TRABAJO FIN DE GRADO – GRADO EN CRIMINOLOGÍA

El crimen organizado en el mundo digital

Autor del TFG:
Beatrice Donzella

Tutor del TFG:
D.ª Susana Berrocal Díaz

UNIVERSIDAD EUROPEA DE VALENCIA

2021/2022

Beatrice Donzella

El crimen organizado en el mundo digital

UNIVERSIDAD EUROPEA
Facultad de Ciencias Sociales
Grado en Criminología

Tutor: Susana Berrocal Díaz

Valencia, a 30 de mayo 2022

AGRADECIMIENTOS

Papà, ci sarebbero un'infinità di cose da dire. Grazie per aver reso possibile questo traguardo, per avermi sostenuta e aver avuto fiducia in me. Per tutti i sacrifici fatti e per esserci sempre anche se a infiniti chilometri di distanza.

Letizia e Leo grazie per essere la mia forza, il mio aeroporto con calma di vento e ciel sereno. Vi voglio un mondo di bene.

Mamma, grazie per il sostegno quotidiano e per la fiducia riposta in me, ti voglio bene.

Lavinia, una persona indescrivibile. Un'Amicizia preziosa, senza tempo, che si rafforza ogni giorno di più e che, anche a distanza di anni e di chilometri, dimostra essere fondamentale per me. Grazie per essere come sei.

Eva y María, mi *DreamTeam*! No tendría el suficiente espacio para agradeceros todo lo que habéis hecho por mi. Por estar siempre en las buenas y en las malas, por apoyarme, escucharme y compartir tantas experiencias conmigo. El recuerdo más bonito de Valencia, que llevaré siempre conmigo, en cualquier parte del mundo estaré.

Resumen

El estudio del crimen organizado trasnacional es un tema recurrente en las últimas décadas, debido a su proliferación y a la necesidad de conocer sus características. El presente Trabajo de Fin de Grado desarrolla el análisis de la relación que se ha originado entre la delincuencia organizada y las nuevas tecnologías. Particular es la influencia que internet ha ido proporcionando hasta evolucionar el modus operandi y estructura de las organizaciones criminales. Por tanto, se parte de la idea de proporcionar conocimientos funcionales a la hora de prevenir y combatir el fenómeno, con la finalidad de reducirlo y cumplir con el Objetivo de Desarrollo Sostenible número 16 de Naciones Unidas. Dicha finalidad se basa en el análisis de los delitos desarrollados por los grupos criminales, del rol facilitador e instrumental que mantienen las plataformas online y en el estudio de la valoración de la amenaza para las posibles víctimas de los delitos en cuestión. Se expondrán una serie de datos publicados por los principales organismos nacionales e internacionales como Interpol, Europol y Naciones Unidas, junto a noticias casi diarias como testimonio de la cantidad de casos existentes. En línea con el O.D.S. número 16 y a partir de las conclusiones realizadas, se observa un aumento de la amenaza, facilitada por el anonimato y el carácter sofisticado de internet. Se expondrán finalmente unas propuestas de prevención de tipo formativo y educativo, tanto por los profesionales, como para los sujetos vulnerables, más propensos a caer víctimas delitos como explotación sexual, tráfico de seres humanos y ciberdelitos de otro tipo.

Palabras-clave: crimen organizado trasnacional, internet, ciberdelitos, delincuencia organizada online.

Abstract

The study of transnational organised crime has been a recurring subject in the last decades due to its spreading and the need to know its characteristics. This Final Grade Work develops the analysis of the relation generated between organised crime and new technologies. In particular, the influence that Internet has provided for the evolution of the modus operandi and the structure of crime organisations themselves. Therefore, it starts from the idea to provide functional knowledge in order to prevent and fight against this phenomenon, with the purpose to reduce it and comply with number 16 of the Sustainable Development Objective of the United Nations. This purpose is based on the analysis of crimes carried out by criminal groups, on the enabling and instrumental role that online platforms hold, and on the study of threat valuation for the possible victims of the subject crimes. Data published from main national and international organisations will be presented, such as Interpol, Europol and United Nations, as well as daily news which put into evidence the quantity of existing cases. In line with the S.D.O. number 16 and from conclusions hereby made, we can determine an increase of the threat, made easier by anonymity and by Internet sophistication. Finally, training and educational prevention proposals will be presented, both for professional and victims subject to fall into sexual exploitation crimes, humans trafficking and other cybercrimes types.

Keywords: transnational organised crime, internet, cybercrime, organised crime online.

ÍNDICE

Pág.

1. INTRODUCCIÓN **1**
1.1. Problema de investigación. 1
1.2. Pregunta de investigación. 2
1.3. Objetivos. 2
1.3.1. Objetivo general. 2
1.3.2. Objetivos específicos. 2
1.4. Justificación: La relevancia, la originalidad y contribución científica al conocimiento académico. 3

2. FUNDAMENTACIÓN TEÓRICA **4**
2.1. Marco teórico. 4
2.1.1. Definiciones. 5
2.1.2. Perspectiva general del Crimen Organizado. 9
2.1.3. Perspectiva general del Ciberdelito. 12
2.1.4. Marco jurídico nacional e internacional de delincuencia organizada y del ciberdelito. 14
2.1.5. Actualidad: Crimen Organizado Informático o nueva forma de Crimen Organizado? 16
2.1.5.1. Tráfico de Seres Humanos y Captación de Víctimas Online. 19
2.1.5.2. Explotación Sexual de Menores Online y Pornografía Infantil 21
2.1.5.3. Tráfico de Drogas. 23
2.1.5.4. Criptomonedas. 25
2.1.5.5. Blanqueo de Capitales. 26
2.1.5.6. Exportación de Armas e Impresión 3D de productos. 27
2.1.6. Crimen Organizado y Ciberdelincuencia en números. 28
2.1.6.1 Crimen Organizado. 29
2.1.6.2 Ciber Crimen. 32
2.1.7. Lucha y Prevención. 35
2.1.8. Objetivo 16: Promover sociedades justas, pacíficas e inclusivas. 41
2.2. Formulación de hipótesis: Resultados esperados. 42

3. METODOLOGÍA DE LA INVESTIGACIÓN **42**

4. ANÁLISIS DE LOS RESULTADOS **43**

5. CONCLUSIONES **44**
5.1. La amplitud y limitaciones de la investigación. 44
5.2. Futuras líneas de investigación. 47

6. REFERENCIAS BIBLIOGRÁFICAS **48**

ÍNDICE DE FIGURAS

Pág.

Figura 1 - Porcentajes de edades víctimas, según plataformas elegidas por los traficantes de seres humanos 20

Figura 2 - Promedio de número de las víctimas según la plataforma escogida por traficantes individuales o pertenecientes a grupos organizados 21

Figura 3 - Promedio global de la criminalidad, de los merados y actores criminales y de la resiliencia en los cinco continentes 29

Figura 4 - Evolución de hechos conocidos por categorías delictivas del 2016 al 2020. 32

Figura 5 - Evolución global de los hechos conocidos, esclarecidos y detenciones/investigaciones del 2016 al 2020 33

Figura 6 - Promedio de medidas implantadas contra el crimen organizado en los cinco continentes 36

ÍNDICE DE TABLAS

Pág.

Tabla 1 - Definiciones de los conceptos 5

Tabla 2 - Definiciones códigos dañinos 8

Tabla 3 - Datos delitos realizados en los cinco continentes por la delincuencia organizada 31

1. INTRODUCCIÓN

1.1. Problema de investigación.

El foco principal de la presente investigación parte de que todos los seres humanos tienen el derecho a vivir en "sociedades justas, pacificas e inclusivas", tal y como Naciones Unidas describe en el Objetivo de Desarrollo Sostenible (O.D.S.) número 16, referido a que cualquier persona proveniente de todas las partes del mundo tiene el derecho a no "tener temor a ninguna forma de violencia" (N.U, s.f., p.2a).

Aunque Naciones Unidas en su Objetivo n. 16 incluye cualquier forma de violencia, este Trabajo se enfoca al análisis de la violencia desarrollada por parte de la delincuencia organizada trasnacional. Esto se debe a que el crimen organizado ha existido durante siglos, por lo que no es un nuevo fenómeno que caracteriza solamente el siglo XXI, pero a partir de los años ochenta y noventa ha sido evidente un aumento de nuevas variantes de actuación de la delincuencia organizada transnacional (Mandel, 2011).

Además, la concentración de la investigación en el fenómeno de grupos criminales organizados es consecuencia de la manifestación de delincuencia como el factor común en diversas situaciones de la desigualdad, los conflictos, la inestabilidad política, el cambio climático, la tecnología y los mercados financieros no regulados, la corrupción y la migración forzada (Global Initiative, 2021).

Más detalladamente, el problema de investigación que se pretende estudiar en el presente Trabajo de Fin de Grado es la influencia que internet ha ejercido en la evolución de la delincuencia organizada y en la manera en que los delincuentes han modificado el modus operandi de sus delitos, mostrando un alto nivel de adaptación e incidiendo cada vez más en la sociedad (Consejo de Seguridad Nacional, 2019).

Este interés surge del protagonismo, cada vez mayor, que internet y las tecnologías más avanzadas van teniendo dentro del ámbito de la delincuencia, como destacan los documentos oficiales de Europol e Interpol, como son *IOCTA*, *SOCTA*, el *Índice global del crimen organizado* del Global Initiative y otros que vendrán analizados a lo largo del Trabajo. En específico, se destaca lo citado por Europol: "El comercio ilícito en los mercados de la

Darknet es una manifestación de la naturaleza cada vez más compleja de la delincuencia organizada transnacional en la Unión Europea" (2017, p.5).

1.2. Pregunta de investigación.

Una vez establecido el problema que se quiere investigar, la pregunta de la que parte el análisis de este Trabajo de Fin de Grado es poder entender si, efectivamente, el origen de internet, su amplitud y su continuo uso, ha podido modificar el método de desarrollo de las acciones delictivas realizadas por mano de la delincuencia organizada. Además, se querrá estudiar en qué manera internet ha llegado a ejercer su influencia en la forma delictiva desarrollada por esta tipología de delincuencia.

1.3. Objetivos.

1.3.1. Objetivo general.

La delincuencia organizada, como se ha indicado en el apartado 1.1. ha ido evolucionando durante décadas, pero en los años noventa los principales actores políticos empezaron a verse afectados por la expansión transnacional del delito y esto viene ampliado mayormente gracias al fenómeno de la globalización y de la importancia y protagonismo que internet ha tenido dentro de esta era histórica (Paoli, 2002). Bajo esta óptica, el objetivo principal del presente Trabajo de Fin de Grado se concreta en analizar las formas en que se ha desarrollado y evolucionado la delincuencia organizada y cuáles son efectivamente las ventajas que internet y las nuevas tecnologías ofrecen para la realización de los delitos y de lo que ahora se conoce por ciberdelito.

1.3.2. Objetivos específicos.

Se definen los siguientes objetivos específicos:

- Establecer los factores característicos del crimen organizado y sus características principales.
- Estudiar la situación actual de la relación entre el crimen organizado e Internet.

- Entender cómo las nuevas tecnologías han afectado la realización de los crímenes.
- Entender cómo las nuevas tecnologías han afectado las estructuras de las relaciones criminales.
- Delitos más frecuentes, cuáles han aumentado o disminuido con el utilizo de internet (ex: pornografía infantil, trata de seres humanos, blanqueo de capitales, etc.).
- Entender si la delincuencia organizada trasnacional se ha desarrollado en países más o menos desarrollados y donde han trabajado juntos o separadamente Europol e Interpol para su lucha y prevención.

1.4. Justificación: La relevancia, la originalidad y contribución científica al conocimiento académico.

El presente trabajo quiere transmitir al lector la importancia del fenómeno del crimen organizado, alertado ya por Naciones Unidas e incluido por la Estrategia de Seguridad Europea como una de las cinco principales amenazas para la seguridad mundial de las próximas décadas (De La Corte y Giménez-Salinas, 2010) y la importancia de internet en la evolución de la delincuencia organizada.

Recientemente, se ha observado el comienzo de un nuevo tipo de delincuencia organizada trasnacional, que desarrolla sus delitos en el ciberespacio, grupos criminales que aún no mantienen un "sistema estable", pero que se consideran igualmente peligrosos (Tropina, 2012). Relacionado con esta preocupación, Europol identifica en *SOCTA 2021* (*Serious and Organized Crime Threat Assessment*, p.10) las amenazas criminales a las que se enfrenta Europa, entre estas se encuentran: redes delictivas de alto riesgo, ciberataques, delitos contra las personas, drogas, etc. En el mismo texto se alerta de que, con la pandemia mundial debida a la emergencia sanitaria del Covid-19, las organizaciones criminales han demostrado una vez más su poder para operar de manera "fluida y sistemática", en un ambiente donde "los obstáculos se convierten en oportunidades criminales". Aumentando de esta manera, en los últimos años, la realización del número de ciberataques cada día más sofisticados.

Considerando la necesidad global de lograr una sociedad justa para los individuos que la componen, reduciendo todo lo posible la manifestación de cualquier tipo de violencia (N.U., s.f.b) y los estudios que la autora de este trabajo se encuentra desarrollando en el ámbito de la Criminología y la Psicología, se estima la importancia de la necesidad de analizar la situación actual del crimen organizado, con un enfoque dirigido a internet y los medios de comunicación implicados en el proceso. Todo ello debido a que cada vez se hace más evidente el daño que un mal uso de internet puede provocar en sujetos vulnerables, sobre todo niños y adolescentes.

En este sentido, solo tenemos que ver que hace tan solo unas semanas, en la población de Burjassot (Valencia) se produjo una presunta agresión sexual a dos menores de tan solo 12 años por al menos un grupo de 6 jóvenes, menores de edad, siendo que, al parecer, las menores fueron engañadas por dos de los jóvenes con quienes quedaron a través de una red social (Martínez, 2022) . Una vez más, se pone de manifiesto la potencialidad de internet en el iter criminis.

Internet se ha convertido en poco tiempo en una herramienta fundamental en la vida de las personas y supone un vehículo de relación a todos los niveles; se encuentra integrado de forma plena en nuestra sociedad y ello hace que sea necesario crear estrategias de gestión que eviten la delincuencia.

