LA INVESTIGACIÓN A TRAVÉS DE DEEP WEB Y DARK WEB: UN ESTUDIO EXPLORATORIO EMPÍRICO

CARMEN SÁNCHEZ PÉREZ

CONSULTORA DE CIBERSEGURIDAD Y COLABORADORA DE LA UNIVERSIDAD CAMILO JOSÉ CELA

CARMEN JORDÁ SANZ

PROFESORA DEL DEPARTAMENTO DE CRIMINOLOGÍA Y SEGURIDAD DE LA UNIVERSIDAD CAMILO JOSÉ CELA

Fecha de recepción: 12/03/2021. Fecha de aceptación: 04/06/2021

RESUMEN

Sin duda, internet ha transformado nuestras rutinas digitalizando conductas, incluidas las constitutivas de delitos. Pero existen espacios específicos que ofrecen ventajas especiales para la comisión de delitos, tal es el caso de la Deep Web y la Dark Web. Este escenario especialmente anonimizado supone un auténtico reto global en términos de persecución policial. Este estudio exploratorio pretende identificar las características principales de las investigaciones policiales de los delitos cometidos en la Deep Web y la Dark Web a partir del estudio de sentencias españolas (n=44): conocer cómo son los delitos a los que se enfrentan nuestras FCSE, cuál es el resultado de la investigación y qué elementos procesales son clave en la persecución de estos delitos son los principales objetivos del presente análisis.

Palabras clave: Deep Web, Dark Web, ciberdelitos, sentencias judiciales.

ABSTRACT

The internet has undoubtedly transformed our routines by digitising behaviour, including criminal behaviour. But there are specific spaces that offer advantages for the commission of crimes, such as the Deep Web and the Dark Web. This particularly anonymised scenario poses a real global challenge in terms of law enforcement. This exploratory study aims to identify the main characteristics of police investigations of crimes committed on the Deep Web and the Dark Web based on the study of Spanish judgments (n=44): what are the crimes faced by our police forces, what is the outcome of the investigation and what procedural elements are key in the prosecution of these crimes are the main goals of this analysis.

Keywords: Deep Web, Dark Web, cybercrimes, court sentences.

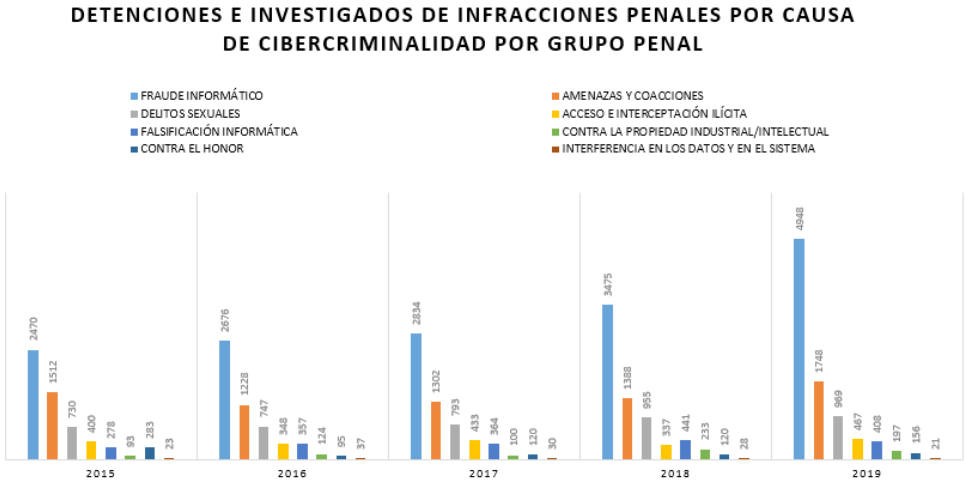
1. MARCO TEÓRICO

A modo de inicio en la materia objeto de estudio del presente trabajo, será necesario abordar una serie de conceptos y elementos primordiales que permitan asentar unas

bases teóricas estables mínimas; esto incluye constatar superficialmente la evidente migración delictiva del entorno físico al virtual, la conceptualización básica de la Deep Web y la Dark Web y la identificación de los fenómenos criminológicos asociados a ellas[1] dadas sus claras ventajas de uso.

1.1. CONCEPTO DE CIBERDELINCUENCIA

El desarrollo de las Tecnologías de la Información y las Comunicaciones, en adelante TIC, ha trasladado muchas de nuestras rutinas al plano digital; y ello ha llevado inevitablemente aparejado el aumento de delitos a través de la red, pues los delincuentes han incorporado las herramientas que estas ofrecen a su modus operandi. Una evidencia de ello es la identificación de los riesgos tecnológicos como una de las mayores preocupaciones sociales (WEF, 2019, 2020), al mismo tiempo que ponen de manifiesto el déficit de gobernanza tecnológica existente actualmente, por tanto, cabe considerarlo como una tendencia al alza. En este sentido, el número de tipologías delictivas perpetradas a través de la red ha aumentado de forma exponencial, siempre por delante de la legislación existente, como es normal en la materia jurídica, si bien en este ámbito la diferencia entre la conducta y el nacimiento de la ley es acuciante. Esto está ocasionado por la naturaleza de la ciencia informática en sí, caracterizada por ser una disciplina en constante evolución (Espinosa, 2019; Barrio, 2017).



Gráfica 1 Detenciones e investigados de infracciones penales relacionadas con cibercriminalidad por grupo penal (2015-2019). Fuente: Ministerio del Interior.

Para ilustrar el incremento de delitos informáticos mencionado, en la gráfica se pone de manifiesto el impacto que las TIC han supuesto en la evolución de la tasa de criminalidad española en base a los datos aportados por el Ministerio del Interior. Se ha tenido en cuenta el periodo comprendido entre 2019, último año con datos disponibles, hasta 2015, año en el que fueron incorporados los datos de todas las comunidades, ya que anteriormente no se disponía de los datos de la Ertzaintza ni de

1 En el presente estudio no se pretende de ninguna manera criminalizar estas fórmulas de navegación, pero sí se asume que una mayor anonimización, por ejemplo, supone un factor de atracción para determinadas actividades delictivas; lo cual no viene a significar en ningún caso que el empleo de Deep Web o Dark Web se haga exclusivamente con fines delictivos, pues aporta también, por continuar con el ejemplo, una mayor privacidad al usuario, ventaja absolutamente respetable.

los Mosos d'Esquadra. En este sentido, cabe destacar el número de Detenciones e investigados de infracciones penales relacionadas con cibercriminalidad desglosado por grupo penal durante el periodo comprendido entre 2015 y 2019, ambos inclusive.

Para abordar esta problemática los expertos en la materia establecieron el término delito informático, derivado de la denominación anglosajona *computer crime* y acuñado por primera vez en los años 80 por varios autores (Espinosa, 2019; Barrio, 2017). El concepto de "delito informático" es bastante amplio y contempla principalmente dos vertientes. Por un lado, las amenazas sobre bienes jurídicos tradicionales que han incorporado el uso de las nuevas tecnologías a su evolución y, por otro, aquellos que atentan sobre las tecnologías propiamente dichas y que amenazan contra el correcto funcionamiento de estas, circunstancia de la cual derivan los riesgos asociados. En este sentido, es posible enumerar algunas de las tipologías delictivas clásicas que en mayor medida han incorporado el uso de las TIC en su comisión; fraude, terrorismo, suplantación de identidad, pornografía infantil o delitos contra la salud pública entre otros. De otro lado, y para facilitar el conocimiento de esta nueva vertiente delictual, se mencionan tipologías como intrusiones no autorizadas a sistemas o ataques de denegación de servicio (DoS). Por su parte, persiguiendo el fin de lograr abordar la ciberdelincuencia de una manera efectiva, el Convenio sobre la Ciberdelincuencia (2001) establece una serie de tipologías delictivas que deberán ser abordadas por las legislaciones vigentes en los diferentes países miembros del Consejo de Europa.

