del cibercrimen está profundamente entrelazada con la evolución de las tecnologías informáticas y de internet. Lo que empezó como experimentos de *hacking* inofensivos se ha convertido en una empresa criminal global que involucra

actores estatales, grupos organizados e infraestructuras sofisticadas. Por lo tanto, enseguida se desarrollan los principales hitos en la evolución del cibercrimen, desde sus orígenes exploratorios hasta su forma industrializada actual.

### **La fase exploratoria: décadas de 1960-1980**

Como ya se mencionó, las raíces conceptuales del cibercrimen se hallan en la manipulación temprana de sistemas informáticos durante la década de 1960. Según Clough (2015), los delitos informáticos inicialmente abarcaban actos como el sabotaje y la manipulación informática, que ocurrían sobre todo dentro de instituciones con acceso a sistemas *mainframe*. Pero durante la década de 1970 dos desarrollos clave sentaron las bases del cibercrimen moderno: en primer lugar, surgió la práctica del *phone phreaking*, que consistía en la explotación de las vulnerabilidades relacionadas con los sistemas de telecomunicaciones para realizar llamadas de larga distancia gratuitas. Cabe destacar que un personaje llamado John Draper, apodado Capitán Crunch, se convirtió en una figura simbólica de esta subcultura. En segundo lugar, la creación del gusano "Creeper", en 1971, representó el primer *malware* autorreplicante conocido, aunque no era en especial dañoso, pues tan solo dejaba un mensaje inofensivo: "Soy el Creeper: atrápenme si pueden".

Sin embargo, para la década de 1980 los delitos informáticos comenzaron a atraer la atención legal y pública. En 1981 Ian Murphy (alias Capitán Zap) se convirtió en la primera persona condenada por un delito informático en Estados Unidos, tras alterar los horarios de facturación en el sistema de AT&T. Y en 1986 el *hacker* alemán Markus Hess se infiltró en las redes militares estadounidenses y vendió el acceso a la KGB, lo que marcó un nuevo nivel de espionaje por medios digitales. Pero el punto de inflexión llegaría en 1988, con el gusano 'Morris', creado por un estudiante de Cornell llamado Robert Morris. Este código autorreplicante causó involuntarias, pero importantes, interrupciones, al bloquear 6.000 sistemas y causar daños estimados en 98 millones de dólares (Alexandrou, 2021).

### **La era de los virus y la respuesta legal: década de 1990**

La década de 1990 marcó la popularización de internet y el consiguiente aumento del cibercrimen. Esta década presenció el desarrollo de sistemas operativos y correos electrónicos intuitivos, que se convirtieron en vectores de transmisión de virus. Ejemplos infames incluyen el virus 'Michelangelo' (1991), el virus 'Melissa' (1999) y el gusano 'ILOVEYOU' (2000), que se propagaron rápidamente a través de archivos adjuntos en correos electrónicos. Al mismo tiempo los gobiernos empezaron a formular marcos legales para contrarrestar las amenazas emergentes.

Estados Unidos aprobó en 1986 la Ley de Fraude y Abuso Informático (en inglés, CFAA, por las iniciales de Computer Fraud and Abuse Act), que se convirtió en una piedra angular para la persecución del cibercrimen. Y a nivel internacional iniciativas como el Convenio sobre Ciberdelincuencia del Consejo de Europa (2001) comenzaron a sentar las bases jurídicas transnacionales. De acuerdo con Nearchou (2023), este período también fue testigo del auge del *phishing*, una forma de ingeniería social en la que actores maliciosos se hacen pasar por entidades legítimas para extraer información confidencial. Suelen incluir imágenes de aspecto oficial, direcciones de correo electrónico y sitios web falsos para engañar al usuario. Los *hackers* envían este tipo de correos electrónicos para robar contraseñas y números de cuentas bancarias o infectar sistemas con virus.

### **La industrialización de la ciberdelincuencia: década de 2000**

A principios de la década de 2000 se inició una nueva era: la profesionalización y comercialización del cibercrimen. A medida que la economía digital se popularizaba, también lo hicieron los incentivos para la explotación criminal. Grupos cibercriminales organizados empezaron a ofrecer lo que se ha venido a denominar *Crime-as-a-Service* (CaaS), mediante el cual herramientas maliciosas como *keyloggers*, *ransomware* y *bots* de *spam* podían comprarse o alquilarse en mercados de la *darknet*.

Desde la perspectiva de Choi et al. (2020), este período coincide con la "Tercera Revolución Industrial" de la ciberdelincuencia, caracterizado por fraudes financieros, robo de identidad y campañas organizadas de *phishing* (tabla 1). El famoso atraco al Citibank, en 1994, cuando Vladimir Levin robó 10 millones de dólares a través de sistemas de banca por internet, es emblemático de esta época. Surgieron foros dedicados a las operaciones de los cibercriminales, que alcanzaron su apogeo a principios de la primera década del siglo XXI. Lusthaus (2018) documenta cómo dichos foros en línea facilitaron el desarrollo de una infraestructura cibercriminal, con sistemas de reputación criminal, servicios de depósito en garantía y roles especializados: desde desarrolladores de *malware* hasta mulas de dinero.

**Tabla 1.** Las cuatro revoluciones industriales, avances tecnológicos y nuevos tipos de crimen

| Revolución industrial         | Periodo          | Avances tecnológicos                                                                                                             | Nuevos tipos de crimen                                                                                     |
|-------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Primera Revolución Industrial | 1760-1840        | Fábricas; ferrocarriles; minería de carbón; textiles                                                                             | Robo de trenes; contrabando; productos falsificados                                                        |
| Segunda Revolución Industrial | 1870-1914        | Electricidad; automóviles; bombillos; teléfono; radio; industria petrolera                                                       | Robo de automóviles; fraude telefónico; robo de servicios públicos; interferencias de radio; robo a bancos |
| Tercera Revolución Industrial | 1969-2010        | Microprocesadores; comunicación por internet; transistores informáticos; energía nuclear; biotecnología; automatización robótica | Hacking; intrusión cibernética; robo cibernético; manipulación de datos; malware; spyware                  |
| Cuarta Revolución Industrial  | 2010- actualidad | Nanotecnología; Internet de las cosas (IoT); inteligencia artificial (IA); criptomonedas                                         | Ransomware para bitcoin; fraude mediante deep fake                                                         |

Fuente: elaboración propia, con base en Choi et al. (2020).

Cada revolución industrial se caracteriza por las tecnologías más significativas de su época. En efecto, la Primera Revolución Industrial fue una era dominada por el vapor y la fabricación mecánica, y estuvo acompañada del auge de la producción en serie característico de la Segunda Revolución Industrial, mientras que la Tercera Revolución Industrial y la Cuarta Revolución Industrial se caracterizaron por la tecnología de la información y las estructuras ciber físicas, que pueden considerarse épocas distintivas, debido a su velocidad, alcance e impacto en la economía global. Desde finales de las décadas de 1960 y 1970 la Tercera Revolución Industrial se ha caracterizado por el desarrollo de las tecnologías de la información y la comunicación (TIC), así como por una creciente industrialización y globalización, y los delitos cibernéticos originados en esta revolución industrial están evolucionando actualmente, debido a las nuevas condiciones de la Cuarta Revolución Industrial. Es decir, si bien persisten los delitos cibernéticos tradicionales, como las estafas en línea, el hackeo y los ataques DDoS, en las últimas décadas se han desarrollado nuevas variantes de estos delitos.

**Ciberdelincuencia globalizada y vinculada al Estado: década de 2010-presente**

La Cuarta Revolución Industrial comenzó en la década de 2010 (Schwab, 2016). Esta revolución ha provocado transformaciones significativas tanto en la vida cotidiana de las personas como en la naturaleza del cibercrimen. Schwab (2016) caracteriza esta era como una marcada por el surgimiento de nuevas tecnologías

que integran los ámbitos biológico, digital y físico, e impactan diversas industrias, economías y campos de estudio. Afirma también que la Cuarta Revolución Industrial genera un entorno global donde los sistemas de fabricación virtuales y físicos colaboran de forma flexible y cohesionada (Schwab, 2016). Esta nueva revolución abarca no solo máquinas y sistemas inteligentes e interconectados, sino también la integración de estas innovaciones y su colaboración en los ámbitos físico, digital y biológico, lo que distingue a la Cuarta Revolución Industrial de sus predecesoras. Durante esta revolución tecnologías emergentes y la innovación generalizada se difunden con mayor rapidez y amplitud que en revoluciones anteriores, y persisten en regiones específicas del mundo (Schwab 2016).

Estas transformaciones tecnológicas y sociales también han introducido nuevas vulnerabilidades y riesgos, sobre todo en lo que respecta a la ciberdelincuencia y la ciberseguridad, por lo que el cibercrimen ha entrado en su fase más compleja hasta el momento. Esta "Cuarta Revolución Industrial" del cibercrimen se caracteriza por ataques patrocinados por Estados, ciberguerra, esquemas de *ransomware* a sueldo y filtraciones masivas de datos. Incidentes notables incluyen el hackeo de Sony PlayStation, en 2011, cuando más de 77 millones de cuentas se vieron comprometidas; la violación de Yahoo, entre 2013 y 2014, que afectó a más de 3 mil millones de usuarios a nivel mundial, y el *ransomware* "WannaCry", de 2017, lanzado por Corea del Norte y que afectó a hospitales y sistemas gubernamentales en alrededor de 150 países. Estas operaciones indican no solo motivaciones financieras, sino también agendas geopolíticas, por lo que algunos académicos, incluyendo a Lusthaus (2018), argumentan que Estados como China y Rusia utilizan cada vez más tácticas de ciberdelincuencia como parte de sus estrategias de gobierno.

En el contexto de la Cuarta Revolución Industrial varios factores críticos pueden contribuir a los desafíos de la ciberdelincuencia y la ciberseguridad: Inicialmente, internet y los ecosistemas tecnológicos, conocidos como "sistemas ciber-físicos" (Schwab 2016), y que abarcan el Internet de las Cosas (IdC; en inglés, IoT) y la computación en la nube crean nuevas oportunidades para que los ciberdelincuentes accedan simultáneamente a los datos y archivos de numerosas personas mediante la infiltración ilegal en los sistemas de computación en la nube (Chaka & Marimuthu 2018). Además, la proliferación de hogares "inteligentes" y los dispositivos del IdC, como Alexa y Google Home, junto con artículos tradicionales como iluminación y mandos a distancia para electrodomésticos, entre otros, permiten a los *hackers* manipular y alterar remotamente estos dispositivos. Los sistemas de reconocimiento facial también pueden ser vulnerados por ciberdelincuentes expertos para obtener acceso no autorizado a teléfonos inteligentes, tabletas y portátiles.

En segundo lugar, en relación con estos nuevos ecosistemas, la integración de dispositivos inteligentes en una red global ha facilitado métodos bancarios innovadores, como Venmo y Zelle. Los sistemas de pago emergentes, como las criptomonedas (Bitcoin y Ethereum), la tecnología *blockchain* y los códigos QR, pueden percibirse como una oportunidad innovadora para los delincuentes, junto con desafíos significativos para las víctimas y las fuerzas del orden (Brenner, 2012). Recientes incidentes de *ransomware* de gran repercusión involucran a ciberdelincuentes que exigen pagos en Bitcoin para evitar la destrucción de datos y archivos personales o comerciales (Luo & Liao, 2009). En este sentido, el anonimato y la confidencialidad de las criptomonedas para ambas partes permiten que este novedoso método de transferencia global de dinero fomente el avance de la ciberdelincuencia transnacional mediante el pago de rescates para la protección de datos valiosos (Mansfield-Devine, 2016).

En tercer lugar, la aceleración de la IA y la automatización se ha visto marcada por la aparición de vehículos sin conductor, aeronaves no tripuladas y sistemas automatizados de venta minorista, como cajeros automáticos y cajas de autoservicio. Estos avances conllevan la aparición de sistemas inteligentes autónomos, que en ocasiones se manifiestan en robots humanoides. Como la IA puede considerarse una convergencia de tecnologías que difumina las distinciones entre los ámbitos físico, digital y biológico, las ramificaciones de la revolución de la IA para el comercio, la industria y la vida siguen siendo parcialmente especulativas. Los problemas más evidentes en este contexto se refieren a la naturaleza cambiante del trabajo y el mercado laboral, que están experimentando una rápida transformación y seguirán haciéndolo (Schwab, 2016).

En resumen, la evolución del cibercrimen refleja transformaciones tecnológicas y sociopolíticas más amplias en comparación con sus formas iniciales, caracterizadas por prácticas aisladas, motivaciones experimentales y capacidades limitadas. Desde los inicios del hackeo motivado por la curiosidad y los gusanos bromistas hasta el *ransomware* actual y las economías de la *darknet* a escala industrial, el cibercrimen se ha convertido en un rasgo característico de la era digital. Asimismo, el cibercrimen también se ha adaptado a nuevas plataformas y tecnologías; la manipulación de redes sociales, *cryptojacking* (minería no autorizada de criptomonedas) y el fraude impulsado por IA ejemplifican esta evolución. Por consiguiente, las tecnologías como la IA, el *big data*, el IdC, la computación en la nube, la realidad aumentada, el Bitcoin y el *blockchain*, entre otras, si bien facilitan la investigación, detección y predicción de actividades delictivas, también introducen nuevas vulnerabilidades que van a ser explotadas por el cibercrimen.

## Tipologías del cibercrimen y la ciberdelincuencia organizada

Comprender las diversas manifestaciones del cibercrimen y la ciberdelincuencia organizada requiere tipologías sólidas que distingan entre comportamientos individuales, métodos tecnológicos y estructuras criminales. Estas tipologías no solo facilitan la claridad analítica, sino que también proporcionan una base estratégica para la aplicación de la ley, el desarrollo legislativo y la inteligencia sobre cibermenazas. En este orden de ideas, la tipología de David Wall (2007) sigue siendo un modelo fundamental en la investigación sobre ciberdelincuencia, en el cual clasifica el cibercrimen en cuatro tipos generales: ciberintrusión, ciberengaño y robo, ciberpornografía y obscenidad, y ciberviolencia. Estas categorías se basan tanto en clasificaciones legales como en distinciones conductuales en la ciberdelincuencia.

La "ciberintrusión" consiste en el acceso no autorizado a los sistemas digitales, comúnmente conocido como *hacking* o *cracking*. Esta categoría abarca tanto intrusiones en sistemas como brechas de red y la implementación de *malware* destinado a comprometer la confidencialidad, la integridad o la disponibilidad. El ciberengaño y el robo incluyen fraudes en línea como el *phishing*, el robo de identidad, las estafas en línea y las violaciones de la propiedad intelectual. Esta suele ser la categoría con más impacto económico, al relacionarse estrechamente con grupos de ciberdelincuencia organizada. La "ciberpornografía" y la obscenidad se refieren a la producción y difusión de contenido sexual ilegal en línea, incluyendo materiales de abuso sexual infantil (MASI) y pornografía no consentida. La "ciber-violencia" comprende actividades que infligen daño psicológico o incitan a la violencia en el mundo real, como el ciberacoso, el ciber-acecho y el discurso de odio en línea.

Estas categorías no son mutuamente excluyentes. Por ejemplo, el uso de *malware* para extorsionar a las víctimas (*ransomware*) puede clasificarse tanto en ciberintrusión como en ciberengaño. Además, la tipología de Wall (2007) ha demostrado ser adaptable, lo que permite su integración con ciberdelitos emergentes como el *cryptojacking*, la sextorsión y las campañas de desinformación (Lusthaus, 2018). Además, los marcos alternativos se centran en las características del objetivo y del actor. Ozkaya e Islam (2019) clasifican el ciberdelito según el objetivo (individuos, propiedades o instituciones gubernamentales), y ahí destaca el ciberterrorismo como una amenaza específica contra las estructuras estatales.