2. FUNDAMENTACIÓN TEÓRICA

2.1. Marco teórico.

En este apartado se van a analizar los aspectos principales acerca de la relación de la delincuencia organizada con las nuevas tecnologías, incluyendo un breve análisis del marco jurídico a nivel nacional e internacional. Con el fin de abarcar un estudio más específico, se mostrarán una serie de definiciones.

2.1.1. Definiciones.

Para poder entender los objetivos y el estudio en sí que se quiere realizar con el presente TFG, cabe explicar en un primer momento diversos conceptos que se desarrollan a lo largo de la revisión bibliográfica. Con esta finalidad, se ha desarrollado la siguiente tabla explicativa con las definiciones de los términos: crimen organizado, Internet, cibercrimen, tecnología de materia programable (PM) y códigos dañinos.

Tabla 1

Definiciones de los conceptos

Crimen Organizado:	
Real Academia Española (s.f.)	Distinción entre: *Crimen* "delito grave" (definición 1, a). *Organizado* "establecer o reformar algo para lograr un fin, coordinando las personas y los medios adecuados" o "poner algo en orden" (definición 1, b).
Naciones Unidas	Dentro de la Convención con contra la Delincuencia Organizada Transnacional del 2000, establece: Art. 2.a.: "Se entenderá un grupo estructurado de tres o más personas que existe durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material". Art.2.c.: "Se entenderá un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada".
Interpol (s.f.b)	Una red de negocios que actúan en diversos ámbitos delictivos, extendidos por varios países. "Es un negocio mundial con

	ganancias estimadas en miles de millones, sus negocios criminales se parecen mucho a los negocios legítimos internacionales". Se caracterizan por "modelos operativos, estrategias a largo plazo, jerarquías, e incluso alianzas estratégicas, todo con el propósito de generar un máximo de beneficios con un mínimo de riesgo".
Consejo de la Unión Europea, citado en De La Corte y Giménez-Salinas (2010, p. 23) (Europol recoge esta definición)	"Para considerar que un delito o un grupo delictivo pertenece a la categoría de la delincuencia organizada, deberá responder como mínimo a seis de las características enunciadas en la lista" cuatro de los cuales serán: 1. Colaboración de dos o más personas; 2. Para un período prolongado o indefinido (este criterio se refiere a la estabilidad y a la posible duración del grupo); 3. Sospecha de haber cometido delitos graves; 4. Movidas por la búsqueda de beneficios o de poder. Entre los indicadores optativos se encuentran: 1. Cada componente del grupo tiene tareas específicas asignadas; 2. Uso de algún mecanismo de control; 3. Actividades internacionales; 4. Empleo de violencia e intimidación; 5. Uso de estructuras comerciales y económicas; 6. Blanqueo de capitales; 7. Ejercicio de influencia sobre políticos, medios de comunicación, administración pública, autoridades judiciales o sobre la actividad económica. Estos indicadores permiten establecer con mayor claridad las características de la delincuencia organizada, con respecto a otras definiciones, aunque entra en conflicto con ellas a incluir factores como el reparto de tareas, la corrupción o la intimidación dentro de los indicadores optativos.

Código Penal español (1995)	Art. 570 bis, en el cual la define como "la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos".
Internet	
Kahn (2022)	Se define como "una arquitectura de sistemas que ha revolucionado las comunicaciones". Nacido en la década del 1970 en Estados Unidos, se ha desarrollado para modificar la mayoría de los hábitos de los seres humanos: métodos de comercio, comunicación, búsqueda de información, vídeos, etc. Siendo de esta forma accesible a cualquier individuo, en cualquier parte del mundo.
Cibercrimen	
UNODC (2020)	No existe ninguna definición aceptada a nivel global de ciberdelincuencia. Se trata de una "forma de evolución de criminalidad transnacional"
Interpol (s.f.)	"Delitos que no conocen fronteras, ni físicas ni virtuales".
Interpol (s.f.) y UNODC (2020)	Delitos realizados mediante el uso de las tecnologías de la información y comunicación, con el intento de atacar redes, datos o sistemas de, hacia cualquier víctima en todo el mundo, con especial atención a Gobiernos o negocios
Darknet	
Aked, S. et al. (2013, p. 14)	No tiene una definición oficial. Biddle, England y otros autores (2002) describieron el término en el documento "*The Darknet and the Future of Content Distribution*" como "una colección de redes y tecnologías utilizadas para compartir contenidos digitales". Se trata de "tecnologías encriptadas que permiten la participación

	anónima", mediando el uso de "una topología de red descentralizada, de igual a igual, que funciona dentro de Internet". Entre muchos ejemplos de Darknet se evidencian: Tor (The Onion Router), I2P (Invisible Internet Project) y Freenet. Para poder funcionar tiene que depender de internet, "pero sus filosofías de diseño y sus objetivos dictan que operan bajo principios fundamentalmente diferentes a los de la Clearnet" (internet normal).
Tecnología de materia programable (PM)	
Campbell et al. (2014, citado por Europol 2019)	"Ciencia, ingeniería y diseño de la materia física que tiene la capacidad de cambiar de forma y/o función (forma, densidad, módulos, conductividad, color, etc.) de forma intencionada y programable".

Nota: elaboración propia.

Tabla 2

Definiciones códigos dañinos

Códigos dañinos (Europol, s.f.)	
Botnet (Red de robots)	se compone por ordenadores que comunican a través de Internet. Vienen usados mediante un centro de comando para el envío de spam, la realización de "ataques de denegación de servicio distribuidos" (DDoS) o desarrollar otros delitos.
Rootkit	Se define como una "colección de programas" que posibilita el acceso a un ordenador o red informática, permitiendo el acceso también a los demás dispositivos conectados a la misma red.
Troyano	Se muestra como un "programa legítimo", pero su finalidad es de naturaleza maliciosa, funcional a "espiar, robar datos, eliminar archivos, expandir una botnet y realizar ataques DDoS".

Infector de archivos:	“Infecta archivos ejecutables (como .exe) sobrescribiéndolos o insertando un código infectado que los desactiva”.
Troyano de puerta trasera / acceso remoto (RAT):	Capaz de acceder a cualquier dispositivo informático de manera remota. Se instala por otra pieza de malware con la finalidad de controlar y diversas acciones como la de “monitoreo, ejecutar comandos, enviando archivos y documentos al atacante, pulsaciones de teclas de registro y tomar capturas de pantalla”.
Ransomware:	Obstácula el acceso a los dispositivos, imponiendo un rescate en línea, para que los propietarios puedan volver a tener el acceso.
Scareware	Hace pasar por un antivirus, pretendiendo escanear las amenazas al malware, pero es falso. El usuario deberá de pagar para que se elimine.
Spyware	Puede ser instalado en un ordenador sin que el propietario se dé cuenta, con la finalidad de “monitorear su actividad y transmitir la información a un tercero”.
Adware	“Muestra banners publicitarios o ventanas emergentes que incluyen código para rastrear el comportamiento del usuario en Internet”.

Nota: Elaboración propia.

2.1.2. Perspectiva general del Crimen Organizado.

En este apartado se quieren exponer una serie de características que describen el crimen organizado para proporcionar una perspectiva general que no contempla solamente el rol de dichos grupos delictivos dentro de la era digital.

En primer lugar, se quiere analizar cuál es el origen de este fenómeno delictivo. El crimen organizado nació hace algunos siglos ya, pero la delincuencia organizada de carácter trasnacional que se quiere analizar en el presente Trabajo, como se ha citado anteriormente,

empieza a desarrollarse ampliamente gracias a los cambios sociales derivados de la globalización. A partir de los años noventa, cambian de esta forma su propia estructura, que pasa de ser a centralizada a descentralizada (Mandel, 2011).

En segundo lugar, subraya cuáles son los factores de riesgo macrosociales y microsociales que llevan a una persona a dar forma a un nuevo grupo criminal organizado o a tomar parte de uno ya existente. A tal propósito, los autores De La Corte y Giménez-Salinas (2010, p. 226-252) exponen que dichos factores son de diversa naturaleza, entre estos se encuentran:

- *Las causas estructurales.* Por un lado, la crisis del Estado y por otro el "vínculo causal y directo entre la delincuencia organizada y ciertas condiciones económicas".
- *Factores económicos.* Una demanda social de determinados productos y la ausencia de la oferta legal.
- *Factores políticos e institucionales.* La corrupción.
- *Cambios sociales y tecnológicos.* Se incluyen: el cambio de demanda de servicios y productos más modernos, el intenso flujo migratorio de los seres humanos y la prostitución y las innovaciones científicas, puesto que internet puede favorecer al crimen organizado (nuevas oportunidades delictivas, mayor anonimáto, etc.).
- *Entorno criminógeno o geográfico.* Existen verdaderos "enclaves territoriales y urbanos". La presencia, por ejemplo, de recursos que favorecen los factores económicos (venta de diamantes o producción y venta de droga), atraen las organizaciones criminales. Además, la posición de un grupo organizado en un determinado país será favorecida por la demanda de la población y posibilidad que mantiene dicho país de comunicarse con otros. Dicho esto, por un lado, serán más vulnerables esas zonas caracterizadas por más de una frontera, en particular es famoso en concepto de Triple Frontera. Por otro lado, serán atractivas aquellas ciudades portuarias, situación que ha caracterizado grandes ciudades como Nueva York, Nápoles, Palermo, Hong Kong, Tokio y Estambul.
- *Anomia, privación de estatus y oportunidad delictiva.*
- *Desorganización social y ausencia de controles sociales.*
- *Asociación, diferencias y factores de aprendizaje.*

En tercer lugar, como ya se ha podido destacar de las definiciones que la comunidad internacional relaciona al concepto del crimen organizado, se entiende que su ámbito de

trabajo es extremadamente amplio y que cada grupo viene organizado y jerarquizado dependiendo de la actividad ilícita que quiere desarrollar. Por tanto, enumerar todas las formas del crimen organizado resulta una tarea difícil debido al dinamismo y a la variedad de modus operandi que caracteriza estos grupos. Es por esto que, cuando se quiere realizar un estudio de las actividades desarrolladas, se tiene que hacer referencia a los indicadores establecidos por la Unión Europea, citados en el apartado de las definiciones, puesto que proporcionan mayor facilidad a la hora de querer identificar, forma universal, las actividades de estas bandas y si realmente se podrían considerar así. (Jordá y Requena, 2013).

Por último, se considera importante analizar cuál es el perfil de una persona perteneciente a la delincuencia organizada. Para describir dicho perfil, se hace referencia a los siguientes factores característicos (Giménez-Salinas, et al. 2011, p.27-29):

- *Factores socialdemograficos*: se destacan unas características distintas con respecto al delincuente común (pero sin especificar cuáles), con una media de edad de 33 años. Por otro lado, en cuanto al sexo, la presencia del hombre es mayor en cuanto a la mujer, aunque, citando a los autores anteriores, "presenta variaciones importantes según las actividades delictivas", ya que aumenta la presencia del género femenino en el desarrollo de delitos como "tráfico de inmigrantes, la trata de personas o el tráfico de drogas de síntesis, la proporción de mujeres es superior a la de otro tipo de actividades delictivas". Además, sobre la nacionalidad de los sujetos, los flujos migratorios han facilitado la entrada de personas extranjeras en los grupos criminales organizados.
- *Factores laborales*: han querido averiguar si el trabajo, o la falta de este, es efectivamente un factor de riesgo influyente en la pertenencia de los sujetos a las redes criminales en cuestión. Resulta de este modo curioso averiguar que un 60% de los sujetos españoles de la muestra considerada, "mantiene un trabajo legal en paralelo a su actividad delictiva y un 40% no tiene trabajo legal". En consecuencia, se afirma que el puesto de trabajo no llega a ser un "factor de desistimiento de la carrera criminal" (Sampson y Laub, 2005, citado en De La Corte et al., 2011) y menos el desempleo se considera un factor facilitador para la delincuencia (Loeber et al., 2009, citado en De La Corte et al., 2011), "sino que el trabajo y la actividad ilegal son compatibles en diversas condiciones".

- *Antecedentes penales*: se destacan numerosos perfiles con una carrera delictiva corta, agrupando la muestra según tres tipos. Los delincuentes primarios, sin antecedentes, comienzan la carrera a partir de las oportunidades presentadas en la edad adulta. Antecedentes en la delincuencia común, adquiriendo experiencia para entrar en el mundo del crimen organizado. Finalmente, el grupo con antecedentes en las redes criminales organizadas, con antecedentes "más numerosos que los sujetos que sólo tienen antecedentes en la delincuencia común".

2.1.3. Perspectiva general del Ciberdelito.

> La ciberdelincuencia crece a un ritmo muy acelerado, con nuevas tendencias emergiendo continuamente. Los ciberdelincuentes se están volviendo más ágiles, explotan las nuevas tecnologías a una velocidad de vértigo, adaptan sus ataques utilizando nuevos métodos y cooperan entre sí de manera nunca vista hasta ahora. Las redes delictivas operan a escala planetaria, coordinando ataques complejos contra sus objetivos en cuestión de minutos (Interpol, s.f.a).

Europol (s.f.) afirma que esta innovación llevada a cabo por los ciberdelincuentes hace posible un aumento en el empleo de la agresividad en las acciones criminales online, como se puede ver en casos de delitos de alta tecnología, las violaciones de datos y la extorsión sexual. La ciberdelincuencia deviene un problema a escala mundial, con una mayor presencia en países donde "la infraestructura de Internet está bien desarrollada y los sistemas de pago están en línea".

En cuanto a los métodos más usados por los ciberdelincuentes, el Centro Criptológico Nacional (CCN-CERT), en el año 2019 cita los siguientes: propagación de código dañino a través de los correos electrónicos, uso de malware de criptojacking/cryptomining, refinamiento del phishing "mediante el uso de técnicas de ingeniería social y la innovación permanente para persuadir a los usuarios de la autenticidad de las estafas". Por último, la innovación en las plataformas del Ciberdelito como Servicio (*Crime as a Service*), puesto que, "además de las mejoras en los servicios ofertados", van permitiendo una mayor facilidad de uso, ampliando su popularidad y desarrollando ataques más eficientes (Europol, 2019, p. 6.)