Aparejado a este ámbito nació el concepto de ciberseguridad, que trata de abordar la necesidad de brindar la seguridad requerida a las TIC (Espinosa, 2019). Sin embargo, resulta un reto especialmente difícil para las legislaciones de los países por ser una fenomenología que abarca conductas de carácter transnacional principalmente, siendo singularmente complejo establecer el lugar de comisión del delito o, cuanto menos, establecer una trazabilidad fiable, lo que implica coordinación internacional en materia de jurisdicción penal (Barrio, 2017) y entorpece las labores de detección e investigación. En este sentido, en el año 2001 en Budapest, el Consejo de Europa elaboró el Convenio sobre la Ciberdelincuencia (CETS No.185), siendo este el primer tratado de carácter internacional, posteriormente ratificado en 2010, cuyo objetivo primordial es "aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional" (Consejo de Europa, 2001).

Asimismo, cabe destacar la figura del agente encubierto cibernético, basado en la figura del agente encubierto contemplada en el artículo 282 LECrim que, en el año 2015, con el objetivo de ampliar el campo de actuación, derivó en la creación del agente encubierto cibernético recogida en los apartados 6 y 7 del artículo 282 bis LECrim, por la que se regula la atribución de una "identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos" previstos e, incluso, contempla la posibilidad de "intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido", todo ello con el fin de lograr la identificación tanto de los archivos como de los autores. En este sentido, la figura del agente encubierto cibernético nace como una línea de acción que pretende abordar el objetivo específico tercero de la Estrategia de Ciberseguridad Nacional de 2013 de "potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio

respecto del ámbito judicial y policial", al igual que pretende dar cabida al tercer eje de actuación previsto en la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023, mediante la cual se pretende "intensificar las acciones contra la venta de drogas online y su distribución, mejorando el control de la web profunda y las empresas de mensajería, así como potenciar el uso del agente encubierto informático en la red" (Ruiz, 2021).

Si bien no fue hasta 2015 que se dio cobertura legal a esta figura de uso profuso en la investigación de la ciberdelincuencia, existen algunas referencias a su empleo por parte de las Fuerzas y Cuerpos de Seguridad del Estado avaladas por la jurisprudencia. "Así en la STS 236/2008, de 9 de mayo, (Ponente: Excm. Sr. Don José Ramón Soriano Soriano), señala que los rastreos utilizados por el equipo de delitos telemáticos de la Guardia Civil en internet sin resolución judicial mediante, en la cual se accedió a los hash de archivos que contenían pornografía infantil, se encontraba dentro de las competencias propias de la Policía Judicial en relación con la prevención del delito" (Ruiz, 2021, p.33).

Teniendo en cuenta el brevísimo repaso al actual contexto en cuanto a ciberdelincuencia se trata, es pertinente realizar una sucinta aproximación teórica al ámbito o escenario donde ocurren los delitos objeto de estudio, esto es, Deep Web y Dark Web.

1.2. APROXIMACIÓN TEÓRICA A LOS CONCEPTOS CLEARNET, DEEP WEB Y DARK WEB

Tal y como se ha expuesto anteriormente, la ciberdelincuencia contempla un amplio número de tipologías delictivas (Espinosa, 2019) por ello, dada la amplitud, este trabajo se centrará en aquellas que transcurren o para cuya perpetración es necesario acudir a Deep Web o Dark Web, por lo que resulta conveniente realizar una aproximación teórica a estos conceptos.

En primer lugar, con el propósito de explicar brevemente el esquema de internet, se realizará una aproximación a través de la metáfora del iceberg (Bergman, 2001), no exenta de controversias en la materia. De acuerdo con lo expuesto por esta amenaza, internet estaría compuesta a rasgos generales por tres particiones en cuanto a perceptibilidad se refiere. En este sentido, y entendiendo Internet como una gran infraestructura de red que alberga y conecta entre si a millones de sistemas a nivel global, permitiendo las conexiones entre estos sistemas, siempre y cuando cuenten con una conexión a internet, cabe presentar el concepto de *clearnet* (Chertoff & Simon, 2015) que abarca la superficie o parte visible, siendo esta el área de internet comúnmente utilizada y conocida por los usuarios. Si bien esto tan solo sería una mínima parte de internet, existe otra parte, que se estima es 500 veces mayor (He, Patel, Zhang & Chang, 2007) que la web visible a la que los usuarios tienen acceso a través de motores de búsqueda que indexan contenido estático, conocida como Deep Web y Dark Web, las cuales se abordan en lo sucesivo (Chertoff & Simon, 2015).

Antes de profundizar en estos términos de forma concreta, conviene explicar cómo funcionan los motores de búsqueda tradicionales, tales como Google, Yahoo!, Bing, entre otros. Un motor de búsqueda, o también denominado Search Engine, es un sistema informático que utiliza rastreadores o indexadores, referidos tradicionalmente como *crawlers*, para ubicar archivos o sitios web disponibles en internet, de manera que permiten

establecer una especie de índice que facilita su búsqueda. Aunque existen diversos tipos, todos ellos tienen en común que disponen de un determinado número de sitios web estáticos indexados a los que tienen acceso. Estos motores de búsqueda cuentan con una gran limitación y es que dependen de una serie de requisitos para poder registrar los sitios web, tales como ser reportados directamente desde los autores de los sitios web o bien porque son rastreados por sus *crawlers* a partir de enlaces de hipertexto que, a su vez, conducen a otros enlaces. Es, ciertamente, esta limitación la que marca la diferencia entre *clearnet* y Deep Web, abarcando esta última todo sitio web disponible pero que no es indexado por los motores de búsqueda tradicionales, por lo que su accesibilidad se ve, cuanto menos, limitada. Si bien, el hecho de que la accesibilidad se vea dificultada y, por ende, no sea posible tener una visión real de la envergadura de lo que la Deep Web abarca, tan solo pone de manifiesto que esta se extiende en realidad a unos confines mucho mayores de lo que los motores de búsqueda habituales son capaces de albergar. Según un estudio realizado veinte años atrás por Michael K. Bergman (2001), al que se le atribuye la creación del término, Deep Web sería 500 veces más grande que la Web superficial. De este modo, teniendo en cuenta el desarrollo exponencial de Internet desde entonces, se estima que esta cifra se ha visto incrementada hasta aproximadamente el 90% (GL, 2018).

No obstante, las características de la Deep Web anteriormente expuestas no implican que necesariamente todo lo que se escapa a los motores de búsqueda tradicionales implique una denotación ilegal. En su mayoría está compuesta por sitios web restringidos por ser, por ejemplo, de pago, por tratase de bases de datos o archivos empresariales protegidos alojados en la nube, o para cuyo acceso es necesario el uso de servidores proxy o VPN (GL, 2018).

Ahora bien, existe una parte de la Deep Web, conocida como Dark Web que cuenta con una característica que la diferencia de lo anterior y es la capacidad de anonimización que ofrece. El término Dark Web acapara la parte de la Deep Web inaccesible a través de los motores de búsqueda tradicionales, cuyo acceso tan solo es posible a través de un software específico, que incluye técnicas de cifrado que enmascaran las direcciones IP en aras de garantizar la privacidad y evitar la monitorización (Chertoff & Simon, 2015; Gehl, 2014). Mientras que la Deep Web abarca el 90% de Internet, se estima que la Dark Web tan solo supone el 0,1% de esta (GL, 2018).

El contenido disponible en Dark Web se encuentra alojado en lo que se conoce como Darknet, una red a la que solo es posible acceder a través de un software específico. Los más populares son la red TOR, i2p, Freenet o ZeroNet, entre otras. De esta forma, el término Darknet hace referencia a cada una de las redes mencionadas anteriormente, mientras que Dark Web sería el concepto general que incluye a todas estas.

Teniendo en cuenta su uso extendido entre los usuarios, se explicará de forma concisa cómo funciona una de las Darknets más populares. TOR, o The Onion Router, facilita el acceso de forma anónima a sitios.*onion* empleando un sistema de cifrado que hace prácticamente imposible rastrear tanto a los visitantes como a los anfitriones de estos sitios web[2].

