Universidad de Alcalá

LA CIBERDELINCUENCIA Y LA DEEP WEB

TRABAJO DE FIN DE MÁSTER

UNIVERSIDAD DE ALCALÁ

MASTER ACCESO A LA PROFESIÓN DE ABOGADO

FACULTAD DE DERECHO

Autor: Javier Galán Ahumada

Tutor: Prof. Dra. Carmen Pérez Sauquillo

Codirectora: Prof. Dra. Raquel Roso Cañadillas

INDICE

RESUMEN:

La sociedad evoluciona a pasos agigantados, y lo que ayer parecía un disparate hoy es una realidad. Es así como internet se creó, se globalizó y pasó a formar parte de la sociedad de una forma rápida y concisa; siendo un medio sin el cual es prácticamente imposible de imaginar la vida en la actualidad.

Pero no todo lo que trae internet es bueno: internet lo hacen las personas y dependiendo de quien sea el usuario final que entra en el mismo, sus funciones y finalidades pueden variar drásticamente. Un usuario con buenas intenciones usará internet como medio de información, comunicación, tecnológico, etc. Pero un usuario con un modo de pensar mucho menos loable puede usar este sistema para lucrarse a costa de los demás, es decir, cometiendo actos ilegales.

En este Trabajo de fin de máster haremos un análisis genérico de la evolución de internet desde su concepción a su funcionamiento actualmente, así como indagaremos en los delitos más comunes que cometen los delincuentes en la red; también entraremos a analizar la parte más oscura de internet, la Deep Web, y profundizaremos en aquellas prácticas delictivas y no delictivas que se pueden encontrar en estos entornos.

Por último, detallaremos aquellas leyes y Ordenamientos Jurídicos destinados a velar por los intereses de los ciudadanos y a proteger sus bienes y derechos frente a estas nuevas tecnologías y nuevas formas de cometer delitos.

PALABRAS CLAVE:

Ciberdelincuencia, Bitcoin, Criptomoneda, Deep Web, Dark Web, Estafa, Internet, Silkroad, Phishing.

ABSTRACT:

Society evolves by leaps and bounds, and what yesterday seemed nonsense today is a reality. This is how the internet was created, globalized and became part of society in a quick and concise way; being a medium which, at present, is practically impossible to imagine being without.

But not everything that the internet brings is good, the internet is made by people and depending on who is the end user who enters it, its functions and purposes can vary drastically. A user with good intentions will use the Internet as a means of information, technology, etc. But a user with a much less praiseworthy mindset can use this system to profit at the expense of others, that is, by committing illegal acts.

In this Master's Thesis we will make a generic analysis of the evolution of the internet from its conception to how it is today, as well as investigate the most common crimes committed by criminals on the network; We will also analyze the darkest part of the Internet, the Deep Web, and delve into what are those criminal and non-criminal practices that can be found in these environments.

Finally, we will detail those laws and legal systems designed to ensure the interests of citizens and protect their assets and rights against these new technologies and new ways of committing crimes.

KEYWORDS:

Cybercrime, Bitcoin, Cryptocurrency, Deep Web, Dark Web, Scam, Internet, Silkroad, Phishing.

1. INTRODUCCIÓN. INTERNET Y SU EVOLUCIÓN HASTA LA ACTUALIDAD

Internet es, sin duda, una de las invenciones más importantes del siglo XX. Desde que se concibió, ha dado pie a miles y miles de avances tecnológicos que ayudan a la sociedad a avanzar tanto personal como tecnológicamente: concebir un mundo sin internet en la actualidad es meramente impensable.

Internet a lo largo de su historia ha generado muchísimas cosas buenas y que han hecho avanzar a la sociedad de una manera drástica en poco tiempo, dando pie a nuevas tecnologías y nuevas formas de tratar el día a día de la gente y la información que puedan manejar en un momento dado.