Se añaden también amenazas delictivas como diversas tecnologías emergentes (Europol, 2019, p.6):

> Inteligencia Artificial (IA), computación cuántica, 5G, redes descentralizadas alternativas y criptomonedas, impresión 3D y biotecnología. Se espera que tengan un profundo impacto en el panorama criminal y la capacidad de las autoridades policiales para responder a las amenazas emergentes. La interrupción proviene de la convergencia entre estas nuevas tecnologías, los casos de uso y aplicaciones nunca antes vistos, y los desafíos planteados por los marcos legales y regulatorios existentes.

En el informe *Do criminals dream of electric sheep?* (2019) Europol dedica un apartado para describir la Darknet y las criptomonedas, instrumentos fundamentales para los delincuentes y "facilitadores clave" para el desarrollo de la delincuencia hoy en día. Detalladamente, la Darknet es cardinal para trabajar bajo anonimato y ocultar la ubicación de los foros, sitios web y mercados ilícitos.

No obstante el cierre de diversas plataformas de la Darknet en 2017, los usuarios siguen activos, puesto que han migrado a otras páginas web y otras plataformas descentralizadas. Dichas plataformas se caracterizan por un diseño que permite el desarrollo de acciones delictivas en pleno privacidad y anonimato, abusando de las tecnologías informáticas, evitando la detección de las fuerzas de seguridad, ya que "en una red descentralizada, ninguna entidad es responsable de operar o almacenar datos y puede ser responsabilizada por el abuso criminal de sus redes" (Europol, 2019, p. 13).

En consecuencia, hay una alta probabilidad de poder aumentar las oportunidades delictivas para la ciberdelincuencia organizada, haciendo posible una amplitud del tamaño, complejidad y confianza de dichos grupos ciberdelictivos organizados. Fundamentalmente, cita Europol, existe "un espacio considerable para las organizaciones cibercriminales de una escala sin precedentes, que supondrán un reto importante para la aplicación de la ley". (Europol 2014, p. 86).

2.1.4. Marco jurídico nacional e internacional de delincuencia organizada y del ciberdelito.

El camino que ha dado origen a la Convención de Palermo ha sido largo y difícil, debido a que no todos los Estados se encuentran en la misma situación de amenaza frente a la criminalidad organizada transnacional, puesto que existen diversas realidades nacionales con especificidades muy particulares. Además, se añade la dificultad de llegar a acuerdos internacionales, ya que algunos países no perciben, o no con la misma magnitud que otros, la amplia amenaza de la criminalidad organizada transnacional. Por ejemplo, se incluye también el hecho de que, en muchos casos, los propios Estados representan diversas formas de criminalidad cuando se refieren al crimen organizado. Todo esto conlleva a la dificultad en alcanzar acuerdos en esta materia, teniendo en cuenta realidades y legislaciones muy diferentes (Zúñiga, 2016).

Tanto a nivel local, como internacional, los acuerdos se establecen con tres principales objetivos (Zúñiga, 2016):

- Fomentar una acción coordinada por parte del Estado con el fin de tratar problemas comunes;
- Reforzar las instituciones internacionales que pueden funcionar con eficiencia;
- Desarrollar normas y procedimientos multilaterales que engloben a todos los poderes, pequeños y grandes, en un marco multilateral.

En cuanto a las legislaciones más importantes a nivel nacional e internacional, se hace referencia a:

1. El *Tratado de Ámsterdam* del año 1997, que mantiene la finalidad de establecer una "Acción Común, relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea" (Comisión Europea, 2001).
2. La *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional* del 2004, focalizada en la importancia de la expansión del fenómeno, de combatirlo y de su prevención.
3. El *Código Penal Español* de 1995, reformado en 2015, con especial referencia al artículo 570 bis, donde se expone las siguientes palabras:

> Quienes promovieren, constituyeren, organizaren, coordinaren o dirigieren una organización criminal serán castigados con la pena de prisión de cuatro a ocho años si aquélla tuviere por finalidad u objeto la comisión de delitos graves, y con la pena de prisión de tres a seis años en los demás casos; y quienes participaren activamente en la organización, formaren parte de ella o cooperaren económicamente o de cualquier otro modo con la misma serán castigados con las penas de prisión de dos a cinco años si tuviere como fin la comisión de delitos graves, y con la pena de prisión de uno a tres años en los demás casos.

Sobre la legislación que regula los delitos del cibermundo, cabe destacar que, contrariamente a la legislación sobre el crimen organizado, no se ha llegado todavía a un consenso común en la comunidad internacional, puesto que diversos países "niegan la existencia de estos delitos, alegando que son delitos tradicionales que tienen encaje en los tipos penales actuales". Por otro lado, otros afirman la necesidad de establecer nuevos tipos penales (Salom, s.f., p.136).

En 1997 el Consejo de Ministros del Consejo de Europa nombra un Comité de Expertos del Ciberespacio, compuesto por juristas, informáticos y policías, al cual podían participar también países como EE.UU, Canadá, Japón o Australia (Salom, s.f.). Con el fin de "lograr una unión más estrecha entre sus miembros", han desarrollado el Convenio sobre Ciberdelincuencia, aprobado el 23 de noviembre de 2001 (Consejo de Europa, 2001).

Este agrupa los delitos informáticos según cuatro tipos (Consejo de Europa, 2001):

a) Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.
b) Delitos por su contenido. Como son los delitos relacionados con la tenencia y distribución de contenidos de pornografía infantil en la Red.
c) Delitos informáticos. Donde se incluyen dos tipos penales: la falsificación informática y el fraude informático.
d) Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines. Se establece una remisión normativa a los convenios y tratados internacionales sobre propiedad Intelectual.

Este Convenio se ha vuelto el referente internacional en cuanto a la delincuencia informática, casi a nivel global, puesto que países de Latino América, como Venezuela, Chile y Argentina, han tomado inspiración de este texto para elaborar sus propias legislaciones (Salom, s.f.).

2.1.5. Actualidad: Crimen Organizado Informático o nueva forma de Crimen Organizado?

Europol (2014) afirma en su publicación *The Internet Organised Crime Threat Assessment (IOCTA)* que la delincuencia organizada tradicional, incluyendo los grupos de tipo mafioso, ha evolucionado su propio modus operandi utilizando los servicios disponibles en internet para desarrollar acciones delictivas teniendo acceso a herramientas más sofisticadas. Se afirma entonces una tendencia a mantener un carácter menos estructurado y más un "modelo organizativo, más transitorio, transaccional", motivada por la oferta de una plataforma más segura, donde el anonimato, el cifrado o las monedas virtuales, que Internet proporciona facilitando la compraventa de bienes y servicios ilícitos.

La falta de necesidad de una estructura jerárquica y el origen de organizaciones criminales de naturaleza más flexible viene también analizada por Jorge Linares, que ya en el año 2008, afirmaba que las relaciones personales y familiares fundamentales para los grupos organizados tradicionales, estaban siendo sustituidas por relaciones en redes sociales que van más allá de las amistades o de la familia. Define este cambio como la formación de redes sociales caracterizadas por individuos y grupos provenientes de diferentes nacionalidades, incluyendo al sector privado, con actores legales y de la política o de las finanzas, "facilitando sus operaciones". Además, el autor subraya que existe una tendencia de "operadores criminales independientes o semiindependientes", que prefieren trabajar singularmente o con pequeños grupos, relacionándose con diversas organizaciones criminales, en vez de tomar parte de un solo grupo (Mcillwain, 1999, citado en Linares, 2008, p.376).

Cabe añadir que este cambio en la flexibilidad y fluidez de los grupos criminales organizados, se debe a que, con el empleo de Internet para el desarrollo de las actividades delictivas, la comunicación, el control y la coordinación se desarrollan con un menor tiempo entre los actores y un menor coste, permitiendo un aumento del volumen y "mejorar la

calidad de la información compartida entre grupos e individuos dispersos geográficamente" (Linares, 2008, p.377).

Una vez analizado esto, resulta necesario distinguir dos fenómenos diversos: la migración de la delincuencia organizada tradicional al ciberespacio y los grupos organizados centrados en la comisión de ciberdelitos. Para el primer fenómeno, internet ya se ha demostrado que se ha convertido en un instrumento clave en la realización en delitos como "el abuso de menores, el tráfico ilícito de drogas, la trata de personas con fines de explotación sexual, la inmigración ilegal, los distintos tipos de fraude y la falsificación". De esta manera, aumentar la publicidad y colocación de productos y fomentar nuevos esquemas de lavado de dinero (Tropina, 2012).

Sin embargo, existen estudios que han demostrado que en la actualidad del crimen organizado, la explotación del ciberespacio por parte de grupos tradicionales del crimen organizado coexiste con estructuras organizadas que operan solo en redes informáticas globales y llevando al cabo solo ciberdelitos. De esta manera, dichos estudios afirman que ha nacido una nueva de evolución del crimen organizado, que se caracteriza por multitud y evolución de las estructuras y por los modernos usos de las tecnologías para la obtención de beneficios ilícitos (Tropina, 2012).

El impacto que internet ha ejercido sobre el fenómeno de la delincuencia organizada viene denunciado también por la Australian Crime Commission (ACC), reconociéndola en 2013 como la amenaza principal para la seguridad nacional, puesto que la delincuencia organizada "penetra en el entorno cibernético y lo aprovecha". Con nada más apretar un pulsante, desde cualquier parte del globo, gracias redes virtuales, mercados virtuales, moneda virtual, llega a afectar miles de australianos de manera simultánea. Esto comporta que, los delitos tradicionales del crimen organizado, como pueden ser "el tráfico de drogas, el fraude y el blanqueo de dinero, sobreviven y están surgiendo nuevas formas". De esta manera, los delincuentes pertenecientes a la delincuencia organizada, "explotan las nuevas tecnologías y se dirigen cada vez más a activos y mercados económicos clave" (ACC, 2014 p17).

En 2017, el Departamento de Seguridad Nacional español publica un análisis sobre el informe *IOCTA 2017* de Europol, evidenciando en los siguientes puntos las principales amenazas y los cambios nacientes del cibercrimen durante dicho año (Europol, 2017, citado en Departamento de Seguridad Nacional, 2017):

- El Ransomware, con operaciones a nivel planetario que han afectado de manera indiscriminada víctimas en diversas industrias, públicas y privadas. Ataques que han llegado a afectar las infraestructuras tanto que "podrían poner en peligro vidas humanas", poniendo en . Así, estos ataques han evidenciado "la conectividad, la falta de estándares de higiene digital y la falta las prácticas de seguridad pueden permitir que tal amenaza se propague rápidamente y se amplíe el vector de ataque".
- Ese mismo año, se han desarrollado los primeros ataques serios de botnets con el uso de dispositivos del Internet of Things (IoT).
- El incumplimiento de la protección de datos proporciona una continua divulgación de enormes cantidades datos, "con más de 2 mil millones de registros filtrados y relacionados con los ciudadanos de la UE, a menudo facilitados la falta de medidas de ciberseguridad".
- La Darknet sigue siendo un "facilitador transversal" para el desarrollo de distintos tipos delictivos, pudiendo acceder fácilmente al suministro de drogas de todo tipo, de armas de fuego, tráfico de datos de pago y documentos para facilitar el fraude, seres humanos y de la inmigración ilegal. Además de "compartir y distribuir material de abuso sexual infantil y para involucrarse con las víctimas potenciales, a menudo tratando de coaccionar o extorsionar sexualmente a menores vulnerables".
- En cuanto al fraude online, es el delito que mantiene el mayor impacto en los sectores minoristas, aéreo y de alojamiento, utilizados como facilitadores de otros delitos, como por ejemplo el tráfico de seres humanos o las drogas y la inmigración ilegal.
- En cambio, una amenaza cada vez más emergente son los que atacan las redes bancarias para la manipulación de tarjetas, controlar los cajeros automáticos y transferir fondos.

Desde un análisis más específico sobre los delitos llevados a cabo por la delincuencia organizada en internet, se quieren evidenciar distintos datos sobre delitos de: tráfico de seres humanos y captación de víctimas online, explotación sexual de menores online, tráfico de drogas, criptomonedas, blanqueo de capitales y la exportación de armas empresas en 3D.

2.1.5.1. Tráfico de Seres Humanos y Captación de Víctimas Online.

La trata de personas se identifica como un crimen silencioso, difícil de identificar (Almagro, 2015). La comunidad internacional reconoce la definición de este delito en el artículo 3 del Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, "que complementa la Convención de las Naciones Unidas contra la delincuencia organizada transnacional, hecho en Nueva York el 15 de noviembre de 2000". Según dicho artículo:

> Se entenderá la captación, el transporte, el traslado, la acogida o la recepción de personas recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder.

El Protocolo incluyen también todas las acciones que, en situación de vulnerabilidad, se obligan a la concesión de pagos o beneficios para obtener el consentimiento de la víctima, con fines de explotación. Se evidencia que "la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos".

La pandemia provocada por el COVID-19 ha conllevado un aumento en la digitalización de la sociedad actual. Un cambio al cual se han ido adaptando los delincuentes, también en el caso de delitos de tráfico de migrantes y de la trata de personas, modificando su forma de "reclutar, transportar y explotar a las víctimas" (Europol, 2022c).

Catherine De Bolle, directora ejecutiva de Europol, expone que dichas redes criminales explotan a las víctimas aprovechándose de aplicaciones móviles, plataformas de citas o herramientas de comunicación encriptadas para "organizar su logística y asegurar sus beneficios", llegando entonces a tener más de 800 investigaciones prioritarias en los últimos seis años, gracias a la colaboración entre los Estados miembros y Europol (Europol, 2022c).