2 En su sitio web oficial, el Proyecto TOR se define a sí mismo como “una red conformada por un grupo de servidores operados por voluntarios que permite a las personas mejorar su privacidad y seguridad en Internet. Los usuarios de TOR emplean esta red conectándose a través de una serie de túneles virtuales en lugar de hacer una conexión directa, lo que permite que tanto las organizaciones como las personas compartan información a través de redes públicas sin comprometer su privacidad”. Por

Como bien reconocen sus propios desarrolladores, la anonimización ofrecida por el proyecto TOR presenta una contrapartida, y es que, al igual que otorga garantías en aras de comunicación segura a aquellos que lo requieren, también ofrece a personas criminalmente motivadas una serie de elementos que hacen más factible la comisión de actos delictivos, por lo que su empleo resulta una práctica ampliamente extendida entre delincuentes. De este modo, a fin de abordar la problemática objeto de estudio, se realizará una breve revisión teórica con el propósito de identificar las principales fenomenologías delictivas vinculadas a Deep Web y Dark Web de manera que sirva como sustento de la investigación empírica sobre esta materia.

1.3. FENOMENOLOGÍA DELICTUAL ASOCIADA A DEEP WEB Y DARK WEB

Aunque en un primer acercamiento pudiese parecer todo lo contrario y, a priori, sea susceptible de solaparse con las bases del presente trabajo, Deep Web y Dark Web no son sinónimos de delincuencia per se. Como se incluye con anterioridad, las premisas bajo las que se constituyen proyectos similares a TOR son las de brindar al usuario la privacidad necesaria para explorar Internet y así promover los derechos humanos, tal y como se expone en el punto anterior. Ahora bien, es innegable que resulta un medio óptimo para la perpetración de actos delictivos (Lovejoy, 2020), tales como:

- Delitos contra el patrimonio y contra el orden socioeconómico (Barrera, 2019; Díaz, 2019; Europol, 2020).
- Delitos contra la salud pública (Díaz, 2019).
- Delitos de organizaciones y grupos terroristas (Europol, 2020; Lovejoy, 2020).
- Pedofilia (Requião y otros, 2020).
- Prostitución y explotación sexual (Díaz, 2019).
- Tráfico de armas (Cámara, 2020).

En este sentido, cabe señalar que Deep Web y Dark Web involucran en gran medida la comisión de hechos delictivos, siendo principalmente promovido a través de redes de contacto (Requião, y otros, 2020; Europol, 2019). Esto se refiere a que las Darknets están principalmente organizadas en foros, que es donde transcurre la mayor parte de la actividad. En muchos de los casos, estos foros son de carácter cerrado y son exigidos una serie de requisitos a los usuarios para poder acceder al contenido que incluyen, sobre todo en aquellos delitos que involucran abusos infantiles y terrorismo. En otros casos, son foros en los que tan solo es necesario registrarse, más en los fenómenos criminales que involucran el tráfico de armas, delitos contra la salud pública y delitos contra el patrimonio y contra el orden socioeconómico (Lovejoy, 2020). En cualquier caso, variará pero, por lo general, cuanto más grave sea el delito

su parte, el proyecto TOR fundamenta su desarrollo en la necesidad de brindar la libertad y privacidad necesarias al usuario, pretendiendo servir a activistas, medios de comunicación y militares, entre otros (Gehl, 2014), ya que “en cuanto están dispuestos a quebrantar la ley, los criminales ya pueden hacer muchas más cosas malas de las que pueden llegar a hacer en base a la privacidad ofrecida por TOR”; por lo que pretende, “brindar protección a la gente común que quiere seguir la ley” para que así esta posibilidad no quede únicamente disponible para criminales.

perpetrado a través de Deep Web o Dark Web mayores protecciones tratarán de auto brindarse los usuarios implicados. Teniendo en cuenta lo anterior, y a efectos de definir la intervención de la figura del agente encubierto cibernético anteriormente descrita, resulta necesario aludir a la diferencia existente entre lo que es considerado "canal de comunicación cerrado" y "canal de comunicación abierto", pues la LO 13/2015 en su exposición de motivos determina que "en los canales abiertos, por su propia naturaleza no es necesaria (autorización judicial)". Así, de acuerdo con Valverde (2016), la diferencia reside en "la participación activa y voluntaria del interlocutor al consentir la admisión en su círculo de contactos a quien pretende intervenir en dicho canal, (…) consecuentemente se considerarán canales cerrados aquellos que sí precisen que el sospechoso activamente autorice o consienta la inclusión del perfil del agente investigador entre sus contactos" (Ruiz, 2021, p.41).

En adición a lo anterior, cabe mencionar que el empleo de criptografía en las comunicaciones de cibercriminales resulta una tendencia a la alza y uno de los aspectos más destacados según el informe anual de Europol sobre el Análisis del crimen organizado en internet (IOCTA), en el que se recogen las principales amenazas y tendencias relacionadas con el cibercrimen en 2020, año especialmente relevante en este ámbito, en tanto ha supuesto una evolución del modus operandi de cibercriminales, adaptándose a las circunstancias derivadas de la crisis suscitada por la pandemia COVID-19. De forma concreta, el informe IOCTA 2020 contempla el uso de Dark Web en términos criminales como una sección individual. En esta sección se hace referencia al contenido esencialmente volátil de los mercados que operan a través de Dark Web, sin que haya llegado a destacar ninguno de ellos tras los notables esfuerzos dedicados a la interrupción de la actividad de muchos de estos mercados en 2019, circunstancia que evidencia la efectividad que la cooperación supone en esta materia. Otro de los aspectos puestos en el foco en el informe de IOCTA 2020 ha sido el incremento de operaciones con criptomonedas, lo que resulta realmente preocupante, tanto para el ámbito financiero en sí mismo como para el aspecto más puramente criminal, ya que permite realizar intercambios sin que sea posible establecer una correcta trazabilidad. En este sentido, cabe resaltar que este informe pone de manifiesto la constante permutabilidad del cibercrimen y privacidad aparejada como uno de los principales retos a los que se enfrentan las Fuerzas y Cuerpos de Seguridad.

A este respecto, tal y como pone de manifiesto el informe de IOCTA 2020, las legislaciones de los diferentes países, así como sus FCSE se han visto obligadas a enmendar los instrumentos empleados en la lucha contra el cibercrimen, en general, y aquella fenomenología delictiva que transcurre a través de Deep Web y Dark Web.

1.4. BREVE MENCIÓN AL CONTEXTO DE ACTUACIONES CONTRA LA CIBERDELINCUENCIA

En un plano internacional, los países se han visto abocados a renovar su legislación en materia de ciberseguridad para así poder hacer frente al notable incremento de la delincuencia perpetrada o para cuya consecución es necesario el uso de internet, circunstancia que se ha visto incrementada a raíz de la pandemia suscitada por la COVID-19.

En este contexto, son incontables los países que han aumentado los fondos estatales destinados a ciberseguridad. Cabe resaltar la reciente orden ejecutiva firmada el pasado 12 de mayo de 2021 por Joe Biden, actual presidente de los Estados Unidos, la cual establece estándares de ciberseguridad que tienen como objetivo fortalecer la ciberseguridad del país mediante la creación de una junta para investigar los incidentes de seguridad integrado por el Departamento de Seguridad Nacional, el Departamento de Justicia, el Pentágono y entidades del sector privado[3]. Esta preocupación queda evidenciada en una hoja informativa publicada por la Casa Blanca en la que se indica que "La ciberseguridad es uno de los desafíos más importantes de nuestro tiempo, por lo que el presidente Biden ha hecho del fortalecimiento de las capacidades de ciberseguridad de Estados Unidos una máxima prioridad".