El modelo heurístico de McGuire (2012) ofrece otra perspectiva, al organizar los ciberdelitos en tres niveles: 1) delitos que ocurren exclusivamente en línea, 2)

delitos que combinan componentes en línea y fuera de línea, y 3) delitos fuera de línea facilitados por herramientas digitales. Este enfoque enfatiza la permeabilidad entre comportamientos delictivos digitales y físicos. Y desde una perspectiva psicológica, los actores cibercriminales también se clasifican en perfiles como “*black hat*” (intenciones maliciosas), “*white hat*” (*hacking* ético) y “*gray hat*” (motivaciones ambiguas), lo que refleja la interacción entre las habilidades técnicas y la intención. La UNODC (2022) diferencia dos grandes categorías: los delitos basados en la cibernética y los delitos facilitados por la cibernética. Los primeros son los que no pueden cometerse sin las TIC, como el acceso ilegal a sistemas, el sabotaje digital, la interferencia de datos o la producción y distribución de *malware*. Los segundos incluyen delitos tradicionales que se potencian a través de la tecnología, como el fraude, la falsificación, la trata de personas o el blanqueo de capitales en línea.

Mientras que las tipologías del cibercrimen se centran en los actos, las tipologías de la ciberdelincuencia organizada examinan las estructuras delictivas. Cabe señalar que no todos los delitos cibernéticos son necesariamente organizados, ni todos los grupos delictivos organizados operan en el ciberespacio. No obstante, con la expansión de las economías ilícitas y las tecnologías de anonimización, el delito cibernético organizado se ha convertido en un fenómeno prominente y distintivo. Lavorgna (2020) sugiere que las redes de ciberdelincuencia organizada a menudo cumplen con las definiciones legales de delincuencia organizada (criterios de estructura, continuidad y propósito delictivo de la Convención de Palermo), sin cumplir obligatoriamente con criterios académicos como el control territorial, el uso de la violencia o la monopolización de los mercados.

Graham y Smith (2024) amplían este análisis identificando categorías operativas dentro del delito cibernético organizado: 1) piratería digital, donde los grupos se dedican a la reproducción y venta masiva de contenido protegido por derechos de autor; 2) falsificación de documentos, a menudo utilizada para facilitar el fraude de identidad o actividades ilícitas transfronterizas; 3) lavado de dinero, mediante técnicas como la estratificación de transacciones financieras; 4) ciberterrorismo, que implica violencia ideológica o política mediada por herramientas digitales, y 5) ataques de amplio alcance, incluyendo campañas de implementación de *malware* a escala global.

Por su parte, Leukfeldt et al. (2017) ofrecen una tipología empírica, basada en las redes de *phishing* en Dinamarca. Identifican tres tipos de ciberdelincuencia organizada: 1) las del tipo I, caracterizadas por una baja tecnología y alta interacción, que se basan en ingeniería social y comunicación directa con las víctimas; 2) las

del tipo II, caracterizadas por una baja tecnología y baja interacción (algunos ejemplos incluyen herramientas de *phishing* automatizadas que reducen la interacción personal), y finalmente, 3) las del tipo III, caracterizadas por una alta tecnología y baja interacción, que utilizan *malware* avanzado, troyanos o *rootkits* para extraer datos de forma invisible y automatizar el blanqueo de capitales. Este modelo ilustra un espectro de sofisticación e intensidad de interacción, lo que ayuda a las fuerzas del orden a evaluar el nivel de amenaza y las contramedidas técnicas necesarias.

Otra conceptualización influyente distingue entre el crimen organizado tradicional que se expande al ciberespacio y los grupos organizados nativos en línea. Los primeros pueden usar tecnologías digitales para potenciar el narcotráfico o el tráfico de personas, mientras que los segundos son nativos digitales y operan por completo dentro de los ecosistemas cibercriminales, como los mercados de la red oscura, organizaciones de *ransomware* o proveedores de alojamiento web. El grupo "Carbanak/Cobalt" ejemplifica la complejidad del cibercrimen organizado: operando desde 2013, el grupo utilizó correos electrónicos de *phishing* selectivo y *malware* personalizado para penetrar en instituciones financieras en más de catorce países. Sus operaciones incluían roles como codificadores, mulas de dinero y coordinadores de retiro de efectivo, e involucraban el lavado de fondos a través de criptomonedas y mercados negros. La respuesta transnacional a su arresto, liderada por Europol y el FBI, demuestra tanto la sofisticación de la empresa criminal como el esfuerzo coordinado necesario para combatirla.

De acuerdo con la UNODC (2022), la estructura interna de los grupos delictivos en el ciberespacio varía entre dos extremos: organizaciones jerárquicas con división del trabajo y liderazgos claros, así como las redes distribuidas o "enjambres" sin estructura fija. Un ejemplo del primer tipo lo constituye DrinkorDie, un grupo dedicado a la piratería digital que tenía una estructura organizativa compleja con funciones definidas como codificadores, empaquetadores y proveedores de distribución. Este tipo de grupos se asemeja a organizaciones criminales tradicionales, con roles funcionales y cadenas de mando bien definidas. En el otro extremo se encuentran redes como "Dream Market", donde la descentralización y anonimato dificultan la atribución de responsabilidades. Según la UNODC (2022), las redes difusas suelen organizarse en torno a servicios específicos sin establecer estructuras jerárquicas estables, y operando a menudo como mercados entre pares que conectan compradores y vendedores. Dichas estructuras maximizan la resiliencia ante intervenciones policiales y fragmentan la trazabilidad del delito. Entre estos dos modelos se ubican formas híbridas, donde coexisten niveles de jerarquía

funcional con dinámicas de red. La combinación de liderazgo técnico y libertad operacional permite a estos grupos adaptarse rápidamente a cambios tecnológicos o amenazas legales.

Desde una perspectiva operativa, la UNODC (2022) clasifica a los grupos de ciberdelincuencia organizada en tres categorías principales: grupos predominantemente en línea, grupos híbridos y grupos predominantemente *offline* que utilizan tecnologías digitales para facilitar sus actividades ilícitas. Los primeros son grupos que realizan todas sus operaciones en entornos digitales y se organizan como enjambres o como nodos. Los enjambres se caracterizan por ser agrupaciones temporales y autoorganizadas que se disuelven tras lograr un objetivo específico. Por otro lado, los nodos son más estables y funcionan como células especializadas que colaboran de forma flexible en distintas etapas del ciclo criminal. Ejemplos de esas estructuras incluyen foros de intercambio de *malware*, grupos de *Ransomware-As-A-Service* y comunidades de *hacking* orientadas al lucro (tabla 2).

**Tabla 2.** *Tipologías de ciberdelincuencia organizada según la UNODC*

| Categoría                                       | Descripción                                                                                                                   | Ejemplos                                                   | Características Clave                                                 |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Jerárquicos (tradicionales)</b>              | Estructuras organizadas con liderazgo definido, división de tareas y operaciones coordinadas                                  | <i>DrinkorDie</i>                                          | Organización vertical; roles funcionales claros; control centralizado |
| <b>Redes descentralizadas (enjambres/nodos)</b> | Grupos sin jerarquía fija que se autoorganizan para tareas específicas. Utilizan plataformas digitales y comunicación cifrada | <i>Dream Market</i> ; foros de <i>hacking</i>              | Flexibilidad; anonimato; cooperación horizontal                       |
| <b>Híbridos agrupados</b>                       | Combinan operaciones físicas y digitales. Hay interacción presencial para coordinar delitos que ocurren en línea.             | Redes de fraude con tarjetas                               | Dualidad operativa (online/offline), coordinación presencial          |
| <b>Híbridos extendidos</b>                      | Grupos descentralizados con mínima o nula interacción física. Operan en la <i>dark web</i> y en mercados virtuales            | <i>Silk Road</i> ; redes de <i>Ransomware-As-A-Service</i> | Descentralización; anonimato extremo; presencia transnacional         |
| <b>Tradicionales digitalizados</b>              | Grupos criminales <i>offline</i> que integran tecnologías para mejorar sus actividades (publicidad, pagos, captación)         | Mafias en apuestas ilegales; prostitución virtual          | Uso instrumental de TIC; estructura criminal preexistente             |

Fuente: elaboración propia, con base en UNODC (2022).

Por su lado, los grupos híbridos combinan operaciones en línea y fuera de línea. Según la UNODC (2022), se dividen en híbridos agrupados, que interactúan físicamente para coordinar operaciones digitales como fraudes con tarjetas, e híbridos extendidos, que mantienen una estructura descentralizada con vínculos personales mínimos, tal cual ocurre con plataformas de la *dark web* tipo Silk Road. Este tipo de organizaciones representa un punto medio entre las mafias tradicionales y los colectivos cibernéticos descentralizados. Y finalmente se encuentran los grupos predominantemente *offline* con apoyo digital. Estas organizaciones son criminales tradicionales que utilizan tecnologías de la información para aumentar su capacidad de acción. Por ejemplo, redes dedicadas a apuestas ilegales o prostitución utilizan herramientas digitales para el reclutamiento, la publicidad y el lavado de dinero. Aunque su núcleo operativo sigue siendo físico, el uso de entornos digitales amplía su alcance y reduce sus riesgos.

Una característica común en estas organizaciones es la fragmentación funcional. Como señala la UNODC (2022), la prestación de servicios criminales se distribuye entre múltiples actores especializados: programadores, diseñadores de *malware*, operadores de infraestructuras de anonimato, expertos en cifrado, mulas de dinero y coordinadores de pagos. Este tipo de esquema modular permite a los grupos subcontratar capacidades y mantener el anonimato entre sus miembros, lo que dificulta las tareas de inteligencia y judicialización. A su vez, la existencia de mercados criminales digitales, donde se venden y alquilan herramientas ilícitas, ha dado lugar a lo que algunos expertos llaman Crimen como Servicio (CaaS), el cual permite incluso a individuos sin conocimientos técnicos participar en campañas delictivas sofisticadas mediante el acceso a kits prefabricados y soporte técnico (tabla 3).

Casos como el de "Shadowcrew" y "Card Planet" ilustran cómo operan estos grupos: estructuras de cientos o miles de miembros organizados en función de habilidades específicas, regulados por foros, sistemas de reputación y filtros de admisión. En el caso de "Dreamboard", los miembros debían aportar imágenes ilegales de forma continua para mantener su membresía, lo que refleja una cultura interna orientada al control, la exclusividad y la complicidad activa. Además, el uso de criptomonedas, redes privadas virtuales (en inglés, VPN, por las iniciales de *Virtual Private Network*), cifrado de extremo a extremo, plataformas de mensajería efímera y mercados de la *dark web* forman parte del arsenal tecnológico que estas redes utilizan para ocultar sus operaciones y dificultar la investigación criminal.

**Tabla 3.** Especialización criminal y Crimen como Servicio (CaaS)

| Categoría                          | Descripción                                                                                                                                                 | Ejemplos                                                    | Características clave                                                      |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>División funcional interna</b>  | Especialización por tareas: programadores, diseñadores de <i>malware</i> , mulas, operadores de pagos, administradores de servidores, etc.                  | Todos los anteriores (tabla 2)                              | Modularidad; subcontratación; anonimato entre miembros                     |
| <b>Crimen como Servicio (CaaS)</b> | Modelo económico donde se comercializan servicios ilícitos listos para usar: kits de <i>malware</i> , <i>hosting</i> anónimo, herramientas de cifrado, etc. | Foros criminales; <i>marketplaces</i> de servicios ilícitos | Profesionalización; acceso para no expertos; economía criminal sofisticada |

**Fuente:** elaboración propia, con base en UNODC (2022).

En conclusión, las tipologías del cibercrimen y la ciberdelincuencia organizada son herramientas esenciales en los contextos académicos y operativos. La tipología de Wall (2007) ofrece una base estructurada para analizar el cibercrimen según su función y daño, mientras que las tipologías de la ciberdelincuencia organizada ayudan a delinear la infraestructura, motivaciones y el carácter transnacional de los grupos cibercriminales. La ciberdelincuencia organizada no es una réplica digital del crimen tradicional, sino una evolución estructural que explota las oportunidades técnicas y sociales del ciberespacio. Desde enjambres efímeros hasta mafias híbridas digitalizadas, estas organizaciones redefinen los parámetros de la criminalidad moderna. Y a medida que evolucionen las tecnologías también deben evolucionar estas tipologías, especialmente para considerar amenazas emergentes como el *ransomware* como servicio, el fraude basado en IA y los actores de amenazas híbridos que difuminan la línea entre las operaciones cibernéticas estatales y no estatales.

### Funciones en la ciberdelincuencia organizada

La ciberdelincuencia organizada es un fenómeno delictivo complejo, transnacional y dinámico, caracterizado por estructuras flexibles, alta especialización y uso estratégico de tecnologías de la información y la comunicación (TIC). A diferencia de otras formas de crimen tradicional, los grupos ciberdelincuenciales organizados operan, en la mayoría de los casos, como empresas con funciones diferenciadas, distribución de tareas, prestación de servicios y control de calidad interno. Como señala Lusthaus (2018), la ciberdelincuencia organizada opera como una “industria de la anonimidad”, donde “los actores criminales participan en un mercado interconectado donde se compran, venden y alquilan servicios ilícitos con reglas internas y reputaciones compartidas” (p. 21). Esta lógica industrial también se manifiesta en la separación de funciones dentro de las organizaciones ilegales, lo que permite la maximización de eficiencia y la reducción de riesgos operacionales.

La UNODC (2022) refuerza la idea de la ciberdelincuencia organizada como un sistema productivo de tipo empresarial, al documentar cómo estos grupos de ciberdelincuencia organizada se componen de múltiples perfiles funcionales, incluyendo codificadores, piratas informáticos, técnicos de infraestructura, encargados de pagos, especialistas en cifrado, ingenieros sociales y mulas de dinero, entre otros. Estos roles son comparables a los departamentos funcionales de una empresa, donde cada unidad cumple con una función específica dentro del ciclo delictivo. Ese diseño funcional permite no solo la sostenibilidad del grupo a largo plazo, sino la escalabilidad de sus operaciones a nivel global.

Los grupos de ciberdelincuencia organizada incluyen diversos roles operativos altamente especializados. Por ejemplo, los codificadores desarrollan *malware*, *exploits* y herramientas personalizadas para cometer delitos cibernéticos. Por su lado, los piratas informáticos (*hackers*) aprovechan vulnerabilidades en sistemas, redes o aplicaciones, ya sea para obtener acceso no autorizado, insertar código malicioso, sustraer información o mantener persistencia dentro de un sistema comprometido. Los responsables del soporte técnico son los encargados de mantener la infraestructura digital del grupo. Esto incluye servidores, VPN, plataformas cifradas de comunicación, canales seguros de intercambio de archivos y actualizaciones de herramientas técnicas. Los anfitriones proveen el entorno técnico necesario para alojar actividades ilícitas en servidores, a menudo bajo servicios de "*hosting* blindado" diseñados para eludir la detección policial y sostener operaciones prolongadas en la red oscura (UNODC, 2022).

Por otra parte, se encuentran los especialistas, o personas con habilidades técnicas excepcionales. Algunos se dedican a desarrollar cifradores, herramientas diseñadas para evitar la detección de programas antivirus. Otros pueden ser expertos en ingeniería social, por lo que se enfocan en manipular víctimas o empleados internos para obtener acceso a sistemas sensibles. Los cajeros y mulas de dinero son los encargados de convertir activos ilícitos en dinero limpio. Pueden operar tanto en el escenario físico, retirando dinero de cuentas comprometidas, como digitalmente, a través de criptomonedas y plataformas de transferencia. Finalmente se encuentran los administradores y moderadores, que operan en las plataformas criminales como los foros de *carding* o los mercados de la *dark web*. Dichos miembros establecen normas internas, filtran nuevos usuarios, organizan jerarquías y aplican sanciones, para así garantizar el orden interno y la confianza entre pares (UNODC, 2022).