En esta línea de pensamiento, cabe destacar el *Global Report on Trafficking in Persons* (UNODC, 2020). El estudio evidencia como internet facilita contactar a un mayor número de clientes y captar a sus víctimas mediante la técnica del *fishing* (pesca). El anonimato de las plataformas alimenta las actividades delictivas desarrolladas y dificultan la identificación del autor y del comprador. De la misma manera, los social media ayudan a los

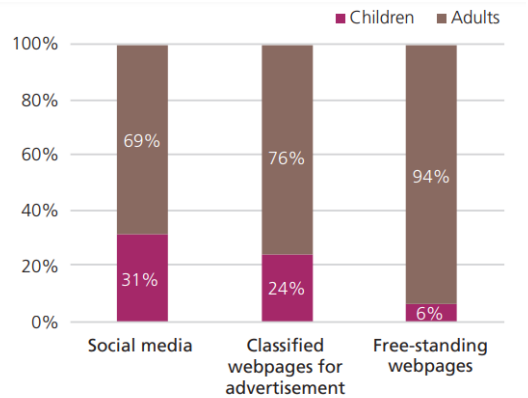
traficantes en escoger las víctimas, gracias a la información publicada por ellas mismas en plataformas como Facebook, ya que vienen seleccionadas en función de si se muestran más "susceptibles de ser cortejadas y engañadas" para su venta y/o explotación.

El análisis publicado por el informe se basa en una serie de datos judiciales, de los que se evidencia que el método de trata y el perfil de la víctima escogidos dependen de la tipología de plataforma utilizada, en particular, existen tres principales categorías de plataforma. La primera trata de las redes sociales como Facebook, Myspace, Skype, WhatsApp y Vkontakte y las víctimas escogidas suelen tener una edad más joven, "no siempre conscientes de los de los peligros de la explotación cuando son abordados por extraños en línea". La segunda incluye páginas web "clasificadas para anuncios", es decir, páginas web de contenido más genérico, donde los traficantes o los posibles clientes publican anuncios para la compra o la venta. Por último, se clasifican las páginas "independientes", originadas por los traficantes que no forman parte de dominios más grandes. Pero con el desarrollo de las redes sociales, su uso ha sido disminuido. Con estas últimas plataformas vienen mayormente captadas víctimas adultas, puesto que tienen menos riesgo de llamar la atención de los cuerpos de seguridad (UNODC, 2020).

En la siguiente figura, se pueden observar las edades de las víctimas y plataforma empleadas por los delincuentes, información sacada de los informes de los casos judiciales en los que se basa Naciones Unidas (UNODC, 2020).

Figura 1

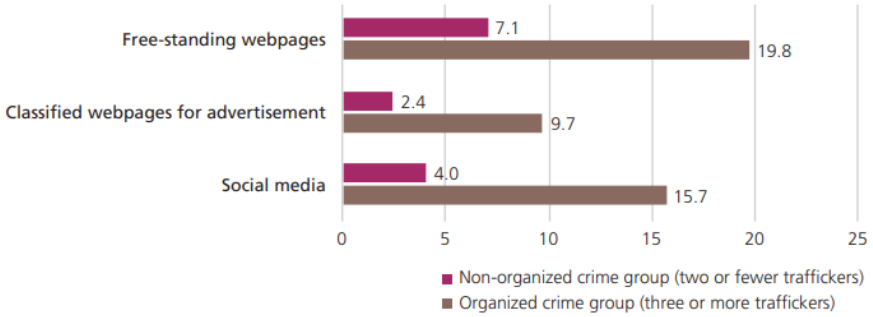
Porcentajes de edades víctimas, según plataformas elegidas por los traficantes de seres humanos



Fuente: UNODC, 2020.

Figura 2

Promedio de número de las víctimas según la plataforma escogida por traficantes individuales o pertenecientes a grupos organizados



Fuente: UNODC, 2020.

En la Figura 2 se observa el número medio de víctimas, según el uso de la plataforma online y se especifica si los traficantes pertenecían o no a organizaciones criminales organizadas (UNODC, 2020).

De todo esto se concluye que los medios de comunicación mantienen un rol fundamental desde el reclutamiento de los menores, hasta su explotación, ya que se utiliza para publicar las fotos de las víctimas y venderlas a los posibles compradores (UNODC, 2020).

Internet mantiene un rol fundamental también en el momento en que el futuro cliente quiera elegir su próxima "compra". Los adquirentes vienen atraídos por las fotos pornográficas publicadas en las redes. La trata de personas, se caracteriza así, como un sistema igual a un mercado online tradicional: el comprador observa y analiza las fotos antes de comprar y pagar el "producto" (Lillie, 2014).

2.1.5.2. Explotación Sexual de Menores Online y Pornografía Infantil

En el texto *The Internet Organised Crime Threat Assessment* de 2014, Europol afirma que la mayor parte de los delincuentes sexuales infantiles suelen realizar los delitos de manera autónoma, sin tomar parte a ninguna red criminal, actuando solos, movidos el interés

sexual hacia los niños. Ahora bien, esto no significa que sus actuaciones sean aisladas de las demás actuadas por los otros autores delictivos. De hecho, existen unos grupos que no se consideran propiamente iguales a los típicos grupos de la delincuencia organizada, sino que se organizan en una "jerarquía análoga" en las plataformas de internet, comunicando a través de redes como IRC, ICQ, grupos de noticias, foros o "redes de intercambio de archivos entre pares". El uso de internet favorece poder conocer otras personas con intereses semejantes, teniendo de esta forma acceso a grupos más grandes de niños, compartiendo cuantos más recursos (Europol, 2014).

En 2015, Naciones Unidas publica el estudio sobre los efectos de las nuevas tecnologías de la información en el Abuso y Explotación de Menores. También en este caso se definen los grupos formados por estos delincuentes como un grupo de personas que "pueden prestarse a redes de corta duración a través de grandes distancias y entre delincuentes que no tienen ninguna conexión en persona" (Naciones Unidas, 2015, p. 33-34).

Diversos grupos actúan online en el ámbito del abuso y la explotación infantil con fines de lucro, desarrollando producción y distribución del material afines a dichos ámbitos. Se destacan las siguientes zonas como los lugares base de la delincuencia organizada en el ámbito de la explotación sexual de menores: Asia, el sureste de Europa sudoriental, la Comunidad de Estados Independientes, México y Nigeria. Gracias a las tecnologías les resulta menos costoso reclutar víctimas menores de edad, comunicar con los cómplices y encontrar los clientes. Además, existen grupos organizados que ofrecen turismo sexual infantil, cobrando a los clientes online y conectar las víctimas con sus compradores a través de las fronteras. Cada vez más animan a los clientes a pagar tarifas adicionales para la grabación del abuso sexual infantil ejercido sobre los menores antes de la venta (Naciones Unidas, 2015 p. 33-34).

El Departamento de Estado de Estados Unidos publica en 2007 sobre la existencia de canales de "cibersexo", donde "los niños pueden ser abusados sexualmente por un adulto mientras las imágenes del abuso se transmiten en directo por Internet, y el acceso a la transmisión se suele comprar mediante tarjeta de crédito". Este método de abuso viene facilitado por necesitar una simple conexión a internet, un ordenador o móvil con una cámara incorporada u otro dispositivo capacitado para la realización de vídeos. Los grupos atraen los clientes con el "espectáculo en directo", puesto que permite a los espectadores de "sentirse

conectados a la actividad sexual", con la posibilidad de poder "simular una participación activa en el abuso", dictando como se tiene dirigir las acciones de las personas que aparecen en los videos mismos (citado en Naciones Unidas, 2015, p.23).

Según el artículo del Human Trafficking Search, publicado en 2014, el 80% de los sobrevividos a la trata de personas, afirman que los delincuentes muestran material pornográfico para que puedan aprender los comportamientos que tienen que cumplir. La pornografía viene utilizada como formación de las víctimas con respecto a las acciones y situaciones sexuales requeridas por el cliente.

Unas de las principales razones que justifica el empleo de la pornografía en la trata es el control psicológico, empleado también a larga distancias, que los traficantes pueden tener sobre las víctimas. Una vez que la imagen viene publicada con la cara de la persona, estará en internet para siempre, esto los delincuentes lo saben y lo emplean como forma de amenaza y chantaje. Otra razón para que pueda existir una gran relación entre la pornografía y la trata de personas es que la industria de la pornografía es fructífera. Más joven es la víctima, más beneficio financiero obtiene el traficante. Efectivamente, la industria de la pornografía infantil y la trata del sexo infantil es el sector más lucrativo de todo tipo de trata (Lillie, 2014).

2.1.5.3. Tráfico de Drogas.

El Global Initiative Against Transnational Organized Crime (Bird et al., 2020), destaca que la mayoría de los vendedores son especialistas y no ofrecen otros productos. Se necesitan menos empleados y hay menores gastos en general, por lo que la venta online conlleva más ventajas. En la Darknet, la venta adviene de manera casi igual a la venta de un producto lícito por internet: el comprador puede buscar el producto que quiere, leer las distintas reseñas de los vendedores y de lo que ofrecen, comprando el producto, pudiendo realizar transacciones en las mismas páginas web. La sustancia ilícita vendida se envía a través de sistemas de correo tanto privados como públicos y el producto se entrega en sitios anónimos, como pueden ser: "apartados de correos anónimos, cabinas automatizadas o estaciones de empaquetado" (p.8). Finalmente, en cuanto a las transacciones, resulta un alto uso de las aplicaciones de pago inteligentes o criptomonedas, destacando EcoCash, esto

porque se evita el utilizo del dinero en efectivo, limitando de esta manera que el dinero utilizado en la compraventa sea incluido como prueba en caso de arresto. Solamente, los delincuentes retienen los pagos hasta que el cliente reciba el producto.

Además, diversos autores afirman que las comunicaciones entre narcotraficantes se realizan en multitud de ocasiones con la plataforma de WhatApp, gracias a la encriptación de extremo a extremo, se vuelve un instrumento fácil y sencillo para poder dirigir estas organizaciones, reduciendo el riesgo de detención o secuestro de drogas. En particular, los vendedores publican mediante vídeos, fotos y estados en Facebook, Instagram y Snapchat o en sus "historias" sus sustancias ilícitas, detallando el precio o la cantidad que venden. Las drogas más publicadas y vendidas por estas redes suelen ser cannabis, cocaína y MDMA (Bird et al., 2020).

Bird y otros autores (2020) señalan además que las redes son utilizadas también para reclutar nuevos vendedores con el engaño de ofrecer trabajo con publicaciones en Facebook, detallando el testimonio de una persona en Nueva York que fue detenida por contestar a una de estas publicaciones y terminando ser un traficante para los cárteles de México. Esto subraya que las redes sociales permiten la creación de nuevas oportunidades de relación entre personas en cualquier parte del mundo y entre diversos grupos criminales, que se sienten más seguros a la hora de vender la droga detrás de una pantalla gracias a la calidad y facilidad de la compraventa y del anonimato, sin mantener un contacto directo entre todos los miembros que participan en el acto.

Otro aspecto del mercado de drogas en las redes sociales es que cada día aumenta el número de compradores jóvenes entre los 16 y 24 años. La estructura misma de las plataformas permiten un acceso más facilitado por parte de los jóvenes y ayuda a los traficantes en la ampliación de sus mercados, puesto que plataformas como Facebook o Instagram tienen la opción de sugerencia de amigos o los hashtags que aumentan el alcance (Bird et al., 2020). Siguiendo con el perfil del comprador, es importante decir que, según RAND (citado en Bird at al. 2020), mantiene un perfil común con el vendedor. Se cita en el escrito que corresponde en la mayoría de las veces a una persona joven, de sexo masculino, de origen de países de habla inglesa o de Europa Occidental, con una buena educación, con alta probabilidad de ser un emprendedor o con excelentes conocimientos de informática.

Finalmente, Europol (2022a) destaca el impacto que la pandemia del Covid-19, ha afectado la venta física de determinadas sustancias como, por ejemplo, la cocaína y las metanfetaminas, por lo que se observó una limitación durante el primer periodo, pero los traficantes supieron adaptarse de manera rápida a la situación, empleando "nuevos métodos" como son los "servicios de mensajería codificados, aplicaciones de medios sociales, fuentes en línea y entregas a domicilio". En particular, se destaca que en 2020, "la metanfetamina fue una de las drogas más incautadas en los envíos postales".

2.1.5.4. Criptomonedas.

Es internacionalmente reconocido que las criptomonedas son un facilitador clave del crimen porque permiten a los vendedores y clientes efectuar transacciones de forma anónima. Los delincuentes están haciendo un uso indebido cada vez mayor de las criptomonedas para financiar delitos o blanquear el dinero de actividades ilícitas. Estas actividades están siendo impulsadas cada vez más por nuevos cambios, como intercambios descentralizados que no necesitan necesariamente unos conocimientos específicos de su cliente, permitiendo a la persona "registrarse e intercambiar monedas virtuales sin revelar su verdadera identidad". El aumento del valor y empleo de las criptomonedas también ha dado lugar al origen de nuevas formas de ciberdelincuencia, "como la minería de criptomonedas, que ha aumentado significativamente desde 2017" (Europol, 2019, p 13).

Los crecientes usos delictivos de las criptomonedas de alta privacidad y las criptomonedas descentralizadas obstaculizan las autoridades encargadas de hacer cumplir la ley "para detectar y recuperar" activos delictivos y prevenir transacciones fraudulentas. El futuro de las criptomonedas y la medida en que sean empleadas por delincuentes y terroristas dependerá de factores como "el anonimato, la futura regulación, las actividades policiales y seguridad de los sistemas" (Europol, 2019 p.13).

En particular, Interpol (2020b) define el cryptoacking como "un tipo de ciberdelito que consiste en el uso de manera subrepticia de la potencia de los ordenadores para generar criptomoneda". Esto ocurre cuando un usuario instala "un programa con secuencias de comando maliciosas", permitiendo al ciberdelincuente el acceso a su dispositivo conectado a

Internet. Dicha conexión permite al delincuente utilizar programas denominados “mineros de monedas” para “generar o extraer criptodivisas”.

Por lo tanto, solo resulta necesario tener disponibles programas informáticos y ordenadores, “hurtando” solamente la potencia del ordenador de la víctima, en verdad es un delito grave a la hora de incluirse fines delictivos, “sin el conocimiento ni consentimiento de dicha víctima, en beneficio del delincuente que crea divisas de manera ilícita” (Interpol, 2020b).

2.1.5.5. Blanqueo de Capitales.

Europol afirma en *SOCTA 2021* que los grupos delictivos de alto riesgo en Europa basan sus actividades ilícitas en el blanqueo de capitales obtenidos gracias a dichas actividades. De este modo, han desarrollado un “sistema financiero subterráneo paralelo” para poder realizar las transacciones y todos los pagos, aislados de los mecanismos de supervisión del sistema financiero legal. Este modelo paralelo permite a los delincuentes una garantía fundamental: “que no se le pueda seguir el rastro de los beneficios delictivos” y que no se le pueda identificar la naturaleza de dicho dinero como parte de una economía criminal, permitiendo de esta manera mantener un alto nivel financiero a las grandes redes delictivas (Europol, 2021, p. 98).