Por su parte, Europa también ha definido como objetivo clave lograr responder a la evolución del panorama de las ciberamenazas. En consecuencia, en diciembre de 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentaron una nueva Estrategia de Ciberseguridad de la UE. El objetivo de esta estrategia es reforzar la resiliencia de Europa frente a las ciberamenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables. De igual manera, en abril de 2021, el Consejo dio luz verde a la creación de un Centro de Competencia en Ciberseguridad que tiene como objetivo poner en común las inversiones en investigación, tecnología y desarrollo industrial en materia de ciberseguridad. De esta forma, la coordinación entre los Estados miembros se instaura como un requisito indispensable, ya que este Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad trabajará de forma conjunta con una Red de Centros Nacionales de Coordinación designados por los Estados miembros, así como organizaciones académicas y de investigación, industrias y otras asociaciones de la sociedad civil, y, sobre todo, queda prevista la cooperación con la Agencia de la UE para la Ciberseguridad (ENISA).

Además, para facilitar en mayor medida el acceso transfronterizo a las pruebas electrónicas para los procesos penales, la Unión Europea se encuentra en proceso de negociación de:

- Un acuerdo con Estados Unidos, el país en el que se encuentran la mayoría de los proveedores de servicios, y cuya comunicación se ve en ocasiones entorpecida principalmente por la protección de datos personales y que requiere una profunda deliberación que, por motivos de envergadura, no puede ser tratada en detalle en el presente trabajo.
- El segundo protocolo adicional del Convenio de Budapest mencionado en el primer punto del presente trabajo.

De esta forma, los países han intentado abordar la problemática que la ciberdelincuencia y la fenomenología delictual asociada plantean actualmente, de manera que estas ofrezcan las bases jurídico-legales necesarias para que los diferentes

3 President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks (12 de mayo de 2021). The White House. Recuperado de: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

organismos y fuerzas del orden competentes puedan abordar estos aspectos desde una perspectiva práctica efectiva. El EC3 de EUROPOL, el CCN-Cert del Centro Criptológico Nacional (CCN), el Mando Conjunto del Ciberespacio (MCCE) del Estado Mayor de la Defensa (EMAD), así como el Grupo de Delitos Telemáticos (GDT) de la Guardia Civil y la Unidad de Investigación Tecnológica (UIT) de la Policía Nacional son solo algunos ejemplos del proceso de especialización que se está llevando a cabo para hacer frente a las complejas investigaciones tecnológicas en la lucha contra la delincuencia, las dificultades en el análisis de evidencias digitales y la ya innegable necesidad de cooperación internacional.

2. OBJETIVOS

El presente trabajo tiene como principal objetivo:

- Identificar los principales modus operandi empleados por los cibercriminales que operan a través de la Deep Web y Dark Web.

De manera adicional, se tratará de:

- Analizar las características particulares de los delitos perpetrados o para cuya consecución es necesario acudir a Deep Web o Dark Web dentro del marco de la justicia española.
- Estudiar el nivel de detectabilidad que los delitos perpetrados o para cuya consecución es necesario acudir a Deep Web o Dark Web dentro del marco español.
- Determinar la eficacia probatoria de los indicios digitales detectados a partir de Deep Web y Dark Web dentro del marco de la justicia española.
- Reseñar la capacidad de resolución de fenómenos delictivos que involucran Deep Web y Dark Web dentro del marco de la justicia española.
- Describir propuestas de mejora para la investigación de esta fenomenología delictiva.

3. METODOLOGÍA

Para lograr alcanzar los objetivos anteriormente descritos, se determinó que la metodología que mejor se adecuaba era la empírica.

Se trata de un estudio exploratorio consistente en un análisis de sentencias, que constituyen los casos objeto del presente artículo.

En cuanto al procedimiento de selección de casos, es decir, la recopilación de sentencias que involucran Deep Web y Dark Web, este proceso siguió unas pautas previamente establecidas. En primer lugar, las búsquedas se focalizaron en la base de datos de jurisprudencia del Centro de Documentación Judicial (CENDOJ). Para lo cual, se establecieron una serie de criterios de búsqueda, que consistieron en seleccionar la lista de palabras clave que se muestra a continuación.

“Deep Web”, “Dark Web”, “Darknet”, “Dark net”, “red oscura”, “hidden Web”, “TOR”, “I2P”, “web”, “red anónima”, “internet”.

Una vez seleccionadas las palabras clave, se comenzó la búsqueda de estos términos de manera individual y combinados, aplicando como filtro que los resultados se encontraran enmarcados dentro de la jurisdicción penal. De esta forma, se lograron recabar un total de 44 sentencias, que fueron tratadas como estudio de casos, por la preponderancia del valor cualitativo sobre el cuantitativo.

Posteriormente, se procedió a recopilar la información relevante de las sentencias en base al interés del trabajo, para ello se elaboró una tabla a modo de base de datos organizada según tres dimensiones que contienen las siguientes variables:

1. Contenido procesal. Esta dimensión involucra todos los aspectos relativos al proceso judicial propiamente dicho, es decir, las variables relativas al procedimiento, tipo de resolución, órgano que emite el juicio, fallo y fechas de comisión de los hechos y de resolución.

2. Contenido criminalístico y problemas probatorios. Este ámbito constituye el aspecto más relevante, ya que en él se abordaba el análisis del contenido criminalístico, entendiendo por contenido criminalístico la extracción de evidencias mediante métodos y técnicas científicas, con el objetivo de recabar los indicios digitales necesarios que serán tenidos en cuenta en la resolución del caso, es decir, trata de valorar la capacidad probatoria de las evidencias digitales asociadas a Deep Web y Dark Web.

3. Características criminológicas. Esta dimensión hace referencia a los aspectos puramente fenomenológicos, con el objetivo de recabar toda la información criminológica relevante posible que permita identificar patrones en aras de mejorar la prevención, tales como el estudio de delincuentes, hechos delictivos, víctimas y contexto social, entre otros aspectos.

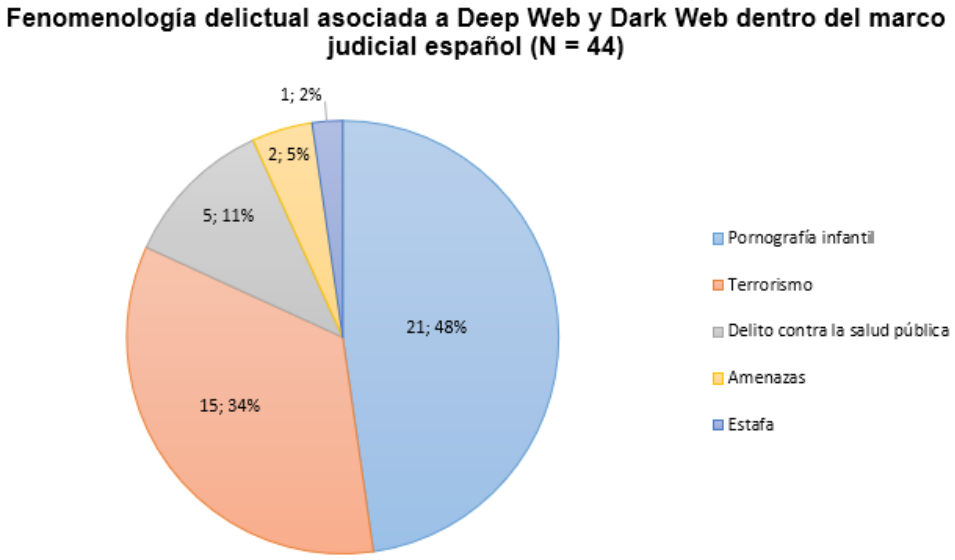
No obstante, la metodología adoptada cuenta con una gran limitación pues, además de ser una muestra muy limitada, el empleo de sentencias como casos implica que solo se tienen en cuenta los hechos conocidos por los juzgados y tribunales de justicia españoles. Dada la particular naturaleza del entorno, en el que predomina el anonimato, existen multitud de hechos que se escapan al conocimiento de los órganos de justicia, lo que supone un sesgo en los resultados obtenidos que fue tenido en cuenta en la interpretación y puesta en contexto de dichos resultados. Este sesgo es lo que se conoce como “cifra oscura” en criminología. Si bien, desde otra perspectiva, es precisamente este sesgo el que permite identificar las características específicas de los delitos relacionados con Deep Web y Dark Web conocidos por el sistema judicial español, poniendo en evidencia cuáles son sus peculiaridades y qué relevancia tienen estas, tanto de cara a la identificación del hecho delictivo y su autor como de cara a la resolución del proceso judicial aparejado.