La expansión de modelos de Crimen como Servicio (*Crime-as-a-Service* [CaaS]) ha propiciado una industria delictiva en la que muchas de estas funciones

pueden incluso ser subcontratadas. De acuerdo con Lavorgna (2020), los mercados digitales permiten que desarrolladores ofrezcan *ransomware*, kits de *phishing*, servidores anónimos y acceso a *botnets* como productos comercializables. Estos servicios facilitan que incluso personas sin mayores conocimientos técnicos puedan participar en campañas delictivas complejas mediante la adquisición de herramientas “listas para usar”. El “apoyo técnico” también puede ser parte de estos servicios, como ocurre en foros donde se venden tutoriales sobre cómo utilizar *malware*, enmascarar IP o crear documentos falsificados. En este contexto muchos grupos del cibercrimen no actúan como una sola organización vertical, sino como consorcios informales, donde los diversos proveedores interactúan temporalmente para ejecutar una operación específica, una estructura típica de los “enjambres” cibernéticos.

Finalmente, y más allá de funciones operativas, estos grupos cibercriminales organizados implementan medidas de control interno y anonimato altamente sofisticadas. Plataformas de la *dark web* como “Dreamboard” y “Card Planet” utilizaban sistemas de membresía controlada con verificación por parte de usuarios activos, cuotas de ingreso y votación interna para aceptar nuevos miembros. En “Card Planet”, por ejemplo, se requería hasta hace poco el pago de 5.000 dólares como garantía para acceder al foro. Estas medidas no solo limitan el acceso de infiltrados policiales, sino que también refuerzan la confianza entre actores anónimos, lo cual es decisivo en entornos sin interacción cara a cara. De hecho, no pocas plataformas adoptan políticas estrictas como la prohibición de acceso a miembros arrestados o inactivos, para así minimizar el riesgo de comprometer las operaciones globales.

En resumen, la ciberdelincuencia organizada no puede entenderse tan solo como un delito cometido con computadores, sino como un entramado funcional, técnico y social donde convergen múltiples actores especializados. En efecto, desde los desarrolladores de *malware* hasta las mulas financieras, cada función cumple un papel clave en una cadena criminal altamente eficiente. Comprender esta lógica funcional es indispensable para diseñar políticas públicas, estrategias de ciberseguridad e intervenciones policiales que respondan al carácter industrial, distribuido y anónimo del crimen organizado en el ciberespacio.

## El estado del mercado y los ingresos del cibercrimen

En 2025 la economía del cibercrimen ha alcanzado niveles sin precedentes de complejidad, madurez y rentabilidad. Es decir, ya no se compone tan solo de actores de amenazas aislados o explotadores *ad hoc*, sino que el mercado actual

del cibercrimen opera como un ecosistema adaptativo altamente estructurado, multinivel y orientado a la rentabilidad, comparable en función y escala a las economías digitales legítimas. Los actores de amenazas se involucran en la especialización, la división del trabajo, el desarrollo de marca, el reclutamiento de afiliados y la innovación competitiva, impulsados por una red global de mercados en la *dark web*, proveedores de *malware* como servicio y canales de monetización de datos (Check Point, 2025).

Como detalla el *Informe de Ciberseguridad 2025*, las campañas de *ransomware* y robo de información se han convertido en los motores económicos de un submundo digital que ahora respalda una amplia gama de servicios, incluyendo el desarrollo de *malware*, la intermediación de acceso inicial, la logística de extorsión, el lavado de dinero, e incluso, la atención al cliente para transacciones ilícitas (Check Point, 2025). Cabe destacar que los ataques de *ransomware* causaron pérdidas por 872 millones de dólares solo a UnitedHealth y Change Healthcare durante el primer trimestre de 2024, lo que ilustra la capacidad de una sola campaña para infligir daños a nivel estratégico. Asimismo, la mercantilización del *software* malicioso, en particular a través de modelos de *ransomware* como servicio (RaaS) y *malware* como servicio (MaaS), ha reducido la barrera técnica de entrada. Los afiliados licencian kits de herramientas como “RedLine Stealer” por entre 150 y 200 dólares al mes y pueden esperar monetizar los registros a aproximadamente 10 dólares por víctima (Check Point, 2025, p. 21). Este modelo refleja una economía de franquicia, donde los desarrolladores se centran en la infraestructura y el soporte, mientras que las filiales ejecutan las operaciones de forma independiente. El resultado es un mercado criminal ágil, descentralizado y difícil de dismantelar.

Los *infostealers* han eclipsado a las *botnets* y troyanos tradicionales como el método más eficaz para el acceso inicial y la vulneración de la identidad. Su popularidad se debe a su bajo coste, facilidad de uso y alto rendimiento. Herramientas como Lumma, RedLine y StealC permiten a los ciberdelincuentes recopilar credenciales, *cookies* de navegador y *tokens* de sesión, que luego se revenden o se utilizan directamente para infiltrarse en entornos corporativos (Check Point, 2025). La economía de los *infostealers* es robusta, con más de 10 millones de registros a la venta en plataformas como Russian Market, algunos de los cuales se dirigen a cuentas de alto valor, como Microsoft 365, VPN y sistemas financieros. De hecho, un análisis de 2024 reveló que el 90 % de las organizaciones vulneradas por *ransomware* ya habían sufrido filtraciones de credenciales en registros de robo de información, lo que subraya el papel decisivo que estas herramientas desempeñan

en la cadena de suministro delictiva (Check Point, 2025, p. 22). La demanda de registros ha incentivado la innovación en los mecanismos de distribución (*phishing*, *malvertising* y repositorios de *software* falsos), así como la automatización de clasificación y transmisión de registros a plataformas como Telegram.

Por consiguiente, el *ransomware* sigue dominando el panorama de ingresos de la ciberdelincuencia. Si bien las operaciones de las fuerzas del orden en 2024 afectaron a actores clave como "LockBit" y "ALPHV", el número total de ataques de *ransomware* ha aumentado, con la incorporación de nuevos actores como "RansomHub", "Play" y "Akira" (Check Point, 2025). Las operaciones de *ransomware* priorizan cada vez más la extorsión por exfiltración de datos (DXF) sobre el cifrado, adoptando un modelo de negocio que minimiza el riesgo técnico y maximiza la presión psicológica. Es necesario señalar que este modelo DXF es particularmente rentable: los datos robados a las organizaciones se subastan en sitios de filtración de datos (DLS) de la *dark web*, o se extorsiona a las víctimas para que paguen, y así evitar la publicación de archivos confidenciales. Grupos como "Bashe" (Eraleign) operan ahora exclusivamente como plataformas de venta de datos evitando por completo el cifrado y diversificando aún más las fuentes de ingresos disponibles para los ciberdelincuentes (Check Point, 2025).

Este cambio también facilita el reciclaje y la atribución falsa de datos, donde los atacantes presentan filtraciones antiguas como nuevos ataques para obtener múltiples rescates. Como resultado, la atribución, la respuesta a incidentes y la adjudicación de seguros cibernéticos se vuelven más complejas y propensas a errores. Además, el ecosistema actual del cibercrimen se asemeja a un sector industrial multicapa. En la cima se encuentran las APT de élite y los desarrolladores de *malware*, mientras que por debajo se encuentran los proveedores de infraestructura que ofrecen alojamiento anónimo, paneles C2 y soporte para afiliados. Los actores de nivel medio incluyen operadores de robo de información, vendedores de kits de *phishing* y agentes de acceso inicial (IAB) que monetizan las vulnerabilidades del sistema y revenden credenciales. Finalmente, los actores de nivel inferior incluyen compradores de registros, ladrones de identidad y estafadores que compran acceso o datos para aplicaciones delictivas especializadas (Check Point, 2025, p. 23). Esa estructura refleja la especialización funcional: en efecto, de modo similar a como las industrias legítimas hacen uso de las plataformas en la nube, procesadores de pagos y proveedores de análisis, los ciberdelincuentes también externalizan el alojamiento, el cifrado y la ofuscación de *exploits* a proveedores de servicios. El resultado es una economía delictiva cada vez más resiliente y con una escalabilidad horizontal.

El mercado del cibercrimen tiene asimismo un alcance profundamente global, pero está controlado de forma asimétrica. Si bien América del Norte y Europa soportan la mayor parte de las pérdidas financieras y el número de víctimas, una gran proporción de la infraestructura, los actores y los registros robados provienen de regiones en desarrollo con mecanismos de control deficientes. Según Check Point (2025), más del 55 % de los registros de robo de información vendidos en mercados clandestinos provienen de países como la India, Brasil, Egipto e Indonesia, donde la adopción de internet es alta y la protección de los *endpoints* es baja. Esta asimetría fomenta un entorno de bajo riesgo y alta recompensa para los perpetradores. El uso de criptomonedas, alojamiento web seguro y redes de anonimización dificulta aún más la aplicación de la ley. Incluso cuando se desmantelan los principales grupos de RaaS, la resiliencia del ecosistema en su conjunto (mediante la reutilización de código, la migración de afiliados y la infraestructura descentralizada) garantiza la continuidad de las operaciones (Check Point, 2025).

Finalmente, si bien las valoraciones precisas del mercado son difíciles, debido a la naturaleza clandestina del cibercrimen, las estimaciones del sector sugieren que los ingresos por ciberdelincuencia a nivel mundial superan los 10 billones de dólares anuales, de los que el *ransomware* y el robo de credenciales representan una parte significativa. Por ejemplo, tan solo la filtración de datos de Change Healthcare en 2024 generó un impacto financiero de casi 900 millones de dólares y pagos de rescates por un total de más de 20 millones de dólares (Check Point, 2025). Estas cifras sugieren que la escala económica de la ciberdelincuencia rivaliza con la de las principales industrias globales, como la energética, la farmacéutica y la del entretenimiento. A medida que los actores de amenazas se profesionalizan, la ciberdelincuencia se conceptualiza cada vez más no solo como un problema de seguridad, sino también como una amenaza estratégica, económica y geopolítica. El Grupo "Lazarus" de Corea del Norte ejemplifica este tipo de convergencia, al realizar robos de criptomonedas para financiar objetivos estatales, mientras que grupos chinos e iraníes combinan la ciberdelincuencia con el espionaje, la guerra híbrida y el sabotaje industrial.

## La *dark web* como ecosistema criminal

Internet es una extensa red global de computadores y dispositivos interconectados que permite a los usuarios acceder a información de la World Wide Web. La World Wide Web es un sistema de información que interconecta documentos mediante

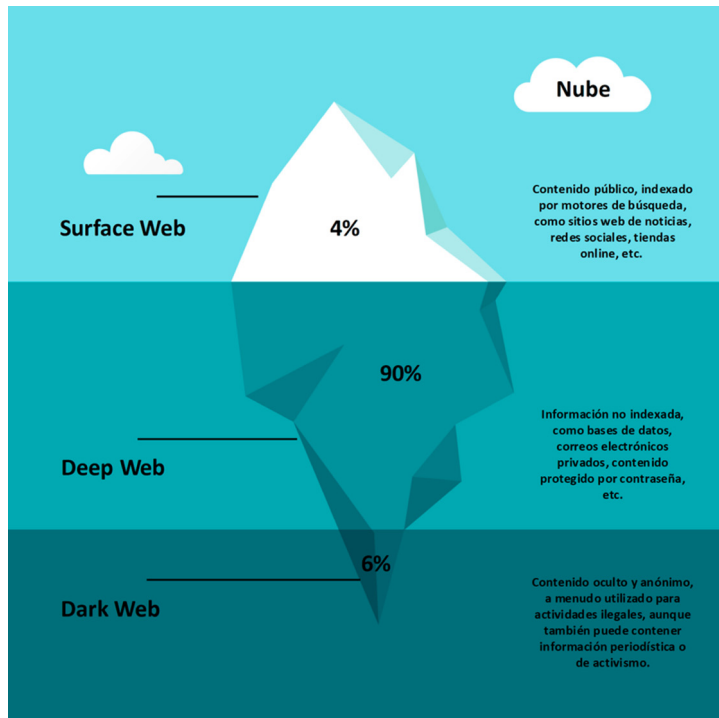
enlaces de hipertexto, lo que permite a los usuarios navegar sin problemas de un documento a otro (Gehl, 2018). Motores de búsqueda destacados, como Google, Yahoo y Bing, utilizan estos enlaces para catalogar diversos documentos, lo que facilita la exploración y la búsqueda de información (East, 2017).

Internet comprende múltiples niveles de accesibilidad. La web superficial, o *surface web*, comprende todos los sitios web de fácil acceso al público, ya que están indexados por los principales motores de búsqueda. Sin embargo, ciertos sitios web permanecen inaccesibles al público, ya que no se encuentran indexados por los principales motores de búsqueda. Dicho estrato de Internet se denomina *deep web* (Symanovich, 2019). Para acceder a estos sitios de la web profunda se debe introducir directamente la URL en un navegador web como Chrome, Internet Explorer o Safari. Otros sitios de la web profunda son inaccesibles al público general debido a la protección con contraseña o cifrado. Este nivel de la web profunda alberga contenido inaccesible para los motores de búsqueda (Symanovich, 2019).

La banca en línea de la actualidad ejemplifica tanto la web abierta como la web profunda. Una persona puede utilizar cualquier motor de búsqueda popular para localizar la página de inicio de banca en línea de su banco preferido. El sistema de banca en línea está protegido por una contraseña, que requiere que los usuarios inicien sesión para acceder a sus cuentas personales. Si bien las páginas de inicio pueden ser indexadas por múltiples motores de búsqueda y son accesibles en la web de superficie, el contenido específico de las cuentas bancarias permanece oculto al público (por ejemplo, la web profunda). Por consiguiente, se estima que la web profunda constituye la mayor parte de internet (Gehl, 2018).

Un computador se reconoce por su dirección de Protocolo de Internet (IP), lo que facilita la comunicación dentro de la red. Esta dirección IP funciona de forma análoga a una dirección residencial en su capacidad para identificar y localizar un dispositivo o computador que accede a internet. Las direcciones IP asocian el historial de navegación a la identidad del usuario (Gehl, 2018). Para mantener el anonimato en línea, los usuarios pueden instalar *software* criptográfico especializado que oculta su ubicación, lo que les permite acceder a internet y a la World Wide Web sin revelar la dirección física del computador y preservando la confidencialidad de su historial de navegación (figura 1). El *software* criptográfico más común es Tor, una aplicación de código abierto que permite a los usuarios acceder a internet a través de una red de servidores virtuales sin establecer una conexión directa (East, 2017).

**Figura 1.** Los niveles de la World Wide Web



**Fuente:** elaboración propia.

La *dark web* se refiere a un segmento de internet que no está indexado por los motores de búsqueda convencionales y al que solo se puede acceder mediante *software* de anonimización, tales como Tor, I2P o Freenet. Dichos sistemas permiten a los usuarios ocultar su identidad, cifrar las comunicaciones y alojar servicios ocultos sin revelar su ubicación física ni sus identificadores de red. Si bien gran parte del discurso público describe a la *dark web* como un submundo distópico repleto de delincuencia, también sirve a usuarios legítimos, como disidentes políticos, denunciantes y periodistas que operan bajo regímenes autoritarios (Gehl, 2018; Nearchou, 2023). Sin embargo, su arquitectura es inherentemente propicia para las transacciones ilícitas, la coordinación de ciberdelinquentes y operaciones clandestinas que son muy difíciles de interceptar para las fuerzas del orden (Ozkaya e Islam, 2019; Akhgar et al., 2021).

El ecosistema de la *dark web* se basa en infraestructuras técnicas que priorizan el cifrado, la descentralización y la ofuscación de identidad. Tor, la más conocida de estas tecnologías, enruta los datos de los usuarios a través de múltiples

capas de “cebolla”, lo que hace casi imposible rastrear el origen o el destino del tráfico si no se cuenta con herramientas avanzadas de desanonimización (Liggett et al., 2020). Tor permite no solo la navegación anónima, sino también el alojamiento de servicios ocultos, a los que solo pueden acceder los usuarios que utilizan el mismo *software* de anonimización.

Los usuarios de la *dark web* también utilizan las criptomonedas (Bitcoin, Monero y Ethereum), para el anonimato transaccional. Por ende, las criptomonedas son clave para mantener el seudonimato en los ecosistemas criminales, respecto a lo que actúan como el principal medio de intercambio de bienes y servicios que abarcan desde narcóticos y armas de fuego hasta *malware* y tráfico de personas (Nearchou, 2023; Akhgar et al., 2021). Como resultado, estos activos digitales cumplen propósitos tanto funcionales como simbólicos dentro de la economía subterránea: permiten pagos irrastreables y refuerzan el espíritu libertario de las subculturas digitales anti-vigilancia (Gehl, 2018).