Para la monetización de las mercancías ilegales (como son los datos e información robados) los ciberdelincuentes utilizan las denominadas "mulas de dinero". Estas mulas pueden ser de distinto tipo en el mundo del crimen organizado y cuando se relacionan con el cibercrimen, se pueden encontrar en forma de spam o falsas ofertas de trabajo, prometiendo buenas recompensas económicas. El fin es poder crear una cuenta bancaria o entrar en la cuenta personal de una persona y emplearla para la trasferencia de dinero en efectivo, en jurisdicciones distintas a la zona donde se ha efectuado el delito (Tropina, 2012).

Europol (2011, citado por Tropina, 2012) define las mulas como la parte visible del crimen organizado, por lo que confiere a las autoridades mayor facilidad a la hora de captar a los delincuentes. Cisco (2011, citado por Tropina 2012) afirma que esta situación hace que las mulas sean pocas, ya que la disponibilidad de tiempo es limitada, teniendo que abandonar

antes de que vengan descubiertas. Por lo tanto, para aumentar el número de mulas, los delincuentes han desarrollado técnicas cada vez más sofisticadas, capaces de engañar a las personas y contratarlas como mulas, las mismas personas que, muchas veces, se consideran "víctimas adicionales" de la ciberdelincuencia, puesto que pueden operar en los blanqueos sin saber lo que están realizando (Tropina, 2012).

2.1.5.6. Exportación de Armas e Impresión 3D de productos.

El tráfico ilícito de armas de fuego es considerado el delito principal dentro del tráfico ilícito de bienes y servicios, motor principal del crimen organizado, mayoritariamente en la modalidad en plataformas online (Commissione al Consiglio e al Parlamento Europeo, 2013, citado in Nunzi, 2018).

La fabricación aditiva, o mejor conocida como la impresión 3D, incluye diversos procesos necesarios a la creación de estructuras tridimensionales caracterizadas por diversos materiales, partiendo de un modelo digital. Esta tecnología empieza a tomar forma a partir de los años ochenta del siglo pasado, desarrollándose de manera masiva en los últimos años. (RAND Corporation, 2018, citado por Europol, 2019).

En consecuencia, gracias a este crecimiento aumentan las oportunidades que ofrece la impresión 3D en una amplia gama de campos, incluyendo en ámbito criminal (Europol, 2019). Entre los diversos materiales que dicha fabricación aditiva ofrece para los delincuentes se encuentran objetos como las armas de fuego 3D. Por ejemplo, esto es el caso de la construcción de armas o dispositivos de robo en cajeros automáticos (Fruehauf, Hartle y Al-Khalifa, 2016) o productos falsificados (Europol, 2015).

En 2014, la preocupación del crecimiento de esta tecnología viene dictada en el informe anual de la Australian Crime Commission (p. 31), donde se evidencia que el empleo de las nuevas tecnologías por parte de los grupos organizados, se ha visto ampliada por la impresión de armas en 3D "para un beneficio criminal en un futuro próximo". La evaluación realizada por los autores australianos se basa en que dicha explotación de las tecnologías, para producir armas en 3D, supone una baja amenaza a corto plazo para los cuerpos de

seguridad. Razón de esto es la experiencia que se necesita para llevar al cabo el desarrollo de dicho producto.

A tal propósito, Jenzen-Jones y McCollum (2017) afirman que las nuevas tecnologías permiten reinsertar en el mercado las armas ilícitas. Esto porque dichos mercados en plataformas electrónicas son gestionados solo por sujetos pertenecientes a grupos de delincuencia organizada, presentes en los territorios de la Unión Europea. Además, es evidente que algunas jurisdicciones sí que permiten la venta de piezas de armas desactivadas, lo cual permite su fácil comercialización en la Darknet y su posterior montaje (Nunzi, 2018).

Por otro lado, otra amenaza asociada indirectamente a la proliferación de la impresión 3D, es la posibilidad que los hackers lleven a cabo daños digitales enormes mediante "bloqueos informáticos, pérdida de datos, cierre de sitios web y servidores" o la interrupción de servicios importantes. Causando, por lo tanto, no solo daños en el mundo cibernético, sino también en el físico. Para comprobar dicha amenaza, un grupo de investigadores universitarios hackearon un "ordenador de sobremesa y alteró el plano digital en 3D de la hélice de un dron", provocando un mal funcionamiento de objeto, haciéndolo estrellar (Belikovestky et al., 2017, citado por Europol, 2019 p.15), confirmando, de esta manera, la amplitud de peligrosidad de dicha tecnología (Europol, 2019).

Esto significa que la posible amenaza podría aumentar si los delincuentes abusaran de la tecnología existente, pudiendo afectar a distintos ámbitos la seguridad del ciudadano, hasta adoptar la tecnología 4D, conocida como la tecnología de materia programable (PM) (Campbell et al., 2014, citado por Europol 2019). Con la PM la delincuencia podría mejorar sus beneficios, adaptándose a entornos cambiantes. Favoreciendo, entonces, un "potencial disruptivo para el comercio mundial, la geopolítica y la seguridad" (Europol, 2019, p.15).

2.1.6. Crimen Organizado y Ciberdelincuencia en números.

La finalidad del presente apartado es la de proporcionar una visión más estadística del fenómeno del crimen organizado trasnacional y de su relación con el mundo digitalizado. Si, por un lado, se expone el estudio a nivel global de las acciones realizadas por la delincuencia

organizada, por otro lado, se proporcionan datos estadísticos y noticias publicadas por Europol, Interpol y otros para entender el fenómeno del cibercrimen.

2.1.6.1. Crimen Organizado.

Toda la información que conforma este apartado proviene del *Índice global de crimen organizado* del Global Initiative, primer instrumento funcional a estudiar los datos sobre el crimen organizado y la resiliencia efectuada por los Estados ante la actividad criminal organizada, en el cual se pueden encontrar los datos del año 2020 sobre los 193 Estados miembros de la ONU (2021).

Figura 3

Promedio global de la criminalidad, de los merados y actores criminales y de la resiliencia en los cinco continentes

CONTINENTE	CRIMINALIDAD	MERCADOS CRIMINALES	ACTORES CRIMINALES	RESILIENCIA
ASIA	5,30	5,21	5,38	4,46
ÁFRICA	5,17	4,94	5,40	3,80
AMÉRICAS	5,06	4,70	5,43	4,83
EUROPA	4,48	4,21	4,76	6,23
OCEANÍA	3,07	2,98	3,16	5,46
PROMEDIO GLOBAL	**4,87**	**4,65**	**5,09**	**4,82**

Fuente: Global Initiative, 2021.

En la Figura 3 se observan los datos de los cinco continentes en cuanto al promedio de criminalidad, mercados criminales, actores criminales y la resiliencia ejercida por los países pertenecientes. La primera región que destaca es el continente asiático, con el nivel más alto de criminalidad (5,30), seguida de África (5,17), las Américas (5,06), Europa (4,48) y Oceanía (3,07).

En algunos países de Asia persisten conflictos de guerra que impulsan mercados como el tráfico de armas y la trata de personas y en otros se producen y comercian las drogas. Si bien Asia es el continente con el promedio de delincuencia más elevado, un desglose regional de los resultados muestra los datos del crimen organizado no se concentran en una zona concreta, sino que se difunden por los continentes.

Sobre África, se señala un desarrollo económico, de infraestructura y tecnológico "sin precedentes" en los últimos 20 años. Dichos sucesos han favorecido el entorno para la delincuencia organizada., puesto que ha empezado a ofrecer oportunidades en aéreas de conflictos e inestabilidad y donde las instituciones débiles son fácilmente corruptibles.

Cabe señalar que, de los resultados obtenidos en el Índice, el continente africano y asiático son los dos únicos en el mundo que presentan en 2020 datos sobre los dos "mercados ambientales (delitos contra la fauna y contra los recursos no renovables) entre sus cinco principales mercados criminales".

En cuanto al continente americano, se indica es caracterizado por uno de los "mercados de origen de drogas más prevalentes a nivel mundial" y la única región a nivel mundial "en tener un mercado de drogas (cocaína) como el más generalizado entre los 10 mercados criminales evaluados". Al proceder con la comparación entre los continentes, los estudiosos señalan que Europa es un "importante punto de tránsito y destino para una variedad de mercados y actores criminales" y donde más se generalizan los mercados de cocaína, drogas sintéticas y heroína. De esta manera, se confirma que los mercados de Asia o americanos inician el tránsito de los narcóticos, mientras que Europa es el punto principal de destino.

Finalmente, aunque Oceanía, como Europa, se caracteriza por la presencia de los mercados de drogas sintéticas, cannabis y cocaína, entre los cinco mercados criminales desarrollados, sigue siendo la región con el promedio de criminalidad más bajo en el mundo, probablemente debido a su "aislamiento geográfico y su pequeña población".

A continuación se ha recopilado una tabla con las cifras publicadas en el documento del Índice, destacando los promedios (locales y globales) de los datos sobre los cinco

continentes, en cuanto a delitos de: trata de personas, tráfico de personas, tráfico de armas, delitos contra la flora, delitos contra la fauna, delitos contra los recursos no renovables, comercio de heroína, comercio de cocaína, comercio de cannabis y comercio de drogas sintéticas.

Tabla 3

Datos delitos realizados en los cinco continentes por la delincuencia organizada

	Asia	**África**	**Américas**	**Europa**	**Oceanía**	**Nivel Global**
Trata de personas	6,63	5,93	5,19	4,94	3,82	5,58
Tráfico de personas	5,67	4,85	4,47	4,72	2,39	4,77
Tráfico de armas	5,21	5,56	5,40	4,23	2,50	4,92
Delitos contra la flora	4,32	4,73	3,94	2,75	2,54	3,88
Delitos contra la fauna	5,32	5,39	4,21	3,24	4,93	4,63
Delitos contra los recursos no renovables	5,35	5,44	4,37	3,35	2,07	4,51
Comercio de heroína	5,29	3,81	2,97	4,36	1,54	3,97
Comercio de cocaína	3,22	4,10	7,14	4,83	2,93	4,52
Comercio de cannabis	5,08	5,26	5,81	4,88	3,46	5,10
Comercio de drogas sintéticas	6,02	4,34	3,46	4,76	3,57	4,62
Mercados criminales	5,21	4,94	4,70	4,21	2,98	4,65

Nota: elaboración propia. Fuente: Global Initiative, 2021.

2.1.6.2. Ciber Crimen.

El Secretario General de Interpol, Jürgen Stock, durante la 8ª Conferencia de Interpol y Europol sobre Ciberdelincuencia en 2020, declaró que "en un mundo en el que más de 4.500 millones de personas están conectadas, más de la mitad de la humanidad corre el peligro de caer víctima de la ciberdelincuencia en cualquier momento" (Interpol, 2020a).

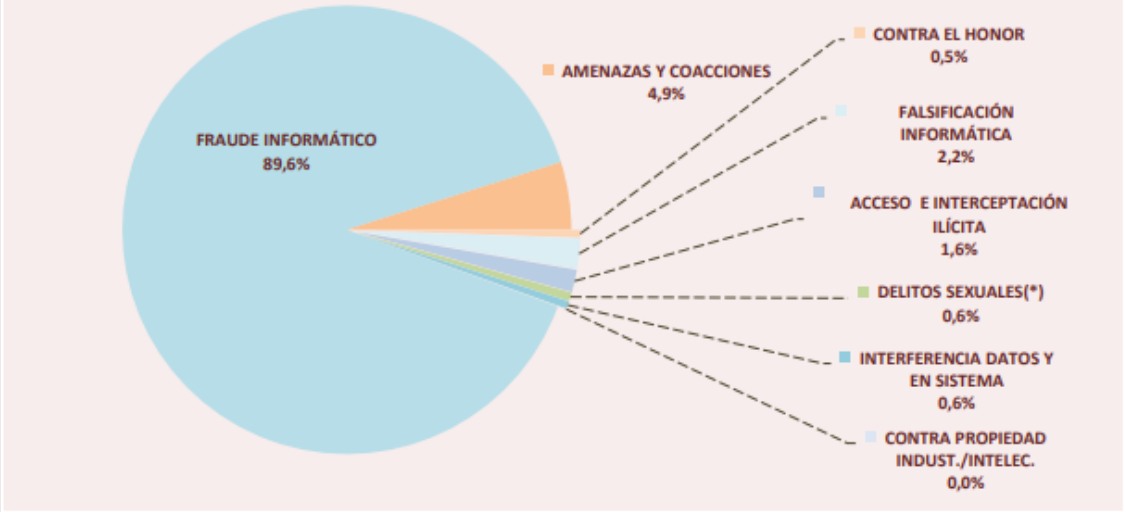
A nivel nacional, se publica en 2020 un estudio sobre la cibercriminalidad en España. De dicho estudio resultan los datos sobre la evolución de los hechos conocidos según la tipología delictiva y la evolución global de hechos conocidos, esclarecidos y detenciones / investigados entre los años 2016 y 2020. Los delitos evidenciados entran dentro de las categorías de actividades ilegales desarrolladas por el crimen organizado (Gil et al., 2020).

Figura 4

Evolución de hechos conocidos por categorías delictivas del 2016 al 2020.

HECHOS CONOCIDOS	2016	2017	2018	2019	2020
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004	4.653
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782	14.066
CONTRA EL HONOR	1.546	1.561	1.448	1.422	1.550
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197	125
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774	1.783
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275	6.289
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375	257.907
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473	1.590
Total HECHOS CONOCIDOS	**92.716**	**117.399**	**160.729**	**218.302**	**287.963**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Fuente: Gil et al., 2020.

Figura 5

Evolución global de los hechos conocidos, esclarecidos y detenciones/investigaciones del 2016 al 2020

Fuente: Gil et al., 2020.