4. RESULTADOS

Tras realizar una aproximación empírica al objeto de estudio, siendo este, de manera muy generalizada, la actividad criminal que transcurre o para cuya perpetración es necesario acudir a Deep Web y Dark Web, tomando como referencia los hechos conocidos por órganos y tribunales de justicia españoles, se obtuvieron los resultados que se describen a continuación.

En cómputo, se identificaron y analizaron 44 resoluciones judiciales, recabadas a partir de fuentes oficiales, en las que, de una manera u otra, se detectó la presencia de Deep Web y Dark Web. De esta forma, con la finalidad de dotar a estos resultados de una mayor accesibilidad, seguidamente se exponen, de forma gráfica, algunos de los aspectos más relevantes susceptibles de interpretación cuantitativa válida, cuyo análisis pormenorizado será desarrollado a continuación.

En primer lugar, en cuanto al fenómeno delictual asociado a cada una de las resoluciones judiciales identificadas, tal y como se muestra en la Gráfica 2, el fenómeno delictual asociado a Deep Web y Dark Web que mayor presencia obtuvo dentro del marco judicial español fue la Pornografía Infantil, el cual involucró el 48% de los casos identificados; le sigue muy de cerca el fenómeno delictual de Terrorismo, el cual acaparó el 34% de los casos detectados; y, en tercera posición, se encuentra el fenómeno delictual de Delito contra la salud pública, con el 11% de los casos analizados. En las últimas posiciones se encuentran las fenomenologías delictuales de Amenazas, con el 5% de los casos, y la fenomenología de Estafa, que se ha involucrado el 2% de los casos identificados.



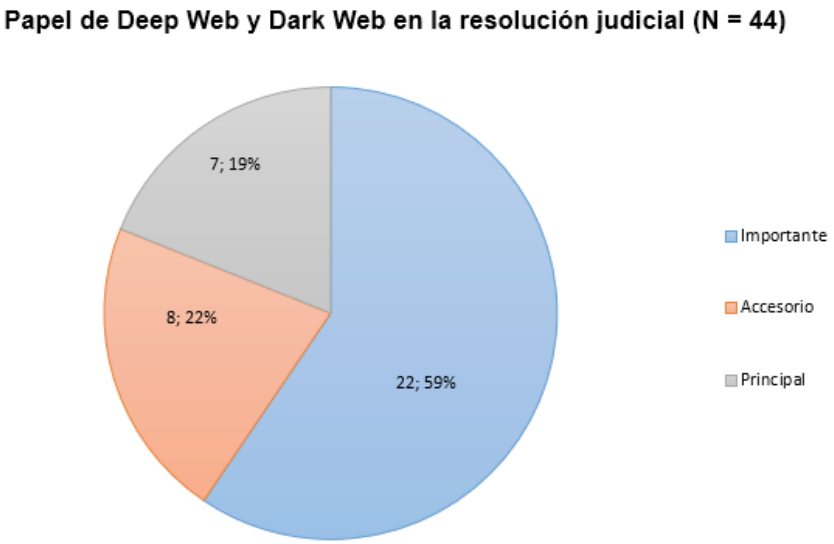
Gráfica 2 Fenomenología delictual asociada a Deep Web y Dark Web dentro del marco judicial español (N=44).

En otro orden de ideas, para tratar de satisfacer la necesidad de conocer el papel que la Deep Web y Dark Web tuvieron dentro de la resolución judicial, se establecieron tres niveles, siendo estos Accesorio, Importante y Principal, ilustrados a través de la siguiente gráfica.

Ordenados de menor a mayor relevancia, el nivel accesorio se asignó a aquellos casos que involucraban Deep Web y Dark Web pero no supusieron una circunstancia de peso en la resolución; en cuanto al nivel importante, hace referencia a aquellos casos en los que la presencia de Deep Web y Dark Web tomó relevancia en la determinación de la resolución en confluencia con otros hechos probados adicionales; por último, el nivel principal se asignó a los casos en los que se tuvo conocimiento

del/los hecho/s delictivos a partir de la investigación de los entornos de Deep Web y Dark Web, o bien la motivación de la resolución estaba basada principalmente en indicios digitales recabados a partir de Deep Web o Dark Web.

Tal y como se puede observar en la Gráfica 3, en el 50% de los casos el papel que Deep Web y Dark Web tuvieron en la resolución judicial fue importante, mientras que en el 34% este papel fue accesorio y, en el 16% restante, el papel fue principal.



Gráfica 3 Papel de Deep Web y Dark Web en la resolución judicial (N=44).

Los resultados plasmados anteriormente permiten realizar un primer acercamiento al objeto de estudio, si bien tal y como se ha descrito en la metodología, dado que se trata de un ámbito de carácter especialmente misceláneo, para comprender la realidad de la fenomenología delictual asociada a Deep Web y Dark Web se consideró necesario abordar esta problemática desde una perspectiva cualitativa, atendiendo a las características reseñables de los diferentes casos de manera más individualizada y así poder extraer conclusiones fructíferas.

4.1. CONTENIDO PROCESAL

Con el propósito de contextualizar las resoluciones judiciales identificadas, se acudió a los aspectos relativos al procedimiento judicial.

En primer lugar, cabe señalar que en el 100% de los casos el fallo fue condenatorio, contra los cuales se interpusieron un total de 14 recursos.

En adicción a lo anterior, y con el propósito de contextualizar las fenomenologías delictuales involucradas, en cuanto al órgano judicial que emitió el juicio fue la Audiencia Nacional en el 25% de los casos, la Audiencia provincial en el 50%, el Tribunal Supremo en el 16%, el Tribunal Superior de Justicia y la Sala de Apelación de la Audiencia Nacional en el 4,5% y, finalmente, el Juzgado de Instrucción en el 2% restante.

4.2. CONTENIDO CRIMINALÍSTICO Y PROBLEMAS PROBATORIOS

Con el fin describir el papel que Deep Web y Dark Web ocuparon en los hechos sentenciados, se realizó un acercamiento más próximo al entorno objeto de estudio en función de cada fenomenología delictiva identificada.

- Pornografía infantil

Dentro de la fenomenología de Pornografía infantil, más aún teniendo en cuenta que se trata de la fenomenología que en un mayor volumen de casos se vio implicada, es decir, el 48% de las detecciones, conviene señalar el papel que ocuparon Deep Web y Dark Web en la resolución judicial, siendo este papel importante en el 38% de los casos, principal en el 33% y accesorio en el 29% de casos restantes. En este sentido, es reseñable el hecho de que todos los casos identificados a partir del análisis global de sentencias en los que el papel de Deep Web y Dark Web fue principal son relativos a la tipología de pornografía infantil, es decir, esto pone de manifiesto que es la única tipología en la que el autor fue detectado como fruto de una investigación policial en Dark Web, ya sea de carácter internacional o nacional, tales como la operación Trojan, DOWNFALL2 Operación FERAS, en las que intervinieron unidades especializadas en esta fenomenología delictiva como INTERPOL, EUROPOL, FBI o el Grupo de Protección a la infancia de la Brigada Central de Investigación Tecnológica.

La circunstancia anteriormente descrita está a su vez relacionada con el funcionamiento de los foros de pornografía infantil en los que su acceso está estipulado de acuerdo con una serie de fases y privilegios, siendo necesario contar con una serie de requisitos para poder acceder a cierto contenido, como puede ser que los usuarios suban contenido al menos una vez al mes o de lo contrario serán desactivados, por lo que no sería posible descargar archivos si no se distribuye contenido. Este aspecto resulta realmente interesante, sobre todo en los casos en los que el sujeto es identificado a través de su participación en un foro de Dark Web, pues, aun desconociéndose su actividad, el mero hecho de ser integrante de un foro de este tipo, más aún si el usuario goza de un nivel de privilegios elevado, es indicativo de que su actividad implica el consumo y la distribución, quedando constatada la capacidad probatoria de este hecho.