Hace más o menos 40 años, los principales medios de comunicación eran el telégrafo y el teléfono; internet y los ordenadores o smartphones que usamos actualmente no existían y en esos tiempos, la sociedad no estaba tecnológicamente preparada para su existencia. Si bien es cierto que existían computadoras en aquella época, estas eran máquinas enormes con el único propósito de realizar cálculos y almacenar información, y estaban al alcance de muy pocas empresas y o gobiernos, por el alto coste que estas tenían.

Entonces ¿cómo hemos llegado a pasar en 40 años de la nada al todo gracias a la existencia de internet? La respuesta se remonta al año 1957, durante la Guerra Fría, cuando EE.UU. y la URSS se enfrentaban entre sí para ver qué Estado era el que tenía mayor potencia ideológica, económica, política, militar y tecnológica.

Mientras que la URSS lanzaba el primer satélite de la historia, el Sputnik 1 en 1957, EE.UU. crea un año después y en respuesta la "*Advanced Research Proyects*

Agency" (ARPA), la cual será clave en la historia de internet, pues fue la encargada de la investigación de nuevas tecnologías con propósitos defensivos y militares y, entre todas estas investigaciones, se encontraban las redes de ordenadores[1].

El estudio de las redes de ordenadores se ve incrementado exponencialmente con el paso de los años gracias a ARPA cuando, en 1962, Paul Baran presentó un sistema de comunicaciones inmune a ataques externos gracias a la comunicación entre computadoras conectadas a una red descentralizada. Este proyecto se puso en marcha hasta que finalmente en 1966 se consiguió conectar un ordenador en Massachussets con otro en California mediante una línea telefónica[2]; después de esto, en 1969, se consigue conectar también la computadora de la Universidad de California en Los Ángeles con otra del Instituto de Investigación de Stanford, siendo ya 4 universidades americanas interconectadas. Esta "red" se denominó ARPANET, cuyo objetivo principal era mantener comunicaciones en caso de posibles guerras.

Esta "red" de ARPANET sigue avanzando tecnológicamente con el paso del tiempo, dando lugar en 1970 a un sistema de comunicación mediante mensajería en red, el predecesor de lo que hoy en día conocemos como correo electrónico. Por esta época esta "red" ya formaba parte de las agencias militares, las universidades y los científicos la utilizaban para poder compartir opiniones y poder establecer colaboraciones en trabajos; es así que en 1972 la "red" ya estaba integrada en 50 universidades y centros de investigación a lo largo de todo EE.UU.

---

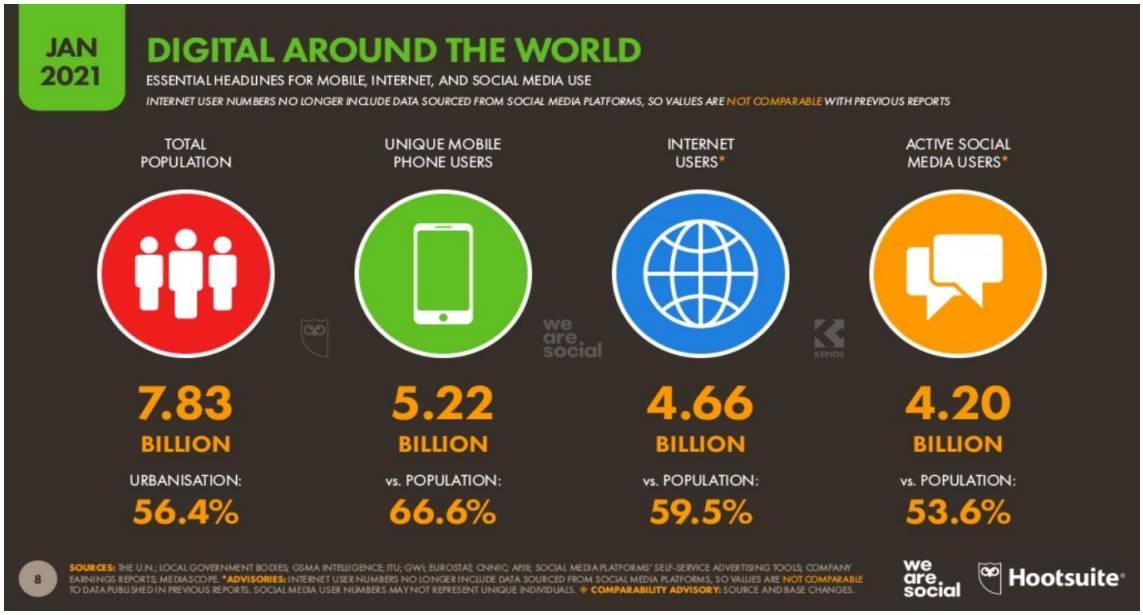
[1] FORERO Tatiana, *"*Conoce la historia de internet desde su nacimiento hasta lo que es hoy*". Rockcontent,* 17 de agosto de 2019. Recurso disponible en: https://rockcontent.com/es/blog/historia-del-internet/ [consulta: 23 de noviembre de 2021].