En la Figura 4 se observa que el fraude informático es el delito informático más cometido con un total del 89,6%, hasta llegar a un total de 257.907 casos solo en el 2020. En la Figura 5 se confirma una amenaza cada vez más evidente, puesto que con los años han ido aumentando tanto los hechos conocidos, como los esclarecidos e investigados (Gil et al., 2020).

Ulterior a este estudio, se pone en manifiesto una serie de noticias publicadas por Europol, Interpol y del Ministerio del Interior Español, con la finalidad abarcar una visión general y más específicas (desde el punto de vista local y global) de algunas operaciones. En consecuencia, se observará la cantidad de amenazas que pueden surgir del ciberdelito y/o del crimen organizado transnacional operando en el mundo digitalizado.

Según *IOCTA 2020* (Europol, p. 39), en el año 2019 se llevaron al cabo un total de 10 hackeos confirmados públicamente, con un robo de criptodivisas evaluadas Con respecto a los dos años anteriores, 2017 y 2018, el número de acciones delictivas fue mayor, pero en 2018 los delincuentes pudieron llegar a robar hasta 950 millones de euros, "incluidos casi 500 millones de euros robados en la bolsa japonesa Coincheck".

Además, Europol (2020, p. 39), en el mismo documento, añade que noventa sospechosos han sido identificados "en una importante operación contra los abusos sexuales a menores en Internet". Grupos policiales de todo el mundo han podido abatir una "una red mundial de abusos a menores con vínculos en más de cuarenta países gracias a una investigación belga apoyada por Europol. El caso fue iniciado por la Policía Judicial Federal de Flandes, una vez conocida la existencia de más de nueve millones de "fotos y vídeos de

los abusos a miles de niños de todo el mundo de todo el mundo durante un registro casa" de cuatro de los detenidos.

Dichas imágenes no se habían visto nunca en circulación, por lo tanto, los investigadores belgas quisieron dar origen a la operación Gargamel junto con Europol en toda Europa y más allá, puesto que tenían la sospecha de que "estaban produciendo su propio material". Europol, gracias a dichas imágenes no solo se logró la identificación de setenta víctimas menores de edad, sino que, gracias a los mismos menores, se pudieron identificar treinta sospechosos. Además, la Policía Judicial Federal belga identificó a 60 sospechosos (24 de orgin belga) y 40 víctimas, llegando a un total de noventa sospechosos y 110 víctimas (Europol, 2020, p. 39).

Gracias a esta operación, las autoridades de más de 40 países confían lograr más detenciones y rescates de menores a nivel global, puesto que podrán examinar todas los miles de imágenes con "los paquetes de inteligencia recopilados de Europol y la información de la Policía Judicial Federal de Bélgica" (Europol, 2020, p. 39).

Por último, de las operaciones precedentemente descritas, caben destacar:

1. El Diario, 5 de julio, 2020: "Desarticulada una red de tráfico de armas para el crimen organizado".
2. Interpol, 8 de noviembre, 2021: "Una operación mundial conjunta contra el ransomware se salda con detenciones y el desmantelamiento de una red delictiva".
3. Interpol, 26 noviembre 2021: "Más de 1 000 detenciones y 27 millones de dólares interceptados en una operación masiva contra los delitos financieros".
4. Interpol, 19 de enero 2022: "Ciberestafa nigeriana: 11 sospechosos detenidos y una banda desarticulada".
5. Interpol, 14 de marzo, 2022: "Los expertos destacan los esfuerzos mundiales para combatir los abusos sexuales a menores en Internet".
6. Europol, 11 de abril 2022: "Detenida en Francia y España una banda de traficantes de personas que explotaban a víctimas sudamericanas".
7. Deutsche Welle, 22 de septiembre 2020: "Detienen a casi 180 personas en operativo mundial contra la "darknet"".

2.1.7. Lucha y Prevención.

Europol (2019) afirma que los líderes e investigadores ya están desarrollando nuevas tecnologías informáticas descentralizadas, fundamentales tanto para la lucha como para la prevención de los delitos relacionados con la ciberdelincuencia.

Naciones Unidas (2022) ha anunciado su apoyo en cuanto a la mejora de las capacidades a todos los países miembros, para "prevenir y abordar mejor la delincuencia organizada transnacional y el tráfico ilícito de personas, falsificaciones y mercancías". Esto porque su objetivo era trabajar con expertos mediante la implantación de programas mundiales y de iniciativas a escala nacional, regional y trasnacional. Principalmente, la Oficina ayuda a los Estados a desarrollar su capacidad para enjuiciar a la delincuencia organizada, brindándoles asistencia jurídica y técnica: promoviendo estrategias de prevención del delito, así como investigaciones y enjuiciamientos. Además, capacita a los organismos encargados de hacer cumplir la ley (fiscales, unidades de inteligencia financiera y otros funcionarios pertinentes), a través de diversos mecanismos para "promover y fortalecer la cooperación internacional y coordinación entre las fuerzas del orden", los profesionales judiciales y otros actores relevantes, incluyendo el uso de "redes regionales e interregionales y el desarrollo de herramientas de software y bases de datos para compartir información".

Pero debido al carácter trasnacional, tanto de los grupos criminales organizados, como de la ciberdelincuencia la falta de una legislación común a todos los países limita la investigación de ambos delitos. En particular, con lo que trata la ciberdelincuencia y si amplitud, es necesaria una cooperación eficaz para limitar las amenazas, pero la poca concienciación sobre las tecnologías y el ciberdelito en sí, dificulta la "capacidad de desplegar las estrategias, las capacidades y los programas adecuados para garantizar un uso seguro y adecuado de las TIC como facilitadores del desarrollo económico" (Naciones Unidas, 2022).

A tal propósito, Naciones Unidas (2022) determina lo siguiente:

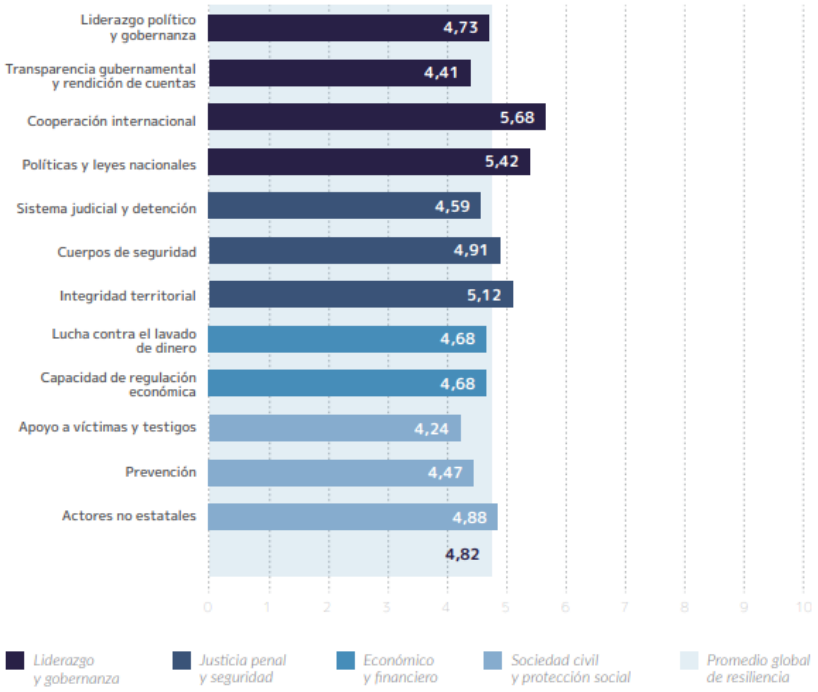
> A medida que las tecnologías digitales se hacen más accesibles, la lucha contra la ciberdelincuencia debe convertirse en una parte normal de la narrativa de la prevención del delito. Las áreas especiales de atención giran en torno a la promoción de

la ciberseguridad entre las mujeres, los niños y los jóvenes, la prevención de la explotación sexual en línea, la concienciación sobre el mercado de la red oscura y la lucha contra el uso indebido de las criptomonedas.

Relacionado con lo anterior, el Índice global del crimen organizado (Global Initiative, 2021, p.46), sostiene que el promedio global de la lucha contra al crimen organizado es igual a un 4,82.

Figura 6

Promedio de medidas implantadas contra el crimen organizado en los cinco continentes



Fuente: Global Initiative, 2021.

Los datos evidenciados en la imagen proporcionan una información general de las medidas implantadas por los países de los diversos continentes, pero indica también que, en 2020, aún no se había establecido "una solución sostenible a los impactos del crimen organizado" y que se hace cada vez más necesaria la atención e inversión económica, tecnológica y profesional para aumentar las medidas de lucha y prevención. Es decir, en el Índice se sigue sugiriendo una cooperación e intervención que no sean solo periféricas, sino que se tiene que considerar una "estrategia global general contra el crimen organizado" (Global Initiative, 2021, p.46).

En relación con la ciberseguridad, en 2020, el Consejo de la Unión Europea aprobó el establecimiento de un Centro de Competencia en Ciberseguridad para aunar "inversiones en investigación, tecnología y desarrollo industrial en ciberseguridad". Proporcionará financiación relacionada con la ciberseguridad de los programas Horizon Europe y Digital Europe y desarrollará el trabajo junto a una Red de Centros Nacionales de Coordinación de los Estados miembros. Además, pone en conjunto industrias, organizaciones académicas, investigativas y organizaciones civiles, formando así una Comunidad de Competencias en Ciberseguridad, con el objetivo de reforzar y difundir los conocimientos específicos de la materia en toda la Unión Europea (2020).

A nivel europeo, cabe analizar además la Plataforma Europea Multidisciplinar contra las Amenazas Criminales (EMPACT). Esta se considera el "instrumento emblemático de la UE para la cooperación operativa, multidisciplinar y multiinstitucional en la lucha contra la delincuencia organizada a nivel de la UE". En dicha Plataforma, Europol introduce diversas medidas como: "los controles en las fronteras exteriores, la cooperación policial, aduanera y judicial", además de "la gestión de la información, la innovación, la formación, la prevención y la dimensión exterior de la seguridad interior, así como las asociaciones entre el sector público y el privado cuando proceda" (Europol, 2022b).

En 2021, el Consejo de la Unión Europea decidió lo siguiente (Europol, 2022b):

- Permanencia del Ciclo de Políticas de la UE para el crimen organizado internacional y grave: "EMPACT 2022+ (8 de marzo de 2021) - esto también introdujo el cambio de nombre a "EMPACT", mientras que la periodicidad de cuatro años de sus pasos se mantuvo sin cambios".
- Mantenimiento de la lucha contra el crimen organizado dentro de las prioridades de EMPACT 2022-2025 y, dentro de los delitos prioritarios, se establecen: las redes delictivas de alto riesgo, los ciberataques, la trata de seres humanos, la explotación sexual infantil, el tráfico de inmigrantes, el tráfico de drogas, el fraude, los delitos económicos y financieros, los delitos contra la propiedad organizados, los delitos contra el medio ambiente y el tráfico de armas de fuego.

En España, se plantea la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (Gobierno de España, 2019), la cual precisa la importancia de la amenaza promulgada por la "aparición y evolución de nuevas actividades criminales" de la delincuencia organizada. En particular, hace el ejemplo de delitos como el fraude en el ámbito de las apuestas en línea, las nuevas modalidades de blanqueo de capitales (criptomonedas) y de los "mercados criminales gestionados a través de internet, principalmente mediante la red profunda".

Además, cabe considerar el coste económico que la delincuencia supone a la nación española, por lo tanto, la Estrategia sugiere el continuo empleo de "estrategias anticipativas para avanzar en la disminución del riesgo asociado a estos fenómenos complejos que tanto inciden en la Seguridad Nacional" y en "las pérdidas de vidas humanas, lesiones físicas y emocionales, servicios asistenciales, gastos de los procedimientos abiertos, etc" (Gobierno de España, 2019, p. 25).

Con tal propósito, en la antedicha Estrategia (Gobierno de España, 2019, p. 36) se establecen los siguientes puntos funcionales a la lucha del crimen organizado y de sus actuaciones online:

- Impulsar la respuesta normativa y la asunción de compromisos internacionales en materia de supervisión y de investigación sobre las nuevas amenazas de naturaleza económica, tales como el uso de criptomonedas para el blanqueo de capitales o el fraude de apuestas en línea mediante el amaño de competiciones deportivas.
- Incrementar las operaciones conjuntas internacionales, formando equipos conjuntos de investigación entre los jueces, fiscales y operadores públicos de seguridad relacionados exclusivamente con el blanqueo de capitales, investigaciones patrimoniales y recuperación de activos en el ámbito del crimen organizado, con intervención directa de la Oficina Europea de Lucha contra el Fraude (OLAF), Eurojust y Europol, debido a la cada vez mayor utilización por la criminalidad organizada de entramados empresariales internacionales basados en complejas metodologías de ingeniería financiera.

En la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (Gobierno de España, 2019, p.44) se alerta además sobre "el riesgo de ataques informáticos contra instituciones, personas físicas y jurídicas, a gran escala, debe ser considerado alto, en

relación con otras formas de delincuencia". Dicha preocupación ha aumentado debido al incremento tanto de los ataques cibernéticos detectados, como de la cantidad cada vez mayor de los dispositivos y medios físicos conectados a Internet, incluyendo la vulnerabilidad de la mayoría de la información sensible, como son "datos personales, sobre la salud, las finanzas, etc.– almacenada en la "nube"".

A partir de dicha preocupación en la Estrategia (Gobierno de España, 2019, p. 45) se plantea un objetivo, formado las siguientes líneas de actuación:

- Fortalecer e incitar la cooperación internacional, de manera "bilateral y multilateral, con otras regiones y países" sobre ciberdelincuencia, obstaculizando el incremento de paraísos cibernéticos.
- Aumentar el control de las criptomonedas como método de pago en las actividades criminales desarrolladas online.
- Favorecer la intervención especializada de todas las unidades investigativas comprometidas en la lucha contra el cibercrimen.
- Incrementar la cooperación en los dos sectores, público y privado, destacando los ámbitos financiero y tecnológico. Favoreciendo de esta forma la participación de personas especializadas y cualificadas del sector privado junto a los funcionarios de los cuerpos de seguridad.
- Impulsar la "adecuación de los instrumentos jurídicos que permita hacer frente a las nuevas modalidades criminales en este campo, mediante la adaptación de los procedimientos de investigación".
- Promover la lucha contra el cibercrimen junto a unidades policiales periféricas, fomentando la actuación "en las investigaciones menos complejas", además de mejorar la formación de su personal en este ámbito.