Como ya se ha mencionado, una de las características que definen a la *dark web* es la presencia de redes cibercriminales organizadas que imitan las jerarquías corporativas y adoptan los modelos operativos similares a los de las empresas legítimas, por lo que estos grupos no son simplemente colectivos coordinados de forma flexible, sino, por el contrario, entidades estructuradas con roles y especializaciones definidos. Nearchou (2023) destaca que los actores organizados en la red oscura mantienen la continuidad operativa adaptándose a las presiones legales y la volatilidad del mercado: por ejemplo, cuando las fuerzas del orden cierran un mercado (como “Silk Road” o “AlphaBay”), sus usuarios y proveedores suelen migrar a otro, a menudo con mayor seguridad operativa. Por lo tanto, esta evolución cíclica de los mercados es emblemática de un ecosistema criminal resiliente y adaptable.

## Mercados y servicios ilícitos en la dark web

La *dark web* alberga una variedad de mercados ilícitos donde se comercializan abiertamente diversas formas de contrabando y servicios delictivos, por lo que, en cierto sentido, estos mercados suelen parecerse a las plataformas de comercio electrónico convencionales, con categorías de productos, reseñas de clientes, calificaciones de proveedores y servicios de depósito en garantía (Liggett et al., 2021).

El tráfico de drogas es, quizá, el componente más investigado y económicamente significativo del comercio delictivo en la *dark web*. Si bien plataformas tempranas como “Silk Road” fueron pioneras en este ámbito, los mercados más nuevos han adoptado protocolos logísticos y de cifrado más sofisticados. Las

investigaciones estiman que los mercados oscuros de drogas generan cientos de millones de dólares al año, con vendedores que ofrecen una amplia gama de narcóticos, desde opioides y estimulantes hasta medicamentos recetados falsificados (Liggett et al., 2020; Nearchou, 2023). Eso sí, lo que distingue a dichas plataformas es su impersonalidad y eficiencia, ya que los vendedores y compradores nunca se encuentran físicamente, las comunicaciones están cifradas y las transacciones se realizan a través de las cuentas de depósito en garantía. Además, las calificaciones de proveedores, las descripciones detalladas de los productos y la confiabilidad del envío se muestran de forma destacada, lo que cultiva una apariencia de confianza y profesionalismo que desmiente la naturaleza criminal del intercambio (Akhgar et al., 2021).

Aunque no es tan frecuente como el tráfico de drogas, la venta de armas de fuego, municiones y explosivos ocupa un lugar destacado en ciertos mercados de la red oscura. Los vendedores ofrecen armas pequeñas, rifles modificados y, ocasionalmente, incluso explosivos, a menudo procedentes de zonas de conflicto o de arsenales militares (Akhgar et al., 2021). Debido al alto riesgo y a los desafíos logísticos, estas transacciones suelen limitarse a corredores regionales específicos, especialmente en Europa y Norteamérica.

El comercio de armas de fuego a menudo requiere coordinación logística fuera de línea, por lo que los vendedores pueden utilizar métodos de entrega en punto muerto o intermediarios de envío redirigidos. Akhgar et al. (2021) señalan que en varios casos documentados los traficantes de armas de la red oscura han estado estrechamente vinculados con redes paramilitares o del crimen organizado fuera de línea, aprovechando el anonimato de la red oscura para facilitar el tráfico sin exposición en la calle.

Por su parte, el fraude es un pilar de las economías criminales de la red oscura. Los mercados especializados ofrecen amplios catálogos de datos robados, incluyendo números de tarjetas de crédito, credenciales bancarias, credenciales de PayPal, números de la Seguridad Social y kits de identidad completos (Ozkaya & Islam, 2019). Estas plataformas centradas en el fraude, a menudo denominadas "foros de *carding*", sirven como sitios de comercio y espacios de formación donde los usuarios intercambian tutoriales, *software* y asesoramiento operativo (Holt & Bossler, 2020). Akhgar et al. (2021) detallan la existencia de servicios delictivos como la construcción de identidades sintéticas, el *phishing* como servicio y las soluciones integrales (comúnmente conocidas como FULZ), que permiten a los actores cometer fraudes bancarios, solicitar préstamos o llevar a cabo esquemas de

fraude fiscal con escasos conocimientos técnicos. Estos ecosistemas de fraude suelen asociarse a redes de mulas de dinero y servicios de blanqueo de capitales, para completar así una cadena de valor delictiva completa.

El desarrollo, la venta y la implementación de *software* malicioso (*malware*) es una característica destacada de la infraestructura delictiva de la *dark web*. Los proveedores ofrecen kits de explotación personalizados, paquetes de *ransomware*, *rootkits* y troyanos de acceso remoto (en inglés, RAT, por las iniciales de *Remote Access Trojan*), a menudo con precios diferenciados según la sofisticación y los servicios de soporte ofrecidos (Liggett et al., 2020; Ozkaya & Islam, 2019). Una innovación significativa ha sido la aparición del *ransomware* como servicio (RaaS). En este modelo los autores de *malware* ceden el acceso a sus herramientas a cambio de una participación en las ganancias o una comisión, lo que democratiza el acceso a ciberarmas destructivas. Ozkaya e Islam (2019) señalan que los programas de afiliados permiten a los actores novatos distribuir *ransomware* entre objetivos seleccionados con un mínimo esfuerzo, a menudo con el soporte de *backend* de los desarrolladores originales. Además, los *exploits* de día cero (vulnerabilidades desconocidas para los proveedores de *software*), también se comercializan en los mercados de la *darknet*, especialmente en foros privados, a los que solo se puede acceder con invitación. Estas herramientas son especialmente valiosas para los actores de los Estados nación y los grupos de amenazas persistentes avanzadas (en inglés, APT, por las iniciales de *Advanced Persistent Threat*), al difuminar la línea entre el crimen organizado y el ciberespionaje (Akhgar et al., 2021).

Entre los dominios más inquietantes de la *dark web* se encuentran foros y repositorios dedicados a la distribución y el consumo de material de abuso sexual infantil (MASI). Estas plataformas operan bajo rigurosos procesos de verificación, que a menudo exigen a los usuarios subir material nuevo o participar en actividades de captación de menores como requisito previo para acceder (Liggett et al., 2020; Nearchou, 2023). Gehl (2018) explora cómo estas comunidades justifican su comportamiento mediante una economía moral subcultural utilizando el cifrado y el anonimato para proteger a sus miembros, a la vez que imponen las normas comunitarias. Asimismo, la persistencia de dichos espacios, a pesar de los múltiples desmantelamientos policiales, demuestra tanto la resiliencia como la depravación de ciertos rincones de la *dark web*. Akhgar et al. (2021) destacan que el abuso sexual infantil a menudo está vinculado a redes más amplias de trata de niños y abusos fuera de línea, lo que representa una amenaza transnacional profundamente arraigada.

## Gobernanza, reputación y confianza en el mercado

A pesar de ser espacios sin ley, los mercados de la *dark web* no carecen de orden. Se basan en mecanismos informales de gobernanza para generar confianza y garantizar la fiabilidad de las transacciones. Gehl (2018) describe esos sistemas como "capitalismo de plataforma desde abajo", con mecanismos como la puntuación de retroalimentación de los proveedores, la resolución pública de disputas y el acceso basado en la reputación.

Los foros suelen emplear moderadores y administradores que examinan a los nuevos usuarios, resuelven conflictos y hacen cumplir las normas. Estas prácticas reflejan los primeros ideales anarco-libertarios que buscaban construir órdenes sociales alternativos basados en la autorregulación en vez de la autoridad estatal (Gehl, 2018; Owen y Marshall, 2021). Algunos mercados también emplean servicios de depósito en garantía, donde los fondos son retenidos por agentes externos hasta que el comprador confirme su satisfacción. La introducción de monederos de criptomonedas multi-firma, que requieren múltiples claves para realizar pagos, ha reforzado la confianza en las interacciones entre vendedores y compradores (Ozkaya & Islam, 2019).

Más allá del comercio, la *dark web* también termina sirviendo como plataforma para el extremismo ideológico y el ciberterrorismo. Grupos extremistas explotan los foros de la red oscura para radicalizar a reclutas, distribuir propaganda y coordinar operaciones clandestinas (Liggett et al., 2020). Materiales como manuales para la fabricación de bombas, manifiestos yihadistas y guías para ataques de lobos solitarios se encuentran con frecuencia en archivos cifrados (Hannigan, 2021). Owen (2021) señala que el ciberterrorismo debe entenderse no solo como un ataque técnico a la infraestructura, sino también como un "acto simbólico" de violencia digital, y argumenta que el ciberterrorismo a menudo opera en el registro afectivo e ideológico con el objetivo primordial de intimidar, desestabilizar y ganar visibilidad en conflictos asimétricos. Cabe destacar que grupos como ISIS y Al-Qaeda han mantenido canales de comunicación cifrados en foros de la *dark web* para su reclutamiento y financiación. El anonimato en este espacio permite a dichos actores evitar la vigilancia, y mantener al mismo tiempo redes ideológicas a nivel global (Akhgar et al., 2021).

Como ya se ha señalado, las criptomonedas constituyen la columna vertebral financiera de la economía criminal de la *dark web*. Su naturaleza descentralizada y su seudonimia permiten transacciones entre pares que eluden los sistemas bancarios tradicionales y la supervisión gubernamental. Si bien Bitcoin sigue siendo la

divisa más reconocida de esta clase, las criptomonedas orientadas a la privacidad, como Monero, Zcash y Dash, son cada vez más preferidas por los delincuentes, debido a sus funciones de ofuscación mejoradas (Ozkaya & Islam, 2019). Gehl (2018) describe las criptomonedas como una forma de “confianza tecnológica”, que permite el comercio en entornos donde no existen mecanismos de aplicación legal. Asimismo, Akhgar et al. (2021) explican que los vendedores de la *dark web* suelen fijar el precio de sus productos en Bitcoin, pero ofrecen descuentos por transacciones en Monero, lo que refleja una tendencia hacia un mayor anonimato.

Los flujos de pago en los mercados oscuros suelen incluir servicios de depósito en garantía, contratos con límite de tiempo y mezcladores/*tumblers*, servicios que combinan múltiples transacciones de criptomonedas para ocultar el origen y el destino. Estos instrumentos, en conjunto, complican las investigaciones forenses dificultando a las fuerzas del orden rastrear las pistas financieras. Además, la integración de cajeros automáticos de criptomonedas, tarjetas de regalo prepagadas y redes de mulas de dinero permite blanquear activos digitales para convertirlos en moneda fiduciaria, y cerrar así el ciclo financiero ilícito. Según Liggett et. al (2020), esta integración refleja la maduración de las finanzas empresariales delictivas, comparable en su sofisticación al comercio global legítimo.

A pesar de las innovaciones estructurales y los mecanismos de confianza, los mercados de la *dark web* siguen siendo volátiles y vulnerables a la traición. Un riesgo importante es la estafa de salida, en la que los administradores del mercado desaparecen repentinamente con los fondos en custodia de los usuarios, que a veces ascienden a millones en criptomonedas (Akhgar et al., 2021). Por ejemplo, Evolution Market, una de las plataformas más exitosas de la *dark web*, desapareció repentinamente en 2015, supuestamente robando más de 12 millones de dólares en Bitcoin. Estas traiciones erosionan la confianza de los usuarios, pero, paradójicamente, no logran disuadir por completo la participación delictiva. Los usuarios suelen migrar a plataformas más nuevas con funciones mejoradas o una gobernanza comunitaria (Gehl, 2018).

La volatilidad del mercado también se ve agravada por las redadas policiales, el hackeo por parte de grupos rivales o las disputas internas. Estas disrupciones han dado lugar a un fenómeno de “salto de mercado”, en el que los proveedores conservan su reputación exportándola a nuevas plataformas, a veces verificadas mediante pruebas criptográficas (Ozkaya & Islam, 2019). Esta resiliencia refuerza la conceptualización de la *dark web* como un ecosistema criminal. No es solo un mercado, sino uno que se adapta, muta y se regenera tras crisis sistémicas.

Combatir la ciberdelincuencia organizada en la *dark web* plantea graves desafíos jurisdiccionales y tecnológicos. La arquitectura anónima de las plataformas,

la distribución global de servidores y el uso de comunicaciones cifradas crean barreras a la vigilancia policial tradicional. No obstante, los organismos internacionales encargados de hacer cumplir la ley han desarrollado nuevas estrategias. Operaciones conjuntas como la Operación Disruptor, la Operación Bayoneta y la Operación Onymous han logrado dismantelar importantes mercados como AlphaBay, Hansa y Silk Road (Liggett et al., 2020). Estas operaciones suelen basarse en la ciberinfiltración, *honeypots*, la implantación de *malware* y técnicas de análisis de *blockchain*.

Akhgar et al. (2021) argumentan que el intercambio colaborativo de inteligencia entre las unidades cibernéticas (Interpol, Europol, el FBI y los CERT nacionales como ColCERT) ha resultado vital. Sin embargo, advierten que la aplicación de la ley por sí sola no puede dismantelar el ecosistema. La descentralización de la *dark web*, las redes de confianza comunitaria y la innovación continua requieren respuestas multisectoriales, que incluyen la regulación de criptomonedas, colaboración con empresas de ciberseguridad e inversión en capacidades forenses digitales. Además, académicos como Owen (2021) abogan por una reevaluación criminológica de la ciberdelincuencia: en efecto, Owen (2021) sugiere que herramientas conceptuales como su "Marco Genético-Social" pueden ayudar a las fuerzas del orden a comprender mejor los perfiles, las motivaciones y los patrones de comportamiento de los delincuentes en contextos digitales.

## La *dark web* como un ecosistema criminal complejo

La *dark web* no es simplemente una capa oculta de internet: es un ecosistema criminal complejo y en constante evolución que fusiona tecnología, comercio, ideología y desviación. Su estructura alberga grupos delincuenciales organizados interconectados, posibilita nuevas formas de comportamiento en el mercado y ofrece protección a actores que operan más allá de la supervisión estatal tradicional. Pero al mismo tiempo, la *dark web* revela paradojas, al ser un espacio que combina orden y volatilidad, confianza y traición, invisibilidad y vigilancia. Sus redes criminales reflejan y desafían los modelos convencionales del crimen organizado, y exigen, en consecuencia, nuevas herramientas teóricas y prácticas para el análisis y la intervención.

El concepto de "ecosistema criminal" no se utiliza como una metáfora descriptiva, sino como una categoría analítica anclada en la teoría de los sistemas complejos adaptativos. Desde esa perspectiva, la arquitectura ilícita del ciberespacio (y en particular, los entornos asociados a la *dark web*) puede entenderse como un sistema dinámico compuesto por múltiples agentes heterogéneos (actores criminales, intermediarios, plataformas, protocolos, infraestructuras técnicas

y usuarios), cuyas interacciones no lineales producen patrones emergentes de orden, adaptación y resiliencia.

De acuerdo con Thurner et al. (2018), los sistemas complejos se caracterizan por la ausencia de control centralizado, la interacción local entre agentes, la no linealidad de los procesos y la emergencia de propiedades globales que no pueden reducirse a la suma de sus componentes individuales. Aplicado al estudio del cibercrimen, este enfoque permite superar las aproximaciones tradicionales que conciben la criminalidad digital como una agregación de delitos aislados o como redes jerárquicas relativamente estables. En contraste, la *dark web* opera como un sistema abierto, evolutivo y autorregulado, en el que la innovación criminal, la especialización funcional, la cooperación táctica y la competencia interna emergen mediante procesos de aprendizaje distribuido y adaptación continua frente a presiones externas como la acción estatal, la regulación jurídica o la disrupción tecnológica. Tal como señalan Thurner et al. (2018), en los sistemas complejos adaptativos la estabilidad no implica equilibrio, sino capacidad de reorganización frente al cambio, una lógica que resulta en particular pertinente a comprender la persistencia del crimen digital.