Asimismo, dentro de la determinación de la capacidad probatoria, se detectó otro caso de uso habitual, que consistió en aquellas detecciones en las que, a consecuencia de la entrada y registro en el domicilio, se detectó el almacenamiento de contenido de carácter pedófilo en los dispositivos digitales investigados, así como la presencia del navegador TOR instalado en el dispositivo, siendo esto suficiente para que quedasen constatados los hechos probados en relación a los delitos de tenencia y distribución de pornografía infantil.

- Terrorismo

En cuanto a la tipología de Terrorismo, es decir el 34% de los casos identificados, de cara a conocer el papel que Deep Web y Dark Web ocupó en la resolución, en el 53% de los casos este fue accesorio, mientras que en el 47% de los casos restantes el papel fue importante. Para contextualizar las cifras anteriormente descritas, es necesario tener en cuenta que este tipo de resoluciones judiciales implican extensas investigaciones que abarcan multitud de acciones por parte de los condenados, o acusados, por lo que en su mayoría Deep Web y Dark Web constituyen un medio más

a partir del que poder desarrollar su actividad delictiva, observándose un mayor uso de las redes sociales y sistemas de mensajería instantánea, es decir fuentes abiertas de información, con el objetivo de llegar a los usuarios con los que se estrechará la comunicación en una fase ulterior.

En cualquier caso, a partir de la revisión de resoluciones relativas a la fenomenología Terrorismo que implicaron el uso de Deep Web y Dark Web, queda constatado que estas son elementos esenciales en la distribución y propagación. En este sentido, se pone de manifiesto las altas capacidades de adaptación de esta fenomenología delictiva, que no solo se nutre de las ventajas de las nuevas tecnologías, sino que optimizan su empleo mediante la incorporación de softwares de anonimización y criptodivisas, para así desarrollar las actividades delictivas en entornos seguro que entorpezcan la investigación policial y evadir la detección.

Finalmente, cabe destacar, de forma similar a lo acaecido en la tipología de Pornografía infantil, la existencia de cuerpos de seguridad focalizados en su investigación, tales como Unidad de Policía Judicial para delitos de terrorismo (TEPOL) o el Grupo de Información de la Guardia Civil, que intervinieron en operaciones conjuntas de carácter internacional.

- Delito contra la salud pública

Dentro de la tipología de Delito contra la salud pública, que constituye el 11% de las resoluciones identificadas, se determinó que el papel que ocuparon Deep Web y Dark Web en la resolución judicial fue importante en el 100% de los casos, en tanto que este era el medio que los implicados utilizaban para distribuir las sustancias, ya fuesen sustancias estupefacientes o medicamentos sin contar con la acreditación necesaria, por tanto era una parte muy importante en su modus operandi. A pesar de que en ninguno de los casos la detección fue a consecuencia de investigar directamente Deep Web o Dark Web, el hecho de que la compra y posterior distribución se realizase a través de sitios de Dark Web queda sufientemente constatado en los hechos probados de cara a la motivación del fallo.

A raíz de lo anterior, cabe destacar el uso de pagos mediante monedas virtuales, en estos casos Bitcoin, ya que resultan un medio óptimo para evadir la identificación, tanto de receptor como emisor de las transacciones, ampliamente utilizado en entornos de Dark Web.

De igual manera, resulta reseñable la labor de investigación llevada a cabo por las Fuerzas y Cuerpos de Seguridad, que cuentan con unidades específicas para la materia, tales como el Equipo de Delincuencia Organizada Antidroga (E.D.O.A.).

- Amenazas

Dada la baja incidencia de la fenomenología Amenazas, siendo esta del 5% de las detecciones, los casos detectados no han sido considerados representativos del objeto de estudio. En el primero de ellos el proceso comienza a raíz de la recepción de un correo de contenido amenazante a través de un cliente de correo de Dark Web, aunque finalmente su investigación no aportó ningún peso a la resolución judicial. De otro lado, en el segundo caso, la referencia se basa en amenazar con el anonimato que TOR en el contexto de una disputa entre una expareja.

- Estafa

Aunque a priori pudiese parecer lo contrario, dada la baja incidencia -el 2% de casos-, resulta una fenomenología realmente interesante para el objeto de estudio, en la que la totalidad de las detecciones Deep Web y Dark Web ocuparon un papel importante.

De manera concreta, el caso identificado versa sobre la modalidad de estafa cibernética denominada *carding*, siendo Deep Web y Dark Web un requisito necesario para su consecución, pues a partir de los hechos constatados puede extraerse que el condenado obtuvo los datos asociados a tarjetas a partir de esta fuente, sin que en ningún momento se indicase que el sujeto contaba con avanzados conocimientos de informática que le permitiesen llevar a cabo las acciones necesarias para obtener la información vinculada a las tarjetas bancarias por sí mismo, siendo más plausible que lograse obtenerlas mediante un mercado de Deep Web o Dark Web.

4.3. CARACTERÍSTICAS CRIMINOLÓGICAS

Finalmente, atendiendo a los aspectos criminológicos más destacables de las diferentes fenomenologías delictivas, de manera que faciliten un mejor conocimiento del objeto de estudio y favorezcan la labor de investigación y detección de estos fenómenos, se tuvieron en cuenta aspectos relativos al autor y, siguiendo a Herrera (2018), investigadora pionera dentro del ámbito de la Victimología española, a la víctima, que tan solo se ve reflejada en la tipología de Pornografía infantil.

En cuanto a las características del autor en la tipología de Pornografía infantil, se descubrió que la totalidad de ellos fueron varones, habiéndose detectado una notable tasa de implicados que contaban con antecedentes penales previos. Por su parte, las características de la víctima, que comprende aquellos casos en los que el implicado llevó a cabo o bien abusos sexuales o elaboración de contenido, existía una estrecha relación entre el autor y la víctima, así como en aquellos casos en los que se identificó la figura del testigo, este formaba parte del círculo cercano.

De otro lado, en cuanto a las características aparejadas al autor en la tipología Terrorismo, cabe destacar un alto porcentaje de implicados de nacionalidad extranjera.

Por otra parte, teniendo en cuenta las circunstancias de los implicados en la tipología de Delitos contra la salud pública, es reseñable la existencia de coautoría.

En cuanto al resto de tipologías, dada la escasa representatividad de estas, se eludirá la alusión a las características criminológicas.

5. DISCUSIÓN Y CONCLUSIONES

A modo de conclusión, extraídas a partir del estudio realizado, se incluyen una serie de enunciados que tratarán de solventar las necesidades planteadas, de forma que justifiquen la realización del presente trabajo poniéndolas en concordancia con lo establecido por los diferentes autores que han venido abordando esta miscelánea materia objeto de estudio.

En primer lugar, aunque ya se ha comentado anteriormente, cabe destacar el escaso número de resoluciones judiciales dentro del ámbito jurídico español que involucran

el uso de Deep Web y Dark Web, circunstancia que evidencia la existencia de la cifra oscura en cuanto a ciberdelincuencia se refiere relacionada con Deep Web y Dark Web.