Por otro lado, sobre lo que trata la prevención del delito, se establece la siguiente información (Gobierno de España, 2019, p. 46).

Desde el punto de vista tecnológico, se pretende fortificar la colaboración con los proveedores de servicios digitales, prestadores de servicios de la sociedad de la información y comercio electrónico, además de las empresas tecnológicas, para la mejora de los sistemas de intercambios de datos, del desarrollo de acciones formativas y otros. Además, se sugiere fortalecer la seguridad del comercio en la red y de los pagos online. De esta manera se

impulsa “un estándar global seguro para las transacciones que posibilite bloqueos de pago como un medio de prevención de fraude y el intercambio de información rápido”, a nivel local y global, como puede ser en los casos de comisión de ciberdelitos en serie (las estafas masivas online).

En el plano educativo, se quiere impulsar “una cultura y conciencia de ciberseguridad, creando una narrativa propia que minimice las amenazas a las víctimas potenciales, difundida en campañas informativas, en las redes sociales y en los medios de comunicación. De esta manera, modernizar y actualizar todos aquellos planes y programas dirigidos a los centros educativos sobre la concienciación de la amenaza, además de establecer “nuevos específicos para otros sectores de población vulnerables, en centros sociales (mayores, personas sin recursos, etc.)”. También añaden la importancia de favorecer la “participación y corresponsabilización” en la difusión de la cultura y conciencia por parte de los usuarios (privados y profesionales).

En cuanto a las investigaciones, se fomenta la mejora de las acciones de inteligencia e investigación, teniendo como prioridad los ciberdelitos de alta gama, es decir, los que pueden llegar a generar más daño. Entre estos citan: fraudes, estafas y pornografía de menores online, extorsiones, violación de la intimidad de las personas, comercio ilícito de datos personales y “los ataques cibernéticos y robo de datos sensibles que afecten al normal funcionamiento de entidades públicas y privadas en diferentes ámbitos (político, económico, social, información, infraestructuras, etc.)”. En este ámbito, se añade también el incremento de las actuaciones en el ciberespacio dirigidas contra “empresarios individuales del delito” los cuales producen “continuas ciberamenazas mediante la comisión de formas de delincuencia grave, como el robo de datos, denegación de servicios, hackeos, etc., que causan alarma en la sociedad”.

Además, la Estrategia añade en cuanto a los cuerpos policiales dos cuestiones importantes. Por un lado, fortalecer la actuación policial y de las unidades especializadas en cuanto a: prevención, investigación tecnológica y análisis forense de dispositivos de almacenamiento de datos en general. Con especial atención a los delitos de pornografía de menores en la red, explotación sexual en línea, acoso, y otros modus operandi de ciberdelincuencia que afectan a colectivos vulnerables”, puesto que conllevan una alta “repercusión social y que generan sensación de inseguridad”, Por lo tanto, se quiere

favorecer “el intercambio de inteligencia para la identificación de víctimas, e incrementar las actividades preventivas de las unidades de participación ciudadana”, para reducir dicha vulnerabilidad. Por otro lado, se establece potenciar la “coordinación multidisciplinar entre administraciones e instituciones nacionales con responsabilidad en esta materia”, enfocándose en la prevención y respuesta, atendiendo además con “actuaciones bien definidas y eficaces”.

Finalmente, el Jefe del Centro Europeo para el tráfico de migrantes, Robert Crepinko, destaca el gran labor realizado por la comunidad internacional, no obstante las dificultades debidas a la rápida evolución tanto de las tecnologías, como de los grupos criminales organizados, destacando que Europol misma sigue siendo la “plataforma perfecta para promover las innovaciones de las fuerzas del orden” (Europol, 2022c).

2.1.8. Objetivo 16: Promover sociedades justas, pacíficas e inclusivas.

En la introducción del presente Trabajo se ha evidenciado que esta investigación parte del Objetivo de Desarrollo Sostenible número 16 de Naciones Unidas. Se considera necesario, entonces, explicar más detalladamente dicho objetivo.

Los Estados Miembros de las Naciones Unidas, el día 25 de septiembre del 2015, decidieron aprobar la Agenda 2030 para el Desarrollo Sostenible, adoptando unos objetivos globales con la finalidad de “proteger el planeta y mejorar las vidas y las perspectivas de las personas en todo el mundo”: los Objetivos de Desarrollo Sostenible (O.D.S.). En definitiva, se trata de “una oportunidad para que los países y sus sociedades emprendan un nuevo camino con el que mejorar la vida de todos, sin dejar a nadie atrás” (Naciones Unidas, s.f.b).

La relación de la temática tratada con el O.D.S. 16 se debe a que “las personas de todo el mundo no deben tener temor a ninguna forma de violencia” y sentirse seguras de poder confiar en “instituciones públicas eficaces e inclusivas”. Puesto que ningún país queda exento de la delincuencia, de la presencia de criminales y posibles delincuentes. Con el fin de evitar consecuencias destructivas a nivel macro y micro social, económico o sobre el bienestar y salud de los niños, es importante que la comunidad mundial tenga acceso y sepa que puede

fiarse de una justicia justa. Por lo tanto, el fin es aquel de concienciar a la población sobre "la realidad de la violencia y sobre la importancia de construir sociedades pacíficas y justas" (Naciones Unidas, s.f., p.2a).

2.2. Formulación de hipótesis: Resultados esperados.

Atendiendo a que nos encontramos ante un trabajo basado en una revisión bibliográfica, concretamente en materia de delincuencia organizada, entendemos la dificultad de formular una hipótesis a la que responder con una serie de resultados más o menos amplios. Si bien lo anterior, como ya se ha expuesto anteriormente, la pregunta que motiva la realización de este trabajo es precisamente el análisis de la situación de este tipo de delincuencia y la evolución que esta ha sufrido debido al uso de internet y a su implantación en el actual mundo globalizado.

Debido a lo expuesto, a lo largo de este trabajo se han expuesto las cuestiones principales que definen la situación del crimen organizado en la actualidad, tanto en nuestro país como en la escena internacional; se establecerán las líneas maestras que han permitido llegar a la situación actual y, posteriormente, se expondrán una serie de puntos a modo de conclusiones.

3. METODOLOGÍA DE LA INVESTIGACIÓN

El presente Trabajo de Fin de Grado se ha desarrollado mediante una metodología fundada en la técnica de revisión bibliográfica, acompañada de un análisis de la información específica. Con esta finalidad se ha recurrido a fuentes primarias y secundarias.

El estudio se ha desarrollado principalmente con la información recopilada por fuentes primarias de datos de organizaciones nacionales e internacionales como: Europol, Interpol, Consejo de Europa, el Consejo de Seguridad Nacional, Naciones Unidas, el Departamento de Seguridad Nacional, el Código Penal español, el Centro Criptológico Nacional, la Plataforma Europea Multidisciplinar contra las Amenazas Criminales y otros.

Por otro lado, en cuanto a las fuentes secundarias (todas oficialmente reconocidas), debido a la poca investigación publicada con respecto al tema protagonista de este estudio, resultan fuentes periódicas como *El País*, libros y documentos académicos de diversos estudios realizados a nivel mundial. De todo ello se han deducido los aspectos determinantes, funcionales a la generación de las conclusiones.

4. ANÁLISIS DE LOS RESULTADOS

Una vez recogidas y estudiadas las cuestiones principales que caracterizan el mundo del crimen organizado trasnacional y su modus operandi dentro del mundo de la ciberdelincuencia, se procede al análisis de los datos propuestos, con referencia al problema y pregunta de investigación que se plantean en el presente Trabajo de Fin de Grado.

Establecido lo anterior, cabe analizar si la llegada de las nuevas tecnologías (en particular de internet), ha limitado o efectivamente favorecido el desarrollo de los delitos ejecutados por el crimen organizado y/o de alguna forma lo ha modificado. Con referencia a esto, se han considerado todos los datos proporcionados por las distintas organizaciones internacionales y de sus estudios, además de las noticias publicadas casi diariamente por parte de Interpol, Europol y las demás fuentes secundarias en las que se basa el presente trabajo. Todas las fuentes consideradas alarman sobre el uso efectivo de las tecnologías como un facilitador efectivo.

Con más de 4.500 millones de personas conectadas a la red, cualquiera, en cualquier momento, puede caer víctima de los grupos criminales online. Tan solo en España: fraude informático es el delito informático más cometido, con un total del 89,6%, hasta llegar a un total de 257.907 casos solo en el 2020. En la Figura 5 se confirma una amenaza cada vez más evidente, puesto que con los años han ido aumentando tanto los hechos conocidos, como los esclarecidos e investigados.

5. CONCLUSIONES

5.1. La amplitud y limitaciones de la investigación.

El tema cardinal de esta investigación es la posibilidad lograr una sociedad donde los ciudadanos puedan sentirse seguros y protegidos, gracias al logro de una justicia igual para todos, sin algún rasgo de violencia, tal y como especifica Naciones Unidas en el O.D.S. n. 16, aún siendo conscientes de la imposibilidad de llegar a un nivel de delincuencia 0.

Relacionado con esto, se evidencia un obstáculo efectivo generado por las actividades ilícitas de la delincuencia organizada trasnacional, la cual no solo dificulta la eliminación de cualquier forma de violencia, sino que se presenta como factor común en momentos de desigualdad, conflictos, inestabilidad política, cambio climático, con la tecnología y con los mercados financieros no regulados, la corrupción y la migración forzada. De la misma forma, también la ciberdelicuencia es un obstáculo a la hora de querer lograr el O.D.S. n. 16, debido a su continuo aumento y a la capacidad de adaptación de los ciberdelincuentes con el desarrollo nuevos métodos, operando a nivel planetario.

En consecuencia, la innovación de la ciberdelincuencia favorece el empleo de la agresividad en las acciones criminales online e influye en desarrollo de las actividades de delincuencia organizada, gracias a la facilidad de apretar una tecla de cualquier instrumento tecnológico conectado a internet, de manera simultánea, favoreciendo la sobrevivencia de delitos ya tradicionalmente conocidos además de las nuevas formas delictivas.

Se confirma entonces que el modus operandi de la delincuencia organizada conocido tradicionalmente, se ha ido modificando gracias a los servicios y anonimato ofertados por las plataformas online, evolucionando, en consecuencia, su estructura, haciéndola más flexible, yendo más allá de las amistades o de la familia. Relacionado con esto se establecen dos fenómenos. Si, por un lado, existe una migración de la delincuencia organizada tradicional al ciberespacio, los cuales consideran internet como el instrumento clave en la realización de delitos específicos, por otro lado, se destaca el origen de grupos organizados centrados en la comisión de ciberdelitos, evolucionando su estructura y herramientas en la comisión de los delitos.

De este modo, se puede concluir que internet no viene únicamente usado como facilitador, sino que ha también aumentado la tipología de los delitos ejecutados por las organizaciones criminales a nivel trasnacional, como es el caso de las criptomonedas o delito informático que anteriormente a la llegada de internet no existían. Al no ser solo un instrumento facilitador gracias al empleo del engaño y del anonimato, internet podría llegar a ampliar mayormente su influencia si no se emplean los conocimientos adecuados para limitar dicha tipología delictiva. Esto conlleva consecuencias graves no exclusivamente hacia sujetos más vulnerables, sino que se incluyen cualquier persona de toda edad y escala social, generando así, una alarma social mayor, como se observa en los delitos de explotación o tráfico de menores y adultos y los delitos ligados al tráfico de drogas, criptomonedas, blanqueo de capitales, exportación de armas empresas en 3D.

Con más de 4.500 millones de personas conectadas a la red, cualquiera, en cualquier momento, puede caer víctima de los grupos criminales online. Esto significaría que, si no se hace todo lo posible para la lucha y limitación de este tipo de delincuencia, esta podría desarrollarse sin control en un mundo todavía desconocido, como es el cibermundo. Dicha posibilidad se debe a que en las conocidas plataformas descentralizadas es difícil establecer un responsable directo, aumentando así el volumen, la complejidad y confianza de los grupos ciberdelictivos organizados, aumentando cada vez más el reto de las fuerzas de seguridad para la aplicación de la ley, pero no por esto se tiene que dejar de combatir este fenómeno.

Relacionado con lo anterior, se resaltan las siguientes formas de lucha y prevención. Ante todo, cabe resaltar la Plataforma Europea Multidisciplinar contra las Amenazas Criminales (EMPACT). En particular, EMPACT 2022-2025 que establece una serie de delitos específicos prioritarios en la lucha del fenómeno: las redes delictivas de alto riesgo, los ciberataques, la trata de seres humanos, la explotación sexual infantil, el tráfico de inmigrantes, el tráfico de drogas, el fraude, los delitos económicos y financieros, los delitos contra la propiedad organizada, los delitos contra el medio ambiente y el tráfico de armas de fuego.

España también trabaja en la lucha mediante la cooperación internacional, alimentando una respuesta normativa y una adecuación de los instrumentos jurídicos para supervisionar y frenar posibles nuevas amenazas económicas (blanqueo de capitales o el fraude de apuestas en línea mediante el amaño de competiciones deportivas).

Favorece, además, la formación e intervención especializada de todos los actores que participan a la lucha, prevención y castigo de la delincuencia organizada online, con intervención directa de la Oficina Europea de Lucha contra el Fraude (OLAF), Eurojust y Europol, debido a la cada vez mayor utilización por la criminalidad organizada con complejas metodologías de ingeniería financiera. Finalmente, España impulsa una especial atención a los ciberdelitos que comportan más daño, como son: "fraudes y estafas en internet, pornografía de menores online, extorsiones, agresiones a la intimidad de las personas, comercio ilícito de datos de carácter personal y los ataques cibernéticos y robo de datos sensibles que afecten al normal funcionamiento de entidades públicas y privadas en diferentes ámbitos (político, económico, social, información, infraestructuras)".