Bajo este marco analítico, ni los mercados ilícitos digitales, ni los foros clandestinos, ni los servicios criminales *as-a-service* ni las infraestructuras técnicas que los sostienen constituyen entidades independientes, sino, más bien, nodos interconectados de un ecosistema criminal digital. Su estabilidad relativa no depende de la permanencia de actores específicos, sino de la capacidad del sistema para recombinar funciones, reemplazar nodos y reorganizar flujos de valor ilícito cuando se producen choques o intervenciones externas. En este sentido, la *dark web* se comporta como un entorno adaptativo complejo, donde la persistencia del crimen digital se explica menos por la fortaleza individual de sus actores, y más, por la lógica sistémica de autoorganización que estructura el conjunto.

Este enfoque permite comprender por qué las estrategias de represión centradas exclusivamente en la eliminación de plataformas, mercados o individuos tienden a generar efectos limitados o contraproducentes, pues al operar sobre nodos visibles sin alterar las dinámicas sistémicas subyacentes, el ecosistema criminal tiende a reconfigurarse, fragmentarse y reaparecer bajo nuevas formas funcionales. Por consiguiente, comprender la *dark web* desde la perspectiva de un "ecosistema criminal" ofrece un marco integral para interpretar su complejidad, resiliencia y potencial de amenaza en constante evolución.

El concepto de "ecosistema criminal", propuesto por Álvarez y Rodríguez (2018), se basa en la ecología funcional y la teoría general de sistemas para caracterizar los fenómenos criminales no como comportamientos aislados, sino como

sistemas en red de una variedad de actores, recursos y entornos interdependientes que sustentan la globalización desviada y erosionan la soberanía estatal (Álvarez & Zambrano, 2017). La *dark web* ejemplifica esta lógica de criminalidad ecosistémica en formato digital. Funciona como un hábitat donde actores ilegales como *hackers*, vendedores, terroristas y blanqueadores interactúan dentro de un territorio tecnológico (Tor, servicios ocultos, protocolos de criptomonedas), el cual sirve tanto de entorno físico como de infraestructura facilitadora. Y al igual que la descripción que hacen Álvarez y Rodríguez (2018) de los ecosistemas criminales territoriales en Colombia, la *dark web* alberga una constelación estructurada de nodos de actividad ilegal (mercados, foros, servicios), y de flujos de capital, *malware*, información y contenido ideológico.

De acuerdo con Álvarez y Rodríguez (2018), los ecosistemas se definen por sus ciclos de retroalimentación, la entrada de recursos y la interdependencia entre actores. Pues bien, en la *dark web* existen ciclos de retroalimentación positivos cuando las estafas exitosas financian un mayor desarrollo de *malware*, lo que, a su vez, aumenta la capacidad de ataque y las ganancias económicas. De igual manera, las rutas de flujo vinculan a los desarrolladores, los distribuidores y los consumidores de herramientas y servicios ilícitos formando una cadena de suministro descentralizada, pero funcionalmente integrada. Estos procesos reflejan la observación, hecha por Álvarez (2017), de que “los ecosistemas criminales generalmente prosperan gracias a las interacciones adaptativas entre los organismos criminales y las oportunidades del entorno” (p. 310).

Así como Álvarez y Rodríguez (2018) identifican a las “regiones portal” y a los “espacios vacíos” como características geográficas clave de los ecosistemas criminales físicos —es decir, las áreas donde la presencia estatal es débil o inexistente (Álvarez, 2017)—, la *dark web* también prospera en los vacíos jurisdiccionales y los puntos ciegos tecnológicos resistiendo la regulación estatal y trascendiendo las fronteras nacionales. Su arquitectura, basada en el anonimato, el cifrado y la infraestructura descentralizada, se asemeja a los factores ambientales que se hallan en ecosistemas físicos con control estatal limitado, como regiones fronterizas remotas o barrios marginales urbanos.

Además, de conformidad con lo señalado por Álvarez y Rodríguez (2018), los ecosistemas criminales se caracterizan por nodos de convergencia, donde se intersecan diferentes economías ilegales. La *dark web* es, precisamente, uno de esos nodos: un metaespacio donde convergen y coevolucionan la comercialización de narcóticos, el fraude cibernético, el terrorismo, la explotación infantil y el tráfico ilícito de armas. Estas formas de convergencia incrementan la complejidad y resiliencia del sistema, y dificultan a las autoridades dismantelar redes enteras

sin fragmentarlas en subredes más ágiles, un fenómeno similar a la descripción de Álvarez y Rodríguez (2018) de las "redes en malla", en las que los actores criminales interactúan de forma policéntrica sin estructuras de mando jerárquicas.

El análisis del cibercrimen (y en particular, el de los ecosistemas ilícitos que operan en la *dark web*) plantea desafíos metodológicos que desbordan los marcos tradicionales de estudio del crimen organizado. Los modelos clásicos, desarrollados principalmente para comprender organizaciones criminales territoriales, jerárquicas y relativamente estables (mafias, carteles, estructuras insurgentes), tienden a privilegiar categorías como liderazgo, cadena de mando, control territorial y economías ilegales delimitadas. Si bien estas aproximaciones han demostrado utilidad en los contextos físicos y estatales, resultan insuficientes para capturar la dinámica fluida, distribuida y transnacional del crimen digital contemporáneo.

Desde la perspectiva de la inteligencia y la defensa, el enfoque de sistemas complejos adaptativos ofrece ventajas analíticas decisivas. En primer lugar, permite comprender el cibercrimen no como un conjunto de actores discretos, sino como un sistema dinámico de interacciones no lineales, en el que múltiples agentes heterogéneos (humanos y tecnológicos) coevolucionan en función de incentivos, oportunidades y presiones externas. Este enfoque desplaza la atención desde las figuras visibles del delito hacia las condiciones sistémicas que posibilitan su reproducción y resiliencia.

En segundo lugar, los sistemas complejos adaptativos permiten explicar por qué muchas intervenciones represivas tradicionales (centradas en la captura de líderes, el cierre de plataformas o la eliminación de mercados específicos) generan efectos limitados o, incluso, contraproducentes. Al operar sobre nodos particulares sin alterar las dinámicas estructurales del sistema complejo, dichas intervenciones suelen provocar procesos de reorganización, fragmentación y adaptación, mediante los cuales el ecosistema criminal se reconfigura y persiste. Para la inteligencia estratégica ello implica que la disrupción efectiva del cibercrimen requiere identificar puntos de fragilidad sistémica, flujos críticos y mecanismos de retroalimentación, más que concentrarse exclusivamente en objetivos individuales.

En tercer lugar, este enfoque resulta en especial pertinente a la defensa en entornos de conflicto híbrido y guerra cognitiva, donde el cibercrimen, el espionaje, la desinformación y las operaciones encubiertas tienden a entrelazarse. Al concebir la *dark web* como un ecosistema adaptativo, se vuelve posible analizar cómo actores estatales y no estatales explotan infraestructuras criminales preexistentes, externalizan capacidades ilícitas o utilizan economías ilegales digitales como instrumentos indirectos de presión estratégica.

Finalmente, la adopción de una perspectiva de sistemas complejos favorece una lógica anticipatoria, central para la inteligencia moderna. En vez de limitarse a la atribución retrospectiva de incidentes, este enfoque permite detectar patrones emergentes, señales débiles y trayectorias de evolución criminal, y contribuye así al diseño de estrategias de prevención, disuasión y resiliencia institucional. En este sentido, el enfoque ecosistémico no solo amplía la comprensión académica del cibercrimen, sino que proporciona un marco metodológico más adecuado para la toma de decisiones en seguridad y defensa en el siglo XXI.

Una vez establecida la pertinencia del enfoque de sistemas complejos adaptativos para el análisis del cibercrimen, resulta posible (y metodológicamente necesario) traducir el concepto de ecosistema criminal a una lógica operativa que permita su utilización por parte de analistas de inteligencia, planificadores estratégicos y tomadores de decisión en seguridad y defensa. En este sentido, el valor del enfoque ecosistémico no reside únicamente en su capacidad explicativa, sino en su potencial para identificar regularidades funcionales, dependencias sistémicas y puntos de intervención estratégica dentro de sistemas criminales que operan sin control centralizado y bajo condiciones permanentes de adaptación.

Con base en lo anterior y a fin de operacionalizar este enfoque, el ecosistema criminal digital asociado a la *dark web* puede representarse de manera sintética a partir de tres dimensiones interdependientes: actores, flujos y tecnologías. Esta representación no pretende reducir la complejidad del fenómeno, sino ofrecer una cartografía funcional mínima que permita comprender cómo se organiza, se reproduce y se adapta el crimen digital en ausencia de jerarquías estables (tabla 4).

**Tabla 4.** Esquema operativo del ecosistema criminal de la *dark web*<sup>3</sup>

| Dimensión      | Componentes principales                                                                                                                                                                                                                                      | Función sistémica dentro del ecosistema criminal                                                                                                                                                                   |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Actores</b> | Desarrolladores de <i>malware</i> y <i>exploits</i> ; operadores de mercados ilícitos; proveedores de servicios <i>crime-as-a-service</i> ; intermediarios financieros y lavadores digitales; usuarios finales; actores híbridos (estatales y paraestatales) | Ejecutan funciones especializadas dentro de una red policéntrica. Los roles no están fijados jerárquicamente, sino que se asignan dinámicamente según reputación, capacidades técnicas y oportunidades del entorno |

Continúa en la otra página

<sup>3</sup> El ecosistema criminal no depende de la permanencia de nodos individuales, sino de la interacción sostenida entre estas tres dimensiones. Por ello, la disrupción aislada de actores o plataformas específicas tiende a ser absorbida mediante procesos de reorganización sistémica.

| Dimensión   | Componentes principales                                                                                                                                                                                    | Función sistémica dentro del ecosistema criminal                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Flujos      | Capital financiero ilícito (criptomonedas); datos robados; <i>malware</i> y <i>exploits</i> ; servicios criminales; contenidos ideológicos y narrativas                                                    | Conectan a los actores mediante rutas múltiples y redundantes. Permiten la adaptación del sistema, su resiliencia frente a disrupciones y la recombinación funcional tras intervenciones externas |
| Tecnologías | Redes de anonimización (Tor, I2P); servicios ocultos y <i>bulletproof hosting</i> ; criptomonedas, mezcladores y <i>privacy coins</i> ; plataformas de mensajería cifrada; infraestructura descentralizada | Constituyen el entorno habilitador del ecosistema criminal. Reducen la trazabilidad, amplían los márgenes de impunidad y configuran tanto oportunidades como vulnerabilidades estructurales       |

Fuente: elaboración propia.

Una vez operacionalizado el ecosistema criminal de la *dark web* en términos de actores, flujos y tecnologías, el siguiente paso analítico consiste en dotar a este esquema de una lógica anticipatoria que permita no solo describir el fenómeno, sino advertir su evolución, mutaciones y posibles escaladas de amenaza. En este punto resulta pertinente introducir el concepto de *warning intelligence* (inteligencia de alerta temprana), una tradición analítica clásica de los estudios de inteligencia que adquiere renovada relevancia en entornos criminales complejos y adaptativos.

Desde la perspectiva clásica, la inteligencia de "alerta temprana" se define como la función de la inteligencia orientada a detectar indicios tempranos de amenazas emergentes, con el fin de proporcionar a los decisores el tiempo y el espacio necesarios para responder antes de que dichas amenazas se materialicen plenamente. Para Grabo (2010), la advertencia estratégica no se basa en la predicción exacta de eventos, sino en la identificación de patrones anómalos, cambios graduales y señales débiles que indiquen una modificación significativa en las capacidades, intenciones o comportamientos de un adversario. En términos similares, Wirtz (2017) subraya que el fracaso de la inteligencia de alerta temprana no suele obedecer a la ausencia de información, sino a la incapacidad para interpretar correctamente señales dispersas dentro de contextos complejos y ambiguos. Gentry y Gordon (2019) amplían este enfoque al señalar que la *strategic warning intelligence* resulta sobremedida desafiante en escenarios donde los actores no estatales, las tecnologías emergentes y las dinámicas no lineales erosionan los supuestos clásicos de previsibilidad. En dichos contextos la advertencia no puede basarse exclusivamente en indicadores lineales o jerárquicos, sino que debe orientarse a la comprensión de sistemas dinámicos, capaces de reorganizarse con prontitud frente a la presión externa.

Esta observación resulta en particular relevante para el análisis del ecosistema delictivo digital. Como ya se argumentó, la *dark web* opera en la forma de

un complejo sistema adaptativo, caracterizado por la ausencia de control centralizado, la recombinación funcional de nodos y la resiliencia estructural frente a intervenciones represivas. En consecuencia, la utilidad de la *warning intelligence* en este entorno no reside en anticipar actos delictivos específicos, sino en detectar transformaciones sistémicas que indiquen procesos de adaptación, escalamiento o convergencia criminal. Desde esta óptica, el enfoque ecosistémico y la inteligencia de alerta temprana se refuerzan mutuamente. Mientras el primero permite mapear la estructura y las interdependencias del sistema criminal, la segunda proporciona una lógica metodológica para observar su dinámica evolutiva. En vez de centrarse en actores individuales o plataformas concretas, la advertencia estratégica se orienta hacia la vigilancia de flujos críticos, innovaciones tecnológicas, cambios en patrones de interacción y mutaciones narrativas, todos ellos indicadores tempranos de transformación del ecosistema.

A fin de traducir esta lógica en una herramienta analítica concreta, la tabla 5 presenta una matriz de identificación de puntos de intervención estratégica, diseñada desde una perspectiva de *warning intelligence* aplicada a ecosistemas criminales digitales.

**Tabla 5.** Matriz de *warning intelligence* para el ecosistema criminal de la dark web

| Elemento del ecosistema criminal     | Indicadores de alerta temprana                                                                                                                           | Valor estratégico para inteligencia y defensa                                                                      |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Flujos financieros ilícitos</b>   | Cambios abruptos en el uso de criptomonedas; migración hacia <i>privacy coins</i> ; aparición de nuevos mezcladores o protocolos de anonimato financiero | Señala procesos de adaptación frente a presión regulatoria o preparación de operaciones criminales de mayor escala |
| <b>Infraestructura tecnológica</b>   | Incremento en el uso de nuevos servicios ocultos; <i>bulletproof hosting</i> o tecnologías emergentes de anonimización                                   | Indica reorganización ecosistémica tras acciones de disrupción estatal o tecnológica                               |
| <b>Mercados y foros clandestinos</b> | Aparición de servicios integrados ( <i>bundling criminal</i> ); especialización funcional extrema, o consolidación de reputaciones transversales         | Refleja maduración del ecosistema y aumento de eficiencia operativa                                                |
| <b>Interacciones actorales</b>       | Convergencia entre actores criminales, ideológicos y estatales en espacios compartidos                                                                   | Alerta sobre procesos de hibridación entre crimen organizado, espionaje y conflicto híbrido                        |
| <b>Narrativas y contenidos</b>       | Circulación de discursos que legitiman el crimen como resistencia, negocio o causa política                                                              | Señal temprana de normalización social del delito y expansión de bases de apoyo digitales                          |

**Fuente:** elaboración propia, con base en Grabo (2010), Wirtz (2017) y Gentry y Gordon (2019).

Desde una lógica de inteligencia anticipatoria, la intervención estratégica eficaz no consiste en “desmantelar” el ecosistema criminal (un objetivo poco realista en sistemas complejos adaptativos), sino en incrementar los costos de adaptación, reducir la velocidad de recombinación funcional y generar fricciones persistentes en flujos y tecnologías críticas. Para la inteligencia y la defensa, ello implica priorizar la detección de señales débiles, identificar cuellos de botella sistémicos y anticipar trayectorias evolutivas del crimen digital, en vez de respuestas reactivas centradas exclusivamente en actores visibles. En conjunto, la integración entre el marco de sistemas complejos, la operacionalización del ecosistema criminal y la lógica de la *warning intelligence* refuerza el valor del enfoque ecosistémico como herramienta analítica, prospectiva y decisional. La *dark web* aparece así no solo como un espacio de ilegalidad, sino como un sistema dinámico de poder criminal, cuya comprensión exige enfoques capaces de articular complejidad, anticipación y estrategia en los escenarios contemporáneos de seguridad y defensa.