[2] BAHILLO Luis, "Historia de internet: como nació y cuál fue su evolución" *Marketing4commerce*, 16 de mayo de 2021. Recurso disponible en: https://marketing4ecommerce.net/historia-de-internet/ [consulta: 23 de noviembre de 2021]

No es hasta 1983 y 1989, y con el auge de la comercialización de computadoras de manera particular en los años 80, que se crean las primeras World Wide Web (www), y cuando toda esta información fue liberada a usuarios externos en agosto de 1991, dando pie a lo que hoy en día conocemos como “internet”.

Desde ese día y año tras año el crecimiento de usuarios en internet ha sido exponencial y esta cifra de crecimiento se ha visto impulsada de manera drástica con el nacimiento de los dispositivos móviles actuales donde internet está, literalmente, “en la palma de nuestra mano”.

En 2021, el 66% de los accesos a internet por parte de la sociedad alrededor del mundo fueron mediante el uso de teléfonos móviles, todo esto gracias a los grandes avances tecnológicos que permitieron llevar internet en el bolsillo o en el bolso de cualquier persona.



(Figura 1: Uso de internet en enero 2021)[3]

[3] Fuente de la imagen: BAHILLO Luis, “Historia de internet: como nació y cuál fue su evolución” *Marketing4commerce*, 18 de mayo de 2021. Recurso disponible en: https://marketing4ecommerce.net/historia-de-internet/ [consulta: 23 de noviembre de 2021]

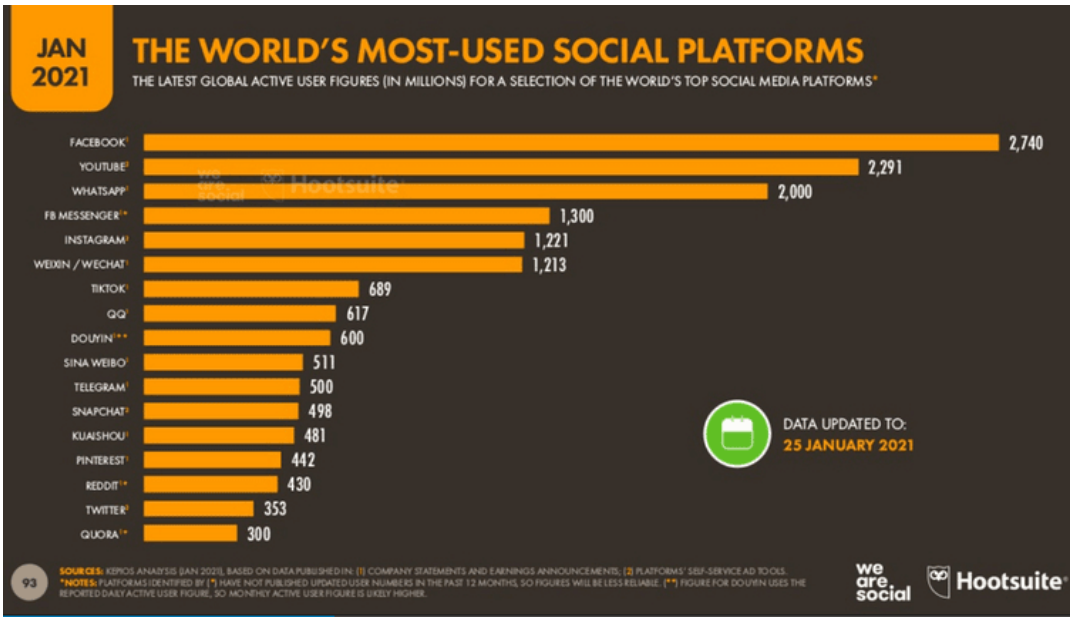
Todo esto se ve potenciado en un momento muy concreto en esta evolución de internet y su acceso por todo el mundo, momento que podemos denominar como "la era de las redes sociales"; esta empieza a mediados de los 90 con la creación de GeoCities, una web que alentaba a los usuarios a alojar sus propias páginas webs en sus servidores de manera totalmente gratuita, algo revolucionario en aquella época, hasta que fue comprado por la multinacional Yahoo! en 1999[4].