En otro orden de ideas, tal y como han venido reflejando diferentes estudios sobre las fenomenologías delictivas asociadas a Deep Web y Dark Web, existen determinadas tipologías que se benefician especialmente de las características que estas ofrecen, incorporándolas en gran medida a sus particulares modus operandi. De esta forma, se ha podido comprobar que las principales fenomenologías delictivas reflejadas por las bases teóricas asentadas sobre la materia, es decir delitos contra el patrimonio y contra el orden socioeconómico, delitos contra la salud pública, delitos de organizaciones y grupos terroristas, pedofilia y explotación sexual, y tráfico de armas, realmente son las que componen el grueso de las principales actividades criminales vinculadas a este ámbito. En este sentido, a partir de la revisión sistemática de resoluciones judiciales extraídas del ámbito español que involucran el uso de Deep Web y Dark Web, se obtuvo como resultado que, de mayor a menor relevancia, Pornografía infantil, Terrorismo, Delitos contra la salud pública, Amenazas y Estafa fueron las fenomenologías más destacadas. Dentro de los actos delictivos enmarcados en la categoría de delitos contra el patrimonio y el orden socioeconómico, se encuentran la fenomenología de Estafa en particular y, de forma indirecta, todos aquellos actos que involucran el empleo de criptodivisas. A su vez, como es obvio, dentro de los hechos delictivos asociados a delitos contra la salud pública, se encuentra enmarcada la fenomenología que ha sido denominada de la misma forma. Por su parte, los actos que envuelven delitos de organizaciones y grupos terroristas acaparan la fenomenología aquí referida como Terrorismo. En cuanto a los actos delictivos de índole sexual, es decir, pedofilia y prostitución y explotación sexual, se encuentra enmarcada la fenomenología Pornografía infantil. Con respecto a los actos que involucran el tráfico de armas, a pesar de que no se ha detectado una relevancia específica tal que permita establecer una fenomenología específica, estos actos han tomado especial relevancia dentro de la fenomenología Terrorismo. Finalmente, cabe mencionar que no se identificaron estudios que avalen el empleo de Deep Web y Dark Web para perpetrar la fenomenología de Amenazas, detectada a partir de la revisión de resoluciones judiciales; esto es porque, tal y como se ha reflejado en los resultados, se trata de detecciones aisladas que poco aportan al estudio de esta materia, sin que sea posible considerar que Deep Web y Dark Web constituyan un medio especialmente significativo para su perpetración, siendo tan importante como cualquier otro.

De forma particular, se han identificado variables significativas en el modus operandi en función de la fenomenología delictiva. Aunque a grandes rasgos son aparentemente similares, pues en todas ellas, Pornografía infantil, Terrorismo, Delitos contra la salud pública, Amenazas y Estafa, los autores acuden a Deep Web y Dark Web para poder perpetrar la actividad ilícita en cuestión sin ser detectados, cuyo flujo transcurre en foros, o markets en su caso, a los que es difícil acceder si no se tiene conocimiento de la dirección URL o IP concreta, información acotada a un círculo de conocedores de la materia en cuestión, es decir, a lo que la literatura se refiere como redes de contacto.

En la fenomenología de Pornografía infantil, el entramado para acceder a los foros en los que transcurre la actividad es especialmente robusto, llegando a existir incluso

un sistema según el cual se determina el nivel de acceso al contenido. Esto es a su vez entorpecedor, por el evidente hecho de que la actividad se encuentra particularmente encubierta, al mismo tiempo que provechoso para la labor investigativa, pues en el momento en el que se logre irrumpir en algunos de estos foros e identificar a una persona quedará suficientemente constatada su participación en la distribución de contenido pedófilo, ya que para ganar el acceso es requisito indispensable aportar contenido de calidad cada cierto tiempo. Esta circunstancia justifica el hecho de que Pornografía infantil fuese la única fenomenología en la que se lograse identificar a los sujetos a través de operaciones policiales encaminadas a la persecución de estos delitos a través de Deep Web y Dark Web. Además, justifica la necesidad de regulación de la figura del agente encubierto cibernético, ya que su labor es especialmente relevante en esta materia, por tanto es esencial que esta figura cuente con todas las garantías legales posibles, de manera que revistan tanto el proceso de investigación como los resultados obtenidos de todos los requerimientos jurídicos necesarios.

Mientras que en otras fenomenologías se ha comprobado que fue más difícil constatar la actividad a través de Deep Web y Dark Web y se acepta que estas tuvieron implicación en los hechos, en cuanto el autor contaba con el software necesario instalado o, en algunas ocasiones, contenido procedente de Darknets o enlaces de acceso, pero por sí mismos estos descubrimientos probablemente no habrían bastado para detectar los hechos delictivos.

En este sentido, se ha observado que en el caso de la fenomenología delictiva de Terrorismo se destinaron grandes recursos dentro de la investigación a la investigación de fuentes abiertas mediante técnicas OSINT. Esto pone de manifiesto la relevancia que las fuentes de información abiertas ocupan dentro del marco de investigación de hechos delictivos que involucran las TIC y, por ende, Deep Web y Dark Web, observándose así la importancia que el ciclo de extracción de inteligencia supone. Este hecho está basado en las particulares dificultades de detección de uno y otro medio. Mientras que monitorizar la actividad que transcurre a través de Deep Web y Dark Web, así como identificar a un sujeto mediante su actividad en este medio resulta realmente dificultoso, si se emplean las herramientas y técnicas adecuadas en la investigación de fuentes abiertas propiamente dichas, tales como redes sociales, altamente empleadas en esta fenomenología delictiva para la difusión y propaganda, resulta relativamente asequible acceder y monitorizar el contenido e identificar a sus autores, si así fuese necesario en base a la gravedad de los delitos y la ausencia de otros medios menos lesivos para obtener la información que se pretende.

Por su parte, en el caso de las fenomenologías de Delitos contra la salud pública y Estafa, aunque en ningún caso se llegase a identificar al autor por su actividad en Deep Web y Dark Web, es evidente que esta integra un parte esencial en su modus operandi y, al contrario que en el caso de la fenomenología de Pornografía infantil, en estos foros o principalmente markets el acceso se ve dificultado en menor medida por los condicionantes requeridos para ser integrantes, lo que podría beneficiar las labores de investigación, aunque en muchos casos existe un sistema de reputación similar. Otro asunto sería el lograr identificar al sujeto en cuestión, es decir, identificar una dirección IP a través de la cual se pueda llegar a la identidad de su propietario, así como su dirección física. Aunque, sobre todo, la escasa incidencia dentro del ámbito jurídico español de estas fenomenologías minoritarias, Delitos contra la salud pública, Amenazas y Estafa, podría deberse a los recursos dedicados a la investigación de las

mismas, que serían menores que en los delitos vinculados con las fenomenologías de Pornografía Infantil y Terrorismo, en los que se observó una mayor especialización de las unidades policiales que intervienen y mayor implicación internacional a nivel de operaciones, o también a la tendencia recogida por Europol en su informe de Análisis del Crimen Organizado en Internet (IOCTA), correspondiente al año 2020, que pone de manifiesto los buenos resultados derivados de los notables esfuerzos dedicados en 2019 a la interrupción de la actividad de numerosos mercados que operan a través de Dark Web.

Desde otra perspectiva, a raíz del estudio de las características relativas a los autores de las diferentes fenomenologías delictivas, se ha identificado una serie de variables específicas que podrían favorecer la investigación. En primer lugar, en los casos de Pornografía infantil se observó que la reincidencia es un hecho habitual. De otro lado, cabe destacar que, en los casos relativos a la fenomenología Terrorismo, la mayor parte de los autores no era de nacionalidad española, lo cual resulta plausible en base a las características específicas de esta tipología delictiva. Finalmente, destacó el hecho de que en la fenomenología Delitos contra la salud pública la participación implicase en un alto grado la coautoría, circunstancia totalmente loable dado que suelen involucrar la existencia de una organización.

Pese a la escasa detectabilidad de los fenómenos delictivos que transcurren a través de Deep Web y Dark Web, cabe resaltar que, a grandes rasgos, en los casos en los que se detectaron indicios digitales, estos tuvieron una gran implicación en la resolución judicial, por lo que cabe atribuirles una buena eficacia probatoria dentro del marco de la justicia española. En muchos de los casos, la detección del software TOR instalado en el dispositivo del autor ya tuvo una implicación importante en el dictamen de la sentencia, esto está basado en las particulares características que reviste este software que implican altas capacidades de anonimización, tal y como se expone en la breve aproximación al concepto de TOR llevada a cabo en el presente trabajo. En relación con la eficacia probatoria, quedó demostrado a través del estudio de casos que los fenómenos delictivos fueron resueltos con fallo condenatorio en la mayoría de ellos, por lo que se considera satisfecha la capacidad de resolución de hechos que involucran Deep Web y Dark Web. Esta circunstancia deriva principalmente del tratamiento del indicio digital, ya que, en el marco de la justicia española, este ha de contar con un determinado protocolo en lo que a su investigación y obtención de la evidencia propiamente dicha se refiere. En este sentido, la investigación e incautación de indicios en los propios equipos no deja de ser sino una verdadera prueba material del hecho delictivo, siempre y cuando cumpla los debidos requisitos de cadena de custodia, así como otros de carácter técnico, necesarios como cualquier otra investigación/inspección ocular.