En definitiva, abordar la *dark web* como un ecosistema criminal digital permite a académicos y profesionales ir más allá de las nociones simplistas del “ciber-crimen como herramienta” y apreciar su naturaleza sistémica, adaptativa e integrada. Reconoce las interacciones multiescalares entre individuos, tecnologías, economías y sistemas de gobernanza que sustentan el submundo cibernético. Así como Álvarez (2017) advierte que la ausencia de autoridad estatal en los ecosistemas criminales físicos de Colombia conduce a una gobernanza basada en la ilegalidad, la ausencia de marcos jurídicos internacionales y de capacidad de aplicación de la ley en el ciberespacio abre la puerta a que actores cibernéticos no estatales ejerzan coerción, legitimidad y control sobre los territorios digitales.

Por lo tanto, el desafío para los responsables políticos de la toma de decisiones y las instituciones de seguridad y defensa no consiste en, simplemente, reprimir a actores aislados, sino en intervenir de manera estratégica en el propio ecosistema: modificando las entradas, alterando las rutas de flujo, reduciendo los incentivos sistémicos y restaurando la gobernanza del espacio digital. En resumen, la *dark web* no es un espacio monolítico de maldad ni una colección aleatoria de actos ilegales: por el contrario, es un ecosistema complejo, dinámico e interconectado (es decir, una biosfera en evolución de delincuencia, desviación y convergencia), que refleja tanto las posibilidades como los fracasos de la globalización del siglo XXI.

## Delitos de conexión e inmersión: redes sociales, metacrimen y desviación digital

La constante evolución del ciberespacio ha dado lugar no solo a nuevas formas de comunicación y de comercio, sino también a nuevas modalidades de comportamiento delictivo. Entre ellas, dos destacan por su complejidad e importancia: el cibercrimen en plataformas de redes sociales y la emergente categoría de *metacrímenes* en entornos digitales inmersivos como el metaverso. Ambos fenómenos trascienden los marcos criminológicos tradicionales, y plantean desafíos únicos para la regulación, la aplicación de la ley y la comprensión conceptual.

El cibercrimen en las plataformas de redes sociales se ha desarrollado a la par con la proliferación de estas plataformas, al igual que el contenido generado por los usuarios. Como argumentan Babu y Siddik (2022), la rápida expansión de las TIC ha creado un terreno fértil para la innovación delictiva, especialmente en ámbitos caracterizados por el anonimato, la velocidad y los flujos transfronterizos de información. Estos incluyen delitos como el robo de identidad, acoso, obscenidad digital y manipulación de datos personales. Sin embargo, como señalan Smith y Haines (2023), las categorizaciones tradicionales a menudo no toman en cuenta la naturaleza fluida y polimórfica de estos cibercrímenes: por ejemplo, muchos cibercrimitos en redes sociales abarcan simultáneamente múltiples categorías, combinando elementos de daño interpersonal, robo de propiedad y sabotaje reputacional.

Paralelamente a estos desarrollos, la aparición del metacrimen (comportamiento delictivo en entornos digitales inmersivos, persistentes y descentralizados, como el metaverso) presagia una ruptura epistemológica en la comprensión del propio delito. El metacrimen no es simplemente una extensión del cibercrimen: abarca un nuevo espectro de desafíos criminógenos, victimógenos, etiológicos y regulatorios, como lo demuestran Zhou et al. (2025). Estos delitos involucran avatares, contratos inteligentes y activos virtuales, y a menudo ocurren en zonas grises legales más allá de la jurisdicción territorial convencional. Además, el metacrimen implica nuevas dimensiones afectivas y cognitivas de victimización, debido a la naturaleza inmersiva y corporizada del metaverso.

Para fundamentar este análisis se hace necesario basarse en dos marcos teóricos complementarios. En primer lugar, la categorización de Wall (2007) del cibercrimen en delitos de contenido, delitos de integridad y delitos de engaño/robo proporciona una tipología útil para analizar el cibercrimen en las redes sociales. En segundo lugar, para el metacrimen adopto la perspectiva conceptual de Tiwari

et al. (2025), quienes argumentan que el delito en el metaverso debe evaluarse a través de las dimensiones criminógena, victimogénica y regulatoria. Estos marcos se emplearán a continuación para sistematizar el debate y destacar los puntos de convergencia y divergencia entre los delitos en redes sociales y el metacrimen.

Finalmente, este apartado se alinea con el modelo de los ecosistemas criminales de Álvarez y Rodríguez (2018), que conceptualizan el cibercrimen como una interacción dinámica entre actores, facilitadores y mercados. Con base en este modelo, la red oscura y las comunicaciones cifradas, al igual que las plataformas descentralizadas, funcionan como facilitadores y sustratos para la evolución de organizaciones criminales. Adicionalmente, las nuevas actividades de ciberdelincuencia, como el acoso en redes sociales o las estafas descentralizadas de *tokens* no fungibles (en inglés, NFT, por las iniciales de *Non-Fungible Tokens*), vienen reflejando la lógica de dicho ecosistema, caracterizado por su modularidad, su adaptabilidad y su alcance transnacional. Como se procura demostrar, tanto la delincuencia en redes sociales como el metacrimen ocupan zonas diferentes, aunque cada vez más superpuestas, dentro de esta arquitectura ilícita en evolución.

## Cibercrimen en redes sociales

Las plataformas de redes sociales han transformado la naturaleza de la interacción pública y privada. Como explica Salter (217), estas plataformas de redes sociales ofrecen tanto el alcance y la velocidad de la comunicación masiva como también la intimidad de la correspondencia privada, a condiciones que propician la delincuencia digital. El diseño algorítmico de plataformas como Facebook, Twitter (X), Instagram y TikTok optimiza la interacción, mas no la seguridad, lo que permite una rápida difusión de contenido dañino, desinformación y la reproducción viral de conductas delictivas (por ejemplo, discursos de odio o pornografía vengativa). A su vez, el anonimato (o *seudonimato*), la transitoriedad del contenido y la escala global de las redes sociales debilitan las respuestas legales convencionales, especialmente al abordar delitos transjurisdiccionales o cuando este tipo de plataformas digitales se resisten a las citaciones judiciales debido a preocupaciones sobre la soberanía de los datos (Singh et. al, 2023). En este contexto, el cibercrimen deja de ser una simple conducta ilícita para convertirse en una característica estructural integrada en el diseño de los sistemas de redes sociales.

A partir de las tipologías propuestas en Roy y Tripathy (2023), el cibercrimen en redes sociales puede clasificarse en cinco dominios interrelacionados: El primero está relacionado con la ciberdifamación, una forma de ciberdelito que implica la

difusión de contenido falso, engañoso o humillante para dañar la reputación de personas. A menudo manifestada mediante imágenes manipuladas, narrativas falsas o campañas de desinformación coordinadas, la difamación se vuelve especialmente perjudicial en casos que involucran a mujeres, funcionarios públicos o grupos minoritarios. La velocidad a la que se comparte este contenido puede amplificar el daño, especialmente en ataques virales masivos o troleo orquestado (Singh et. al, 2023).

El segundo ámbito de los ciberdelitos en redes sociales es el relacionado con el acoso cibernético, que incluye el seguimiento, vigilancia o intimidación persistentes a través de mensajes directos, etiquetado o publicación repetida de datos personales. Cabe señalar que las redes sociales permiten a los acosadores monitorear a sus objetivos en múltiples plataformas en tiempo real; asimismo, el acoso puede ser de género, racial o político, lo que constituye violencia digital (Salter, 2017). El tercero es el *grooming* y la explotación infantil en línea: en efecto, una de las amenazas más graves es el uso de las redes sociales para iniciar, desarrollar y agravar conductas de *grooming*, donde los adultos manipulan a los menores para que realicen actos sexuales o de explotación. Estas interacciones pueden culminar en imágenes sexuales autogeneradas, trata o, incluso, secuestro. La capacidad para suplantar identidades y explotar la ingenuidad digital de los jóvenes usuarios exacerba el riesgo de este delito cibernético (Kumari et al., 2023).

El cuarto dominio de los ciberdelitos en las redes sociales es la desinformación e interferencia electoral, ya que las redes sociales también son un vector principal de comportamientos como la desinformación política, la desinformación relacionada con la salud (propaganda antivacunas) y los medios manipulados digitalmente (*deepfakes*). Estos comportamientos son instrumentalizados cada vez más por actores estatales y no estatales que buscan erosionar la confianza en las instituciones o manipular los procesos democráticos. Finalmente, se encuentra el *doxing*, donde la exposición deliberada de información personal (dirección, lugar de trabajo, números de teléfono) con intenciones maliciosas, conocida como *doxing*, se emplea cada vez más contra periodistas, funcionarios públicos, activistas u otras figuras públicas. Esta forma de ciberdelito utiliza como arma datos disponibles públicamente, y a menudo resulta en amenazas reales, pérdida de empleo o traumas de salud mental.

Una característica del ciberdelito en las redes sociales es su papel facilitador de la arquitectura de las mismas plataformas. Características de diseño como las funciones de retuitear/compartir, los “me gusta” y los comentarios, la difusión

algorítmica de contenido y una mínima configuración de privacidad predeterminada facilitan, a su vez, la viralidad del contenido dañino. Además, muchas plataformas monetizan los datos y la interacción de los usuarios, lo que crea incentivos perversos para retener durante más tiempo contenido controvertido o sensacionalista. Por ello, las plataformas de redes sociales no son intermediarios pasivos en la ciberdelincuencia: más bien, funcionan como facilitadores sociotécnicos que moldean, sostienen y, en ocasiones, amplifican la conducta delictiva en línea (Roy & Choudhary, 2023).

Salter (2017) profundiza esta crítica argumentando que la lógica económica y de diseño de las plataformas, impulsada por la mercantilización del contenido generado por los usuarios, genera lo que él denomina “daño predecible”. Es decir, el abuso en línea, que incluye el acoso, las amenazas y la distribución no consensuada de imágenes no es una aberración, sino un resultado estructural de las posibilidades de la plataforma. Es más, Salter (2017) sitúa esto dentro de una teoría crítica del abuso en línea, al señalar que estos daños rara vez son priorizados por los moderadores o las fuerzas del orden, especialmente cuando las víctimas son mujeres o usuarios marginados.

Pero a pesar de la creciente evidencia que vincula la arquitectura de redes sociales con algunos ciberdelitos, los marcos legales siguen siendo reactivos y fragmentados. Roy y Choudhary (2023) critican la insuficiencia de las leyes nacionales actuales señalando que la mayoría de los marcos (incluida la Ley de Tecnologías de la Información de la India y leyes comparables en el Sur Global), carecen de fuerza para su aplicación, debido a la escasez de recursos en las unidades policiales y a la insuficiente capacitación digital. Además, en jurisdicciones como la de Estados Unidos, el artículo 230 de la Ley de Decencia en las Comunicaciones ha protegido históricamente a las plataformas de redes sociales de la responsabilidad por el contenido de terceros. Aunque fue modificada por FOSTA-SESTA, en 2018, para permitir el enjuiciamiento civil y penal de los sitios web involucrados en la trata de personas con fines de explotación sexual, la ley sigue siendo controvertida y de alcance limitado.

A nivel internacional, la coordinación regulatoria también sigue siendo un desafío. Si bien la Convención de Budapest representa, hasta el momento, el principal tratado internacional sobre ciberdelincuencia, Estados clave, como la Federación de Rusia y la República Popular de China no son signatarios, y ello dificulta su aplicación a nivel mundial. Hayes y Luther (2018) destacan las disparidades jurisdiccionales que surgen cuando los perpetradores, las plataformas y las víctimas

operan en diferentes territorios legales, lo que conduce a una aplicación inconsistente de la ley y a una reparación deficiente para las víctimas.

Esta disyuntiva socio-legal se hace visible en estudios de caso de alto perfil. El incidente de “Bois Locker Room”, en la India (2020), reveló cómo los chats grupales de Instagram pueden servir de repositorios de contenido misógino, que superan tanto a los sistemas disciplinarios escolares como a los moderadores de la plataforma. De igual manera, la campaña #Gamergate (2014-presente) utilizó como arma las posibilidades de la plataforma, como las etiquetas y el anonimato, para coordinar el abuso contra las mujeres en los videojuegos, lo cual vino a revelar los puntos ciegos sistémicos en los algoritmos de moderación de Twitter y Reddit. Finalmente, el Disturbio del Capitolio en los Estados Unidos del 6 de enero de 2021 ejemplificó la transición de la incitación digital a la violencia física, propiciada por las cámaras de resonancia de las plataformas y la incapacidad de la moderación algorítmica para anticipar la movilización a gran escala.

## Metacrimen: criminalidad inmersiva en el metaverso

El término “metacrimen” se refiere a los actos ilícitos cometidos en entornos virtuales inmersivos, persistentes y tridimensionales, como, por ejemplo, el metaverso. A diferencia del cibercrimen convencional, que ocurre en contextos bidimensionales mediados por pantallas, el metacrimen surge de las interacciones corpóreas basadas en avatares en espacios digitales diseñados para imitar y extender la realidad física (Tiwari et al., 2025). Estos ciberdelitos son posibles gracias a tecnologías como la realidad virtual (RV), la realidad aumentada (RA), la cadena de bloques (*blockchain*), la inteligencia artificial (IA) y los contratos inteligentes, por lo que desafían la jurisprudencia convencional, debido a su indeterminación espacial, ambigüedad jurisdiccional e intensidad psicológica. Tiwari et al. (2025) argumentan que el metacrimen presentaría al menos cinco dimensiones que lo distinguen del cibercrimen: 1) criminógeno (nuevas oportunidades), 2) victimógeno (vulnerabilidades únicas), 3) etiológico (causas distintas), 4) ético (daño inmersivo) y 5) regulatorio (fallos de las fuerzas del orden).

En este orden de ideas, el metaverso no sería tan solo una nueva plataforma para el cibercrimen existente, sino un novedoso terreno criminológico que reconfigura las relaciones entre el espacio, la identidad, el delito y la justicia. Interpol (2024) ha descrito recientemente siete categorías principales de metacrimen: los delitos de identidad, los delitos financieros, los delitos contra la propiedad intelectual, los delitos contra la propiedad, los delitos sexuales, los delitos contra menores

y el cibercrimen generalizado. Estos se comprenden mejor si se analizan a través de unas modalidades específicas:

1. Violencia sexual basada en avatares y acoso inmersivo: uno de los aspectos más controvertidos del metacrimen se refiere a la agresión y el acoso sexual que sufren los avatares en entornos de RV. Aunque no hay contacto físico, el realismo perceptual de los trajes hápticos, audio espacializado e interfaces corpóreas crea sensaciones intensas que las víctimas experimentan como profundamente violentas. Zhou et al. (2025) enfatizan que el impacto psicológico de una agresión virtual inmersiva puede rivalizar con el trauma psicológico del mundo real, lo que dificulta la distinción entre daño simbólico y daño material.
2. Estafas de NFT, *Rug Pulls* y comercio de lavado: los metaversos basados en la infraestructura *blockchain* admiten NFT y activos digitales como terrenos, *wearables* o avatares. Estos ecosistemas *tokenizados* han generado variadas estafas como *Rug Pulls* (abandono de un proyecto tras recaudar fondos de inversores), comercio de lavado (transacciones simuladas para inflar precios) y mercados falsos de NFT (Annison, 2022). Además, la falta de protección a los inversores, los protocolos KYC/AML deficientes y los mecanismos de intercambio descentralizados facilitan estos fraudes (Tiwari et al., 2025).
3. Blanqueo de capitales y financiación del terrorismo: los delincuentes explotan la fluidez de los criptoactivos para blanquear ganancias ilícitas, y evadir así a las instituciones financieras tradicionales. Como detallan Tiwari et al. (2025), las plataformas de metaverso permiten a los delincuentes convertir fondos ilícitos en monedas digitales, comprar terrenos virtuales o avatares y luego venderlos a monederos limpios. Estos rastros de dinero virtual son difíciles de rastrear y se complican aún más por el anonimato de los identificadores descentralizados.
4. Suplantación de avatar y robo de identidad *deepfake*: la suplantación de un avatar permite a los actores engañar, manipular o defraudar a otros actores en entornos persistentes. Con renderizado en tiempo real, además de retroalimentación biométrica y herramientas de IA generativa, los avatares pueden imitar convincentemente a personas reales. Estas suplantaciones pueden utilizarse en esquemas de *phishing*, captación de usuarios, extorsión y campañas de desinformación (Zhou et al., 2025). Es importante destacar que el realismo psicológico de las interacciones de los avatares intensifica el impacto del engaño.