Una vez establecido esto, se hace evidente que internet es parte de la vida de casi todo ser humano, influyendo en las acciones cuotidianas del día a día. Si a esto se le añade la relación que la delincuencia establece con internet, es clara la amenaza que conlleva, aún más, cuando se trata de delincuencia organizada trasnacional. Las estrategias proporcionadas en la presente Investigación tienen un origen muy reciente, por lo que se limita la posibilidad de proporcionar su valoración, además la legislación existente es casi nula. Pero dicha limitación no quita la importancia a la necesidad de implantar un sistema formativo, no solamente para los actores que luchan contra dicha tipología delictiva.

Debido a la posibilidad de acceder muy fácilmente a las plataformas online, tanto por parte de los criminales, como por parte de las posibles víctimas, se necesita impulsar una formación que sea para todos, con especial atención a los niños. Fomentar, por tanto, campañas y cursos formativos sobre internet, su uso y concienciar sobre la existencia de posibles amenazas, que no son lejanas y que podrían afectar cualquiera. Engaños como estafas online, delitos con criptomonedas son los que más podrían afectar en el día a día cualquier sujeto. Pero no cabe quitar importancia a concienciar los más pequeños sobre las violaciones de datos o la extorsión sexual, proporcionando entonces cursos más frecuentes de como se utiliza internet y de las posibles amenazas.

Finalmente, para lo que trata las limitaciones encontradas a la hora de elaborar el presente Trabajo, se evidencia lo siguiente:

- Internet es una herramienta relativamente reciente y aún no se conoce todo lo que puede ofertar, por lo tanto, es imposible entender de qué manera exacta va a

evolucionar el modus operandi de la delincuencia organizada trasnacional gracias a ello.

- No obstante la redacción anual de informes oficiales, como son IOCTA o SOCTA, solo en los últimos dos años se han realizado estudios efectivos como el Índice Global con los datos específicos.
- No existe una legislación bien definida a la hora de limitar la fenomenología delictiva analizada.
- No se ha podido contactar directamente con los investigadores en este ámbito/fuerzas y cuerpos de seguridad nacionales e internacionales.

5.2. Futuras líneas de investigación.

La figura del criminólogo es esencial a la hora de implantar investigaciones sobre el tema tratado en el presente Trabajo de Investigación. Detalladamente, las investigaciones futuras que se deberían de efectuar a partir de las cuestiones evidenciadas tendrían que tener una naturaleza formativa y disciplinaria. Si, por un lado, es evidente formar de manera específica las personas involucradas en la lucha contra el crimen organizado a nivel global, por otro lado, resulta un déficit a la hora de conocer los medios tecnológicos con los que este tipo de delincuencia se desarrolla.

Internet es un mundo que evoluciona cada día y es difícil seguir o anticipar las novedades que ofrece, aún más cuando se contempla dar lugar a actividades delictivas online. Es por esto que se quiere fomentar también investigaciones funcionales a la hora de poder investigar y obstaculizar la actividad ilícita online con mayor facilidad. Pero no hay que olvidarse de la formación en cuanto a la concienciación de las personas que nos rodean y de los niños y niñas que podrían caer víctima. Por lo tanto, se deben de desarrollar programas formativos para colegios, funcionales a concienciar personas de todas las edades y que desarrollan un sistema de prevención eficaz para los delitos analizados en el presente Trabajo de Fin de Grado.

6. REFERENCIAS BIBLIOGRÁFICAS

Almagro, L. (2015). Trata de Personas, la esclavitud del siglo 21. *El País*. https://elpais.com/internacional/2015/07/27/actualidad/1438033364_325813.html.

Aked, S., Bolan y Brand, M. (2013). *Determining What Characteristics Constitute a Darknet*. Australian Information Security Management Conference. Australia. p.14.

Australian Crime Commission. (2014). *Annual Report 2013-2014*. Australian Crime Commission. https://www.acic.gov.au/sites/default/files/2020-8/acc_ar_2013_14.pdf

Bird, L., Haysom, S., Hoang, T., Stanyard, J. y Walker, S. (2020). *TRANSFORMATIVE TECHNOLOGIES How digital is changing the landscape of organized crime.* Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/wp-content/uploads/2020/06/Transformative-Technologies-WEB.pdf

Kahn, R. (2022) Internet. *Britannica*. https://www.britannica.com/technology/Internet.

Centro Criptológico Nacional. (2019). *Ciberamenazas y Tendencias 2019* . Gobierno de España. https://www.ccn-cert.cni.es/en/reports/public/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html.

Comisión Europea. (2000). Prevención de la delincuencia en la Unión Europea - Reflexión sobre unas orientaciones comunes y propuestas en favor de un apoyo financiero comunitario. *EURLex*. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:52000DC0786.

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia*. Consejo de Europa. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

Consejo de la Unión Europea. (11 diciembre 2020). Nuevo Centro de Competencia en

Ciberseguridad y nueva red: acuerdo informal con el Parlamento Europeo. https://www.consilium.europa.eu/es/press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/pdf.

Consejo de Seguridad Nacional. (2019). *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023*. https://bit.ly/36YDAZL.

Convención de las naciones unidas contra la delincuencia organizada transnacional y sus protocolos. *Naciones Unidas*. 2004. https://www.unodc.org/documents/treaties/untoc/publications/toc%20convention/tocebook-s.pdf.

De La Corte, L., Giménez-Salinas, A. (2010). *Crimen.Org*. Ariel.

De La Corte, L., Giménez-Salinas, A. y Requena, L. (2011). ¿EXISTE UN PERFIL DE DELINCUENTE ORGANIZADO? Exploración a partir de una muestra española. *Revista Electrónica de Ciencia Penal y Criminología ISSN 1695-0194* http://criminet.ugr.es/recpc/13/recpc13-03.pdf.

Departamento de Seguridad Nacional. (2017). *Evaluación de Amenazas del Crimen Organizado en Internet 2017 de Europol (IOCTA)*. https://www.dsn.gob.es/es/actualidad/sala-prensa/evaluaci%C3%B3n-amenazas-del-crimen-organizado-internet-2017-europol-iocta.

Deutsche Welle. (22 de septiembre 2020). *Detienen a casi 180 personas en operativo mundial contra la "darknet"*. https://www.dw.com/es/detienen-a-casi-180-personas-en-operativo-mundial-contra-la-darknet/a-55019949.

El Diario (5 de julio, 2020). *Desarticulada una red de tráfico de armas para el crimen organizado*. https://www.eldiario.es/politica/desarticulada-una-red-de-trafico-de-armas-para-el-crimen-organizado_1_6082579.html.

Europol. (2014). *The Internet Organised Crime Threat Assessment (iOCTA)*. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/europol_iocta_/europol_iocta_en.pdf.

Europol. (2015). *Exploring tomorrow's organised crime*. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_OrgCrimeReport_web-final.pdf.

Europol. (2017). *Drugs and the darknet Perspectives for enforcement, research and policy.* https://www.europol.europa.eu/cms/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf.

Europol. (2019). *Do criminals dream of electric sheep?*. https://www.europol.europa.eu/cms/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf.

Europol. (2020). *IOCTA, 2020. Internet Organised Crime Threat Assesment.* https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf. p.39.

Europol. (2021). *Serious and Organised Crime Threat Assessment (SOCTA).* https://www.europol.europa.eu/publications-events/main-reports/socta-report.

Europol. (11 de abril 2022). *Detenida en Francia y España una banda de traficantes de personas que explotaban a víctimas sudamericanas*. https://www.europol.europa.eu/media-press/newsroom/news/human-trafficking-gang-exploiting-south-american-victims-busted-in-france-and-spain.

Europol. (2022a). *EU drug markets analyses from Europol and the EMCDDA*. https://www.europol.europa.eu/media-press/newsroom/news/2022-eu-drug-markets-analyses-europol-and-emcdda?mtm_campaign=newsletter.

Europol. (2022b). *EU Policy Cycle - EMPACT*. https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.

Europol. (23 febrero 2022c). *Migrant smugglers and human traffickers: more digital and highly adaptable.* https://www.europol.europa.eu/media-press/newsroom/news/migrant-smugglers-and-human-traffickers-more-digital-and-highly-adaptable?mtm_campaign=newsletter.

Europol. (s.f.). *Cybercrime.* https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime.

Fruehauf, J., Hartle, F y Al-Khalifa, F. (2016). 3D Printing: The Future Crime of the Present. *ISCAP*.

Gil, V., Gómez, M., Herrera D., López, J., Martínez, F., Rubio, M., Sánchez, F. y Santiago, A. (2020). Estudio sobre la Cibercriminalidad en España. Gobierno de España. http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3.

Global Initiative. (2021). *Índice global del crimen organizado*. https://ocindex.net/assets/downloads/global-ocindex-report-spanish.pdf.

Gobierno de España. (2019). *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave*.

Human Trafficking Search. (2014). *The Connection Between Sex Trafficking and Pornography.* https://humantraffickingsearch.org/the-connection-between-sex-trafficking-and-pornography/.

Instrumento de Ratificación del Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la delincuencia organizada transnacional, hecho en Nueva York el 15 de noviembre de 2000, de 11 de diciembre de 2003. *BOE*, núm. 296. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2003-22719#:~:text=trata%20de%20personas.-,3.,sectores%20de%20la%20sociedad%20civil.

Interpol. (6 de octubre de 2020a). *8ª Conferencia de INTERPOL y Europol sobre Ciberdelincuencia: "Media humanidad está en peligro"*. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/8a-Conferencia-de-INTERPOL-y-Europol-sobre-Ciberdelincuencia-Media-humanidad-esta-en-peligro .

Interpol. (2020b). *Cryptojacking*. https://www.interpol.int/es/Delitos/Ciberdelincuencia/Cryptojacking.

Interpol. (8 de noviembre, 2021). *Una operación mundial conjunta contra el ransomware se salda con detenciones y el desmantelamiento de una red*. delictiva. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2021/Una-operacion-mundial-conjunta-contra-el-ransomware-se-salda-con-detenciones-y-el-desmantelamiento-de-una-red-delictiva.

Interpol. (26 noviembre 2021). *Más de 1 000 detenciones y 27 millones de dólares interceptados en una operación masiva contra los delitos financieros*. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2021/Mas-de-1-000-detenciones-y-27-millones-de-dolares-interceptados-en-una-operacion-masiva-contra-los-delitos-financieros.

Interpol. (19 de enero 2022). *Ciberestafa nigeriana: 11 sospechosos detenidos y una banda desarticulada*. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/Ciberestafa-nigeriana-11-sospechosos-detenidos-y-una-banda-desarticulada

Interpol. (14 de marzo, 2022). *Los expertos destacan los esfuerzos mundiales para combatir los abusos sexuales a menores en Internet*. https://www.interpol.int/en/News-and-Events/News/2022/Experts-highlight-global-efforts-to-combat-online-child-sexual-abuse.

Interpol. (s.f.a) *Ciberdelincuencia*. https://www.interpol.int/es/Delitos/Ciberdelincuencia#:~:text=La%20ciberdelincuencia%20crece%20a%20un,manera%20nunca%20vista%20hasta%20ahora.

Interpol. (s.f.b) *Delincuencia Organizada.*

https://www.interpol.int/es/Delitos/Delincuencia-organizada.

Jenzen-Jones, N. y McCollum, I. (2017). Web Trafficking Analysing the Online Trade of Small Arms and Light Weapons in Libya . *Small Arms Survey, Graduate Institute of International and Development Studies*. Geneva. https://www.smallarmssurvey.org/sites/default/files/resources/SAS-SANA-WP26-Libya-web-trafficking.pdf.

Jordá, C. y Requena, L. (2013). ¿Cómo se organizan los grupos criminales según su actividad delictiva principal? Descripción desde una muestra española. *Criminalidad*.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *BOE*, núm. 281, de 24 de noviembre de 1995.

Lillie, M. (2014). *The Connection Between Sex Trafficking and Pornography.* Human Trafficking Search. https://humantraffickingsearch.org/the-connection-between-sex-trafficking-and-pornography/.

Linares, J. (2008). Redes criminales transnacionales: Principal amenaza para la seguridad internacional en la posguerra fría. *Criminalidad*. http://www.scielo.org.co/pdf/crim/v50n1/v50n1a12.pdf .

Mandel, R. (2011). *Dark Logic*. Standford University, California.

Martínez, J. (2022). La Policía detiene a cinco menores por la agresión sexual que sufrieron dos niñas de 12 y 13 años en Burjassot. *Las Provincias*. https://www.lasprovincias.es/sucesos/agresion-sexual-burjassot-20220518092950-nt.html?ref=https%3A%2F%2Fwww.google.com%2F.

Naciones Unidas. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*. https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf. p33-34.

Naciones Unidas. (2022). COMBATING TRANSNATIONAL ORGANIZED CRIME. https://www.unodc.org/southasia/en/topics/frontpage/2009/combating-transnational-organised-crime.html.

Naciones Unidas. (s.f.a). Paz, justicia e instituciones sólidas: POR QUÉ ES IMPORTANTE. https://www.un.org/sustainabledevelopment/es/wp-content/uploads/sites/3/2017/01/Goal_16_Spanish.pdf.

Naciones Unidas. (s.f.b). *17 objetivos para transformar nuestro mundo*. https://www.un.org/sustainabledevelopment/es/.

Nunzi, A. (2018). EUROPOL E IL CONTRASTO DEL COMMERCIO INFORMATICO ILLEGALE DELLE ARMI. *Cross.* https://riviste.unimi.it/index.php/cross/article/view/10457/pdf.

Paoli, L. (2002). The paradoxes of organized crime. *Crime, Law & Social Change.*

UNODC. (2020). *Global Report on Trafficking in Persons 2020*. Naciones Unidas. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf.

Real Academia Española. (s.f.a). Crimen. En *Diccionario de la lengua española*. https://dle.rae.es/crimen.

Real Academia Española. (s.f.b). Organizar. En *Diccionario de la lengua española*. https://dle.rae.es/organizar#RBn9hqd.

Salom, J. (s.f.). El ciberespacio y el crimen organizado. *Dialnet*.

Tropina, T. (2012). The Evolving Structure of Online Criminality. *Uecrim.* https://www.corteidh.or.cr/tablas/r15111.pdf.

Zúñiga, L. (2016). El concepto de criminalidad organizada transnacional: problemas y

propuestas. *Dialnet*. https://dialnet.unirioja.es/descarga/articulo/5627154.pdf.