Asimismo, cabe destacar un correcto entendimiento generalizado de la materia por parte de los órganos de justicia españoles, acudiendo a los términos de manera cierta y reflejándolo de forma accesible en la sentencia, lo cual es esencial para abordar de forma correcta esta problemática. En este sentido, cabe mencionar que la Cámara de Delegados de la Asociación de Abogados del Estado de Nueva York (“NYSBA”) aprobó, a comienzos de septiembre, un informe proponiendo que el Comité Ejecutivo de NYSBA recomiende a la Junta de Educación Legal Continua del Estado de Nueva York que se modifique el requisito de CLE bienal para requerir un crédito en ciberseguridad en el desarrollo de la práctica jurídica. Aunque hasta la fecha en España no se

ha detectado ningún movimiento de propuesta similar, es previsible que pueda surgir en cualquier momento, ya que esta circunstancia es una evidencia más del impacto que el desarrollo de las TIC ha supuesto en el mundo físico y sobre todo jurídico, poniendo de manifiesto la necesidad de optimizar su resolución.

En definitiva, se trata de un ámbito de estudio realmente complejo por sus peculiares características de privacidad y anonimización, lo cual no quiere decir que unas correctas pautas de investigación no deriven en la consecución de resultados favorables. Tal y como se ha expuesto hasta ahora, resulta evidente que la dedicación de esfuerzos en la lucha contra la ciberdelincuencia es esencial, avalada por los buenos resultados obtenidos cuando esta circunstancia fue puesta en práctica. En consecuencia, como se expone al comienzo del presente trabajo, al tratarse la ciberdelincuencia de una fenomenología que se extiende al ámbito internacional, la elaboración de convenios y tratados internacionales tales como el Convenio sobre la Ciberdelincuencia de Budapest de 2001, que buscan crear un marco legal común que sirva como base a las diferentes naciones en la lucha contra el cribercrimen, resultan primordiales dentro de la actual coyuntura socioeconómica. Necesidad que se ha visto incrementada a raíz de la pandemia de la COVID-19, que ha acelerado el proceso de digitalización y desarrollo de las Tecnologías de la Información y las Comunicaciones.

BIBLIOGRAFÍA

Barrera, S (2019). Ciberpol. Metodología para la investigación del cibercrimen. Universidad Internacional de la Rioja (UNIR), Logroño.

Bergman, M. K. (2001). The Deep Web: Surfacing Hidden Value. Journal of Electronic Publishing, Volume 7. https://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main

Barrio, M. (2017). Ciberdelitos: Amenazas Criminales del Ciberespacio. Adaptado reforma Código Penal 2015 (pp. 9-30). REUS, Madrid.

Best, R. A., & Cumming, A. (2008). Intelligence Issues and Developments. En T. M. Paulson, & T. M. Paulson (Ed.), Open Source Intelligence (OSINT): Issues for Congress (75-79). New York: Nova Science Publishers, Inc.

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. Derecho y cambio social, 498.

Chertoff, M., & Simon, T. (2015). The Impact of the Dark Web on Internet Governance and Cyber Security. Global Commission on Internet Governance, Paper Series nº 6, 2-7.

Consejo de Europa (2001). Convenio de Budapest sobre la ciberdelincuencia. 23 de noviembre de 2001, ratificado el 17 de septiembre de 2010. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Consejo General del Poder Judicial (s.f.). Centro de documentación judicial (CENDOJ). http://www.poderjudicial.es/search/indexAN.jsp

Díaz, M. (4 de abril de 2019). Persecución de delitos en la Darknet: un análisis de la jurisprudencia española. Click Jurídico. https://clickjuridico.es/delitos-deepweb-jurisprudencia-espana/

Espinosa, J.F (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. La razón histórica. Revista hispanoamericana de Historia de las Ideas, nº 44, 153-173. ISSN 1989-2659.

European Union Agency for Law Enforcement Cooperation (2019). Internet Organised Crime Threat Assessment (IOCTA) 2019. https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

Internet Organised Crime Threat Assessment (IOCTA) 2020. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Gehl, R. W. (2014). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. SAGE Journals, Volume 18(7), 1219-1235.

GL, J. (2018). Técnicas OSINT para investigación en Internet. Manual para investigadores.

Metodología OSINT para investigar en Internet (2020).

He, B., Patel, M., Zhang, Z., & Chang, K. C.-c. (2007). Accessing the Deep Web. Communications of the ACM, 50(5), 95-101.

Herrera, M. (2018). "Las víctimas en el sistema penal y su derecho a los derechos" reflexiones a propósito de "derecho de las víctimas a tener derechos", de José Luis Eloy Morales Brand. Revista Electrónica de Estudios Penales y de la Seguridad: REEPS, Nº. 3.

Lovejoy, G. (2020). Inside the Dark Web. Security and Society in the Information Age, Vol. 2, 124-145.

Ministerio del Interior (s.f.). Portal Estadístico de Criminalidad. https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis

National Security Agency Center (NSA) (2013). Untangling the Web: An Introduction to Internet Research.

Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. BOE núm.46. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-2442

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. BOE núm.103. https://www.boe.es/eli/es/o/2019/04/26/pci487

Ramos, L. (6 de mayo de 2018). STS 173/2018, de 11 de abril, el agente encubierto digital. Rodríguez Ramos Penal & Compliance. https://www.rodriguezramos.es/2018/05/06/conclusiones-del-abogado-general-m-campos-sanchez-bordona-presentadas-el-12-de-septiembre-de-2017-asunto-c

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. 17 de septiembre de 1882. BOE núm.260. https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

Requião, B., MacCarron, P., Passold, J., Walmocyr, L., Oliveira, K., & Gleeson, J. (2020). Assessing police topological efficiency in a major sting operation on the dark web. Natureresearch: Scientific Reports.

Retenaga, A. M. (28 de mayo de 2014). OSINT - La información es poder. INCIBE-CERT. https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

Roop, J. E. (1969). Chapter 1 - Early Beginnings. En J. E. Roop, Foreing Broadcast Information Service History. Central Intelligence Agency.

Ruiz, T. (2021). "Las Nuevas Diligencias de Investigación Electrónicas".

TOR Project (s.f.). Documentation: Abuse FAQ. https://2019.www.torproject.org/docs/faq-abuse.html.en

World Economic Forum (2019). The Global Risks Report 2019. Insight Report. 14th Edition.

(2020). The Global Risks Report 2020. Insight Report. 15th Edition.

AUTOS Y SENTENCIAS

SAN-2196-2020

SAP-C-1656-2020

SAP-CC-811-2020

SAP-IB-145-2020

SAP-TF-1071-2020

SAP-VA-842-2020

STS-3448-2020

SAN-5286-2019

SAN-633-2019

SAN-1447-2019

SAN-5421-2018

SAN-3383-2019

SAN-4717-2019

SAP-C-1383-2019

SAP-MA-2751-2019

SAP-P-337-2019

SAP-PO-2479-2019

STS-1535-2019

SAN-4611-2018

SAN-2472-2018

STS-2205-2019

SAP-B-13263-2018

ATS-11793-2018

SAP TF-284-2018

STSJ-ICAN-1961-2018

SAP-TF-1900-2018

SAP-V-3858-2018

SAN-2462-2018

SAN-2750-2018

SAN-4993-2018

STS-1385-2018

SAP-LU-471-2017

STS-4554-2018

SAP-CC-819-2017

ATS-12884-2017

STSJ-ICAN-981-2017

SAP-TF-500-2017

SAN-3016-2017

SAP-C-1461-2017

SAP-GC-2515-2017

SAP-M-6587-2017