5. Explosiones de contratos inteligentes y robo de activos virtuales: los contratos inteligentes automatizan las transferencias de activos, pero son altamente sensibles a las vulnerabilidades a nivel de código. Tiwari et al. (2025) documentan cómo los atacantes han manipulado contratos inteligentes para vaciar billeteras, falsificar *tokens* dentro de la plataforma y crear versiones falsas de activos digitales legítimos. Un ejemplo de ello fue la falsificación de Robux, en Roblox, donde las transacciones no autorizadas minaron la confianza en la plataforma.
6. Delitos internos-internos y entre reinos: Seo et al. (2023) clasifican los metadelitos en cuatro categorías: 1) internos-internos (p. ej., robo completamente dentro del metaverso), 2) internos-externos (el delito ocurre en el metaverso, pero sus efectos se presentan en el mundo real), 3) externos-internos (delitos en el mundo real facilitados a través del metaverso) y 4) multifacéticos (delitos de doble contexto con evidencia en ambos ámbitos). Esta tipología enfatiza la naturaleza híbrida y difusa del metacrimen.

Por otro lado, una característica muy importante del metacrimen es el realismo de la victimización. Tiwari et al. (2025) argumentan que las cualidades inmersivas de los entornos de RV reducen la distancia psicológica entre la simulación y la realidad, ya que las víctimas internalizan el daño del avatar como daño personal. Por ejemplo, el acoso, el manoseo o la agresión en RV pueden desencadenar disociación, trastorno de estrés postraumático (TEPT) o ansiedad similar a la del trauma del mundo real. Además, los avatares actúan como gemelos digitales: prototipos mejorados biométricamente que imitan la postura corporal, la voz, las expresiones faciales y las señales fisiológicas. Esta continuidad encarnada hace que la victimización en el metaverso sea plausible y personal, lo que complica las distinciones legales entre avatar y usuario (Gehl, 2018; Tiwari et al., 2025).

Con base en lo anterior, la regulación del metacrimen se enfrenta a tres desafíos principales. El primer desafío es una falta de coherencia jurisdiccional, ya que ningún organismo soberano gobierna el metaverso. Tiwari et al. (2025) argumentan que esas lagunas jurisdiccionales permiten a los delincuentes operar con impunidad a través de las fronteras, por lo que estas empresas del metaverso se constituyen en jurisdicciones favorables, limitan el alcance de la persecución penal y complican la aplicación transnacional de la ley.

El segundo desafío son los derechos de propiedad intelectual poco claros, ya que la propiedad de los NFT, avatares y territorios digitales a menudo carece de una

definición legal sólida. Según Tiwari et al. (2025), los contratos inteligentes automatizan la transferencia de propiedad, pero no resuelven las disputas sobre el código fuente, los derechos de autor o la replicación no autorizada. Esto crea zonas grises legales en torno al robo de activos, la suplantación de marca y la falsificación.

El tercer desafío es la ambigüedad de la responsabilidad de los avatares: o sea, ¿quién es responsable cuando un avatar comete un delito? Tiwari et al. (2025) afirman que los avatares pueden servir como extensiones psicológicas de los usuarios, pero también son entidades legalmente distintas. Ello plantea interrogantes sobre la atribución de agencia y culpabilidad, especialmente en casos de los *deepfakes*, perfiles pirateados o avatares generados por IA.

## Análisis comparativo e integración del ecosistema

Si bien el cibercrimen en redes sociales y el metacrimen difieren en la complejidad de sus plataformas, sus lógicas delictivas subyacentes muestran una superposición sustancial. Los puntos de convergencia son los siguientes:

1. El cibercrimen en las redes sociales y el metacrimen están tecnológicamente habilitados: Se basan en infraestructuras digitales (algoritmos de redes sociales o plataformas inmersivas) diseñadas principalmente para la conectividad y la monetización, y no para la seguridad del usuario ni el cumplimiento legal.
2. El cibercrimen en las redes sociales y el metacrimen son impulsados por el anonimato: Los delincuentes explotan las posibilidades de seudónimos de los nombres de usuario en redes sociales o avatares del metaverso para ofuscar la identidad, reducir la trazabilidad y ampliar el alcance operativo.
3. El cibercrimen en las redes sociales y el metacrimen son jurisdiccionalmente evasivos: Ambos tipos de ciberdelito dejan en evidencia la incapacidad de las geografías legales para regular espacios digitales sin fronteras. Un acosador que opera desde un país o un estafador que blanquea NFT de otro a menudo quedan atrapados en la nada (zona gris).
4. El cibercrimen en las redes sociales y el metacrimen buscan la explotación de datos: Ya sea mediante la recopilación de datos personales en Facebook o el rastreo de datos biométricos mediante trajes hápticos en el metaverso, estos ciberdelitos se basan en la asimetría informativa entre las arquitecturas de las plataformas y los usuarios (Roy & Tripathy, 2023; Tiwari et al., 2025).

Estas similitudes apuntan a una arquitectura criminógena compartida, que Álvarez y Rodríguez (2018) describen como las "condiciones del sustrato" de los ecosistemas criminales: ausencia de supervisión, densidad de oportunidades, incentivos de mercado y flujos de recursos que propician la conducta ilícita. Sin embargo, el metacrimen no es una extensión del cibercrimen, sino, por el contrario, una ruptura paradigmática, ya que es un salto criminológico hacia la desviación pospantalla, integrada espacialmente. Por eso, y a pesar de su solapamiento, el metacrimen puede entenderse como una frontera cualitativamente nueva. Los puntos de divergencia con relación con el cibercrimen en redes sociales son las siguientes:

1. Daño inmersivo: En redes sociales la victimización se basa en la pantalla y es principalmente textual o visual. En el metacrimen las víctimas experimentan sensaciones físicas y violaciones encarnadas a través de avatares, lo cual hace que el daño se acerque psicológicamente a la agresión física (Tiwari et al., 2025).
2. Ambigüedad ontológica: Los usuarios de las redes sociales son claramente humanos. En el metaverso los avatares pueden ser controlados por el usuario, operados por *bots* o generados por IA, lo que difumina las fronteras entre agencia y responsabilidad.
3. Complejidad de activos: Los delitos en las redes sociales rara vez involucran propiedad tokenizada. En contraste, el metacrimen gira en torno a tierras digitales, NFT y propiedad mediada por contratos inteligentes, lo que complica la restitución y la valoración.
4. Dispersión probatoria: El metacrimen puede abarcar plataformas y ámbitos (por ejemplo, un incidente de acoso en realidad virtual con evidencia en Discord y *blockchain*), lo que dificulta exponencialmente la reconstrucción forense (Tiwari et al., 2025).

En el contexto descrito, el modelo de ecosistema criminal es en especial relevante para sintetizar estos dominios. Por lo tanto, el modelo define los ecosistemas criminales como constelaciones dinámicas de (Álvarez & Rodríguez, 2018): 1) actores (individuos, grupos e intermediarios); 2) tecnologías (plataformas, cifrado, contratos inteligentes); 3) territorios (espacios virtuales o físicos de control o influencia); 4) flujos (de dinero, datos, poder, contenido), y 5) reglas (normas implícitas, códigos o estructuras formales).

Los delitos en redes sociales funcionan dentro de un ecosistema con alta densidad de actores, difusión algorítmica de contenido (flujo) y reglas formales débiles

(por ejemplo, ausencia de jurisprudencia robusta en la materia). Sus facilitadores incluyen el anonimato, la viralidad y la baja rendición de cuentas de la plataforma. El metacrimen, en cambio, opera en un ecosistema descentralizado que se caracteriza por territorios inmersivos (mundos de realidad virtual), flujos mediados por *blockchain* (criptomonedas, NFT), así como reglas ambiguas (por ejemplo, responsabilidades poco claras de los avatares). Sus facilitadores incluyen la presencia espacial, las posibilidades de los avatares y los contratos inteligentes. En ambos casos es válida la idea de Álvarez y Rodríguez (2018) de que la delincuencia prospera donde las instituciones formales se retiran o no se adaptan; al igual que en su análisis original de los ecosistemas criminales urbanos colombianos, los análogos digitales observados aquí muestran un repliegue institucional y una ilegalidad adaptativa.

Además, tanto el cibercrimen en las redes sociales como el metacrimen presentan zonas de convergencia horizontal, donde se interceptan distintas economías criminales. Por ejemplo, una campaña de *doxing* en X (un actor) puede extenderse al metaverso, donde el avatar de un usuario es el objetivo. Una estafa de NFT (delito basado en activos) puede financiar una campaña de acoso en Discord o Instagram. Un evento de acoso en VRChat puede dar pie a un chantaje en el mundo real a través de Telegram. Estos puntos de convergencia sugieren que la delincuencia digital del presente no debe analizarse de forma aislada, sino como sistemas ecológicos superpuestos que interactúan a través de flujos de capital, información y violencia simbólica. También es necesario señalar que los ecosistemas criminales son inherentemente adaptativos. Tal como lo señalan Álvarez y Rodríguez (2018), cuando se aplica presión a un nodo (por ejemplo, las fuerzas del orden interrumpen Silk Road) el sistema se regenera en otro (nuevos mercados, como Hydra o AlphaBay). La misma lógica se aplica ahora a plataformas descentralizadas que resisten la intervención estatal, generadores de avatares impulsados por IA que logran ocultar la identidad y sindicatos multiplataforma que integran redes sociales con realidad virtual y criptomonedas para generar sinergias operativas.

Por consiguiente, y de cara al futuro, la convergencia de la Web 3.0, la tecnología inmersiva y las finanzas descentralizadas (DeFi) parece sugerir una nueva generación de "ecologías híbridas" ciberdelictivas, marcadas por identidades estratificadas, la agencia de la IA y dilemas de gobernanza postterritorial. En este futuro el llamado de Álvarez y Rodríguez (2018) a mapear, intervenir e interrumpir las rutas de flujo de los ecosistemas criminales se convierte en un imperativo estratégico, no solo para los Estados, sino también para las instituciones multilaterales, las plataformas privadas y las coaliciones de la sociedad civil.

En resumen, el surgimiento del cibercrimen en redes sociales y del metacrimen reflejan una profunda transformación en la naturaleza, el alcance y la arquitectura de la delincuencia digital. No se trata simplemente de nuevos delitos en nuevas plataformas: representan la formación de nuevos entornos criminógenos, caracterizados por la presencia inmersiva, la gobernanza algorítmica, las finanzas descentralizadas y la convergencia del anonimato con una interacción de alto impacto. Este capítulo ha procurado demostrar cómo estas formas de ilegalidad digital interactúan con el diseño de plataformas, el comportamiento social, la ambigüedad legal y la complejidad tecnológica.

Sin embargo, para comprender plenamente las implicaciones de estos desarrollos, es necesario considerar el papel de la desviación digital como puente conceptual entre la violación de las normas en línea y la delincuencia estructurada. Como argumentan Graham y Smith (2024), la desviación digital incluye el troleo, la resistencia subcultural, el "acoso gamificado" y los actos performativos que difuminan la legalidad y la moralidad. Estos comportamientos funcionan como iniciadores culturales socializando a los actores en redes, lenguajes y lógicas que facilitan o, incluso, normalizan la entrada a los ecosistemas cibercriminales. La desviación digital no es periférica, sino fundamental. Constituye el sustrato a partir del que puede crecer el crimen organizado, y por lo tanto sirve como puerta de entrada cultural, técnica y social a estructuras criminales más formalizadas. La progresión desde la participación desviada en campañas de desinformación o suplantación de avatares hasta la plena participación en esquemas de *ransomware* o fraudes con NFT se ve facilitada por las porosas fronteras morales y la validación subcultural presentes en muchas comunidades en línea.

El cibercrimen en redes sociales y el metacrimen funcionan como subsistemas adaptativos dentro de un ecosistema criminal policéntrico más amplio, caracterizado por la autoorganización, la modularidad y los flujos transnacionales de datos, capital y daños. El énfasis de Álvarez y Rodríguez (2018) en los flujos, los nodos y los facilitadores ayuda para aclarar cómo las economías ilícitas se distribuyen entre plataformas, cómo los actores se especializan o coordinan, y cómo estos sistemas evolucionan bajo la presión de las fuerzas del orden o el escrutinio público. Para afrontar tan complejas realidades, las intervenciones políticas deben evolucionar más allá de la aplicación reactiva de la ley. Deben incluir:

1. Reforma de la gobernanza de las plataformas, con transparencia exigible, rendición de cuentas algorítmica y sólidos estándares de protección del usuario.

2. Innovación legal capaz de abordar los daños específicos del metaverso, incluyendo la responsabilidad por avatares, el consentimiento inmersivo y la regulación descentralizada de activos.
3. Programas de educación y alfabetización digital que desmitifiquen las prácticas desviadas en redes sociales y doten a los usuarios, especialmente a los jóvenes, de herramientas cruciales para gestionar el riesgo y resistir la normalización del daño en línea.
4. Cooperación transnacional en ciberseguridad, especialmente en el análisis forense, la criptorregulación y la investigación interjurisdiccional de delitos cometidos en mundos virtuales inmersivos.
5. Investigación sociotécnica que integre criminología, interacción humano-computador, psicología del comportamiento y antropología digital para adaptar continuamente los modelos de amenazas a la innovación de las plataformas.

En consecuencia, el estudio de las nuevas actividades de ciberdelincuencia en redes sociales y entornos metaversales debe basarse no solo en la tecnología o el derecho, sino también en la desviación cultural, la evolución del comportamiento y la teoría de sistemas. Solo vinculando la desviación digital con los ecosistemas criminales podremos empezar a comprender, y eventualmente desmantelar, las arquitecturas de daño que ahora están arraigadas en nuestros espacios digitales más avanzados.

## Conclusiones

Este capítulo abordó la pregunta central: ¿Cómo operan y evolucionan las redes ciber criminales organizadas dentro de los ecosistemas de la *dark web*, y cuáles son las dinámicas estructurales, tecnológicas y criminológicas que sustentan estas economías ilícitas? Pues bien, a lo largo del presente análisis se logró el objetivo de identificar las estructuras, funciones y dinámicas operativas de la ciberdelincuencia organizada en la *dark web* articulando perspectivas criminológicas, sociotécnicas y estratégicas, para revelar la complejidad y resiliencia del ecosistema criminal digital.

En efecto, las redes ciberdelincuenciales organizadas no son entes aislados, sino subsistemas interdependientes que interactúan dentro de una arquitectura más amplia que integra anonimato, especialización funcional, mercados

descentralizados y lógica empresarial. Al igual que sus contrapartes en el mundo físico, estas redes aprovechan vacíos regulatorios, fallas de gobernanza tecnológica y subculturas digitales desviadas para sostener una cadena de valor delictiva transnacional, sostenida por criptomonedas, plataformas de anonimización y entornos digitales inmersivos.

La evolución de la ciberdelincuencia organizada en la era digital de la actualidad refleja la convergencia de las motivaciones delictivas tradicionales con las nuevas posibilidades tecnológicas. En efecto, la ciberdelincuencia ha pasado de ser solo *exploits* de *hacking* aislados a operaciones estructuradas y orientadas a servicios, integradas en los mercados ilícitos globales. Esta transformación se caracteriza por la profesionalización de los ciberdelincuentes, la proliferación de modelos de crimen como servicio (CaaS) y el uso estratégico de tecnologías de anonimización como las VPN, las criptomonedas y la red Tor.

No obstante, una perspectiva clave es la naturaleza cada vez más ecosistémica de la delincuencia digital, ya que las organizaciones ciberdelincuenciales no operan de forma aislada: por el contrario, forman parte de una red interconectada de servicios, intermediarios, plataformas y actores que facilitan todo, desde el diseño y la distribución de *malware* hasta el blanqueo de capitales ilícitos y la facilitación del mercado ilegal. Dentro de dicha estructura, la desviación digital cumple una función vital, aunque a menudo subestimada. Como argumentan Graham y Smith (2024), la desviación digital abarca una gama de prácticas subculturales, posturas ideológicas y comportamientos que traspasan los límites de la legalidad y la legitimidad. Estos incluyen el troleo, el *doxing*, la piratería y el vigilantismo digital. Prácticas que no siempre pueden clasificarse como delitos, pero, sin embargo, desafían las normas sociales y erosionan las fronteras entre la legalidad y la ilegalidad.

Es importante destacar que la desviación digital actúa como precursor cultural y conductual de formas más organizadas de ciberdelincuencia. Las comunidades desviadas normalizan la conducta transgresora en línea proporcionando bases de reclutamiento, justificaciones morales y habilidades técnicas que alimentan organizaciones delictivas más formalizadas. Además, la visibilidad y la proliferación de comportamientos desviados contribuyen a un ambiente cultural más amplio, donde la legalidad se vuelve negociable, la aplicación de la ley se dificulta y la ciberdelincuencia se camufla ideológicamente.

Por lo tanto, la ciberdelincuencia organizada no solo debe entenderse en términos técnicos o económicos, sino también como parte de un continuo socio digital más amplio, en el que la desviación, la subcultura y la innovación criminal

coevolucionan. Por ende, las futuras investigaciones y respuestas políticas al cibercrimen deberían adoptar una perspectiva multidisciplinaria (integrando la criminología, la sociología, la ciberseguridad y los estudios culturales digitales), para comprender la arquitectura completa de las operaciones cibercriminales en el siglo XXI.

Este capítulo demuestra que tanto la ciberdelincuencia organizada en la *dark web* como los delitos emergentes en redes sociales y metaverso constituyen expresiones diferenciadas, pero convergentes, de un ecosistema criminal digital en evolución. Este ecosistema se caracteriza por su modularidad, descentralización y adaptabilidad, lo que dificulta el uso de marcos legales tradicionales y herramientas de seguridad unidimensionales. La desviación digital, además, emerge como un factor cultural y conductual clave: normaliza el comportamiento transgresor y facilita la transición hacia formas más estructuradas de criminalidad. Desde una perspectiva de los estudios en seguridad y defensa, y considerando la especificidad del entorno colombiano, se proponen las siguientes líneas de acción:

1. Fortalecer la inteligencia cibernética estructural. La ciberdelincuencia organizada del presente no puede enfrentarse solo con “ciberpatrullajes” o respuestas tácticas. Se requiere un modelo de inteligencia estratégica del ecosistema criminal digital, que identifique nodos, flujos, roles funcionales y convergencias entre mercados, plataformas y actores ilícitos.
2. Crear un Centro Nacional de Estudios Criminológicos Digitales. Colombia necesita un espacio interdisciplinario que articule criminología, ciberseguridad, sociología digital y ciencia de datos para comprender y anticipar la evolución del crimen en entornos virtuales. Este centro debe formar parte del Sistema Nacional de Inteligencia y Contrainteligencia.
3. Actualizar el marco jurídico penal y procesal para tipificar ciberdelitos asociados a: 1) la inmersión digital y los avatares (metacrímenes); 2) la participación en economías ilícitas digitales; 3) el desarrollo y comercialización de herramientas delictivas (*malware*, *exploits*), y 4) la complicidad algorítmica y negligencia de plataformas.
4. Impulsar un esquema robusto de cooperación interagencial y con el sector privado, articulando a: 1) Ministerio de Defensa y Policía Nacional (Dirección de Investigación Criminal e Interpol); 2) MinTIC y Ministerio de Justicia; 3) Superintendencia Financiera y la Unidad de Información y Análisis Financiero (UIAF) (por criptoactivos), y 4) Grupo de Respuestas a Emergencias Cibernéticas de Colombia (ColCERT) y sector académico en ciberseguridad.

5. Establecer mecanismos de gobernanza algorítmica, y además, exigir a plataformas que operan en Colombia: 1) protocolos de moderación más transparentes; 2) mecanismos rápidos de remoción de contenido criminal, y 3) colaboración con autoridades judiciales, sin invocar sistemáticamente el “puerto seguro” de la neutralidad tecnológica.
6. Diseñar una estrategia nacional de prevención de la desviación digital, con énfasis en: 1) alfabetización crítica para los jóvenes en las redes sociales y plataformas inmersivas; 2) intervenciones tempranas en las comunidades digitales de alto riesgo, y 3) visibilización de las consecuencias psicológicas del metacrimen y el acoso virtual.
7. Integrar el concepto de los ecosistemas criminales a la estrategia colombiana de ciberseguridad reconociendo que: 1) el ciberespacio debe ser concebido como un entorno operativo fluido y estratégico; 2) las intervenciones deben ser sistémicas, y no aisladas, y 3) las políticas deben orientarse a modificar las condiciones del entorno, y no solo a capturar individuos.

En suma, comprender la *dark web*, el metacrimen y el crimen en redes sociales desde una lógica de ecosistemas criminales digitales permite avanzar hacia un modelo de seguridad predictivo, adaptativo y multidimensional. Colombia, como potencia regional emergente en ciberseguridad, debe liderar en la región de América Latina la transición hacia un paradigma de gobernanza estratégica del ciberespacio, que combine tanto la soberanía tecnológica como la disuasión jurídica, la alfabetización cultural y la cooperación internacional inteligente.

## Referencias

- Alexandrou, A. (2021). *Cybercrime and information technology: Theory and practice - The computer network infrastructure and computer security, cybersecurity laws, internet of things (IoT), and mobile devices*. CRC Press.
- Álvarez, C. (2017). Ocupación de los espacios vacíos: una condición sine qua non para la seguridad multidimensional en Colombia. En Álvarez, C. (ed.), *Escenarios y desafíos para la seguridad multidimensional en Colombia* (pp. 307-386). Sello Editorial ESDEG.
- Álvarez, C. y Zambrano, J. (2017). Globalización desviada: plataforma de convergencia criminal. En Álvarez, C. (Ed.), *Escenarios y desafíos para la seguridad multidimensional en Colombia* (pp. 249-306). Sello Editorial ESDEG.
- Álvarez, C. y Rodríguez, C. (2018). Criminal ecosystems: Habitats for convergence and deviant globalization. *Revista Científica General José María Córdova*, 16(24), 1-30.
- Akhgar, B.; Gercke, M.; Vrochidis, S. y Gibson, H. (Eds.). (2021). *Dark web investigation*. Springer.
- Annisson, T. (2022). *The Future of Financial Crime in the Metaverse: Fighting Crypto-Crime in Web 3.0*. Elliptic.
- Bandler, J. y Merzon, A. (2020). *Cybercrime investigations: A comprehensive resource for everyone*. CRC Press.
- Brenner, S. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. UPNE.
- Brewer, R.; de Vel-Palumbo, M.; Hutchings, A.; Holt, T.; Goldsmith, A. y Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Palgrave Macmillan.
- Chaka, J. y Marimuthu, M. (2018). Curtailing the threats to cloud computing in the fourth industrial revolution. En Fields, Z. (Ed.), *Handbook of research on information and cyber security in the fourth industrial revolution* (pp. 112-141). IGI Global.
- Check Point Software Technologies (2025). *2025 Cyber Security Report: Understanding Cybercrime Trends and Threat Vectors in a Post-RaaS Era*. <https://www.checkpoint.com/downloads/cyber-security-report-2025.pdf>
- Choi, K.; Lee, C. y Louderback, E. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. En Holt, T. y Bossler, A. (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 27-43). Palgrave Macmillan.
- Clough, J. (2012). The council of Europe convention on cybercrime: Defining 'crime' in a digital world. *Criminal Law Forum*, 23, 363-391.
- Clough, J. (2015). *Principles of cybercrime (2nd ed.)*. Cambridge University Press.
- Daras, N. (Ed.). (2019). *Cyber-security and information warfare*. Nova Science Publishers.
- Donalds, C., Barclay, C. y Osei-Bryson, K. (2022). *Cybercrime and cybersecurity in the Global South: Concepts, strategies and frameworks for greater resilience*. CRC Press.
- East, C. (2017). Demystifying the Dark Web. *ITNOW*, 59(1), 16-17.
- Friedrichs, D. (2009). *Trusted criminals (4th ed.)*. Cengage.

- Gehl, R. W. (2018). *Weaving the Dark Web: Legitimacy on freenet, Tor, and I2P*. MIT Press.
- Gentry, J. y Gordon, J. (2019). *Strategic Warning Intelligence: History, Challenges, and Prospects*. Georgetown University Press.
- Grabo, C. (2010). *Handbook of Warning Intelligence: Assessing the Threat to National Security*. Scarecrow Press.
- Graham, R. y Smith, S. (2024). *Cybercrime and digital deviance (2nd ed.)*. Routledge.
- Hannigan, K. (2021). Vygotsky and Internet Grooming: The Darker Side of ZPD and Scaffolding. En Owen, T. y Marshall, J. (Eds.), *Rethinking Cybercrime: Critical Debates* (pp. 23-40). Palgrave Macmillan.
- Hayes, R. y Luther, K. (2018). *#Crime: Social Media, Crime, and the Criminal Legal System*. Palgrave Macmillan.
- Hollinger, R. y Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. *Criminology*, 26, 101-126.
- Holt, T.; Bossler, A. y Seigfried-Spellar, K. (2022). *Cybercrime and digital forensics: An introduction (3rd ed.)*. Routledge.
- INTERPOL (2024). *Metaverse a Law Enforcement Perspective: Use Cases, Crime, Forensics, Investigation, and Governance*. INTERPOL
- Jenkinson, A. (2022). *Ransomware and cybercrime*. CRC Press.
- Kardya, M. y Mitrou, L. (2007). *Internet forensics: Legal and technical issues. Second international workshop on digital forensics and incident analysis*. WDFIA.
- Kremling, J. y Sharp Parker, A. (2017). *Cyberspace, cybersecurity, and cybercrime*. SAGE Publications.
- Krone, T. (2005). *Concepts and terms: High Tech Crime Brief*. Australian Institute of Criminology.
- Kumari, K.; Singh, J. y Suman, S. (2023). Analysis and Detection of Cyberbullying in Reddit Discussions. En Roy, P. y Tripathy, A. (Eds.). *Cybercrime in Social Media: Theory and Solutions* (pp. 107-120). CRC Press.
- Lastowka, F. y Hunter, D. (2004). The laws of the virtual worlds. *California Law Review*, 92, 1-73.
- Lavorgna, A. (2020). Organized Crime and Cybercrime. En Holt, T. y Bossler, A. (Eds.). *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 117-134). Palgrave Macmillan.
- Leukfeldt, E.; Lavorgna, A. y Kleemans, E. (2017). Organised cybercrime or cybercrime that is organised? *European Journal of Criminology*, 14(1), 100-119.
- Liggett, R.; Lee, J.; Roddy, A. y Wallin, M. (2020). The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets. En Holt, T. y Bossler, A. (Eds.). *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 91-116). Palgrave Macmillan.
- Luo, X. y Liao, Q. (2009). Ransomware: A new cyber hijacking threat to enterprises. En Gupta, J. y Sharma, S. (Eds.), *Handbook of research on information security and assurance* (pp. 1-6). IGI global.

- Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.
- McGuire, M. (2012). *Organized crime in the digital age*. John Grieve Centre for Policing and Security and BAE Systems Detica.
- Mansfield-Devine, S. (2016). *Ransomware: Taking businesses hostage*. Network Security, 10, 8-17.
- Nearchou, N. (2023). *Combating crime on the dark web: Learn how to access the dark web safely and not fall victim to cybercrime*. Packt Publishing.
- Neto, J. (2017). Social Network Analysis and Organized Crime Investigation: Adequacy to Networks, Organized Cybercrime, Portuguese Framework. En Viano, E. (Ed.), *Cybercrime, organized crime, and societal responses: International approaches* (pp. 179-200). Springer.
- Noble, W.; Owen, T. y Speed, F. (2017). *New perspectives on cybercrime*. Palgrave Macmillan.
- Owen, T. (2021). CyberTerrorism: Some Insights from Owen's Genetic-Social Framework. En Owen, T. y Marshall, J. (Eds.), *Rethinking Cybercrime: Critical Debates* (pp. 3-22). Palgrave Macmillan.
- Ozkaya, E. e Islam, R. (2019). *Inside the dark web*. CRC Press.
- Parker, D. (1976). *Crime by computer*. Scribner.
- Payne, B. (2020). Defining Cybercrime. En Holt, T. y Bossler, A. (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 3-26). Palgrave Macmillan.
- Roy, P. y Choudhary, J. (2023). Emotions Detection from Social Media Text Using Machine Learning. (2023). En Roy, P. y Tripathy, A. (Eds.), *Cybercrime in Social Media: Theory and Solutions* (pp. 41-66). CRC Press.
- Roy, P. y Tripathy, A. (Eds.) (2023). *Cybercrime in Social Media: Theory and Solutions* (pp. 1-22). CRC Press.
- Sabell, E.; Manaf, A. e Ismail, Z. (2012). Development of Malaysian digital forensics investigator competency identification methods. En Hassanien, A.; Salem, A.; Ramadan, R. y Kim, T. (Eds.), *Advanced machine learning technologies and applications* (pp. 554-565). Springer.
- Salter, M. (2017). *Crime, Justice and Social Media*. Routledge.
- Schwab, K. (2016). *The fourth industrial revolution*. Crown Business.
- Seo, S.; Seok, B. y Lee, C. (2023). Digital Forensic Investigation Framework for the Metaverse. *The Journal of Supercomputing*, 79(14), 9467-9485.
- Singh, B.; Kumar, A.; Adhikari, D.; Pradhan, J.; Singh, D. y Mishra, D. (2023). Fundamental Theories Behind the Detection of Fake News and Rumors. En Roy, P. y Tripathy, A. (Eds.), *Cybercrime in Social Media: Theory and Solutions* (pp. 1-22). CRC Press.
- Smith, T. y Haines, K. (2023). A Doubled- Edged Sword Called Cyberspace: Introducing the Concept of Cybercrime. En Roy, P. y Tripathy, A. (Eds.), *Cybercrime in Social Media: Theory and Solutions* (pp. 121-142). CRC Press.

- Symanovich, S. (2019). *How to safely access the deep and dark webs*. Norton.
- Thurner, S.; Hanel, R. y Klimek, P. (2018). *Introduction to the Theory of Complex Systems*. Oxford University Press.
- Tiwari, M.; Zhou, Y.; Gilmour, P. y Bernot, A. (2025). Confronting metacrime: complexities, enforcement challenges and regulatory pathways. *Law, Innovation and Technology*, 17(1), 159-176.
- UNODC. (2004). *United Nations Convention against Transnational Organized Crime (Palermo Convention)*. Organización de las Naciones Unidas.
- UNODC. (2022). *Compendio de Ciberdelincuencia Organizada*. Organización de las Naciones Unidas. Organización de las Naciones Unidas.
- Viano, E. (2017). Cybercrime: Definition, Typology, and Criminalization. En Viano, E. (Ed.), *Cybercrime, organized crime, and societal responses: International approaches* (pp. 3-22). Springer.
- Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity.
- Wang, Z. (2012). *Method for providing terminals of IMS network firewall and firewall system*. U.S. Patent Application.
- Watters, P. (2024). *Cybercrime and cybersecurity*. Routledge.
- Willems, E. (2019). *Cyberdanger: Understanding and guarding against cybercrime*. Springer.
- Wirtz, J. (2017). *Understanding Intelligence Failure: Warning, response and deterrence*. Routledge.