Gracias a la revolución de GeoCities y la facilidad de alojar multitud de páginas web en poco tiempo, en el año 2003 se crean redes sociales como MySpace y LinkedIn, pero no es hasta 2004 cuando un universitario de Harvard llamado Mark Zuckerberg crea la red social que a día de hoy es la más importante del mundo y la que revolucionó internet hasta ser lo que es hoy: Facebook.

Actualmente las redes sociales son las páginas que mayor tráfico de personas mueven a lo largo de internet; algunas, como Google+, se quedaron por el camino en esta "era de las redes sociales", pero otras consiguieron posicionarse entre las mejores aplicaciones sociales de la red, siendo utilizadas por millones de usuarios incluso en la actualidad: aplicaciones como Twitter, Twitch, WhatsApp, TikTok, Instagram, Facebook y YouTube entre las más famosas, siendo estas últimas las que más tráfico de personas manejan en la actualidad, con 2.740 millones de usuarios y 2.291 millones respectivamente[5].

[4] ORELLANA Rodrigo, "Qué fue de GeoCities, el desaparecido Beverly Hills de internet" *Digitaltrends,* 7 de abril de 2021. Recurso disponible en: https://es.digitaltrends.com/computadoras/que-fue-geocities/ [consulta: 23 de noviembre de 2021]

[5] BAHILLO Luis, "Historia de internet: como nació y cuál fue su evolución" *marketing4commerce*, 18 de mayo de 2021. Recurso disponible en: https://marketing4ecommerce.net/historia-de-internet/ [consulta: 23 de noviembre de 2021]



(Figura 2: Las redes sociales más usadas en 2021)[6]

Al igual que las redes sociales, la creación tan radical de infinidad de páginas web y la evolución paralela de los teléfonos móviles han hecho que los comercios físicos, los bancos, etc. también aprovechen estas nuevas tecnologías para ampliar aún más su radio de captación y venta, creándose el "e-commerce", es decir, el comercio electrónico, donde los vendedores ponen a un click de distancia del usuario el artículo que ellos quieran sin necesidad de salir de su domicilio, siendo plataformas como Amazon, Ebay, o Aliexpress las más famosas en este ámbito. Esto ha conseguido que muchos establecimientos hayan conseguido pasar de un comercio más local a un comercio prácticamente globalizado a todo el mundo en la mayor parte de los casos, incrementando sus beneficios de manera drástica en muy poco tiempo.

Como hemos podido ver, el internet que conocemos actualmente no tiene nada que ver al que existía hace 40 años. Se trata de una evolución histórica en muy pocos

[6] Fuente de la imagen: BAHILLO Luis, "Historia de internet: como nació y cuál fue su evolución" *Marketing4commerce*, 18 de mayo de 2021. Recurso disponible en: https://marketing4ecommerce.net/historia-de-internet/ [consulta: 23 de noviembre de 2021]

años que ha hecho avanzar a la sociedad a un mundo donde se puede encontrar todo tipo de información o relacionarte con cualquier persona a un click de ratón en un ordenador personal, o a un deslizamiento de pantalla en cualquier smartphone.

Pero no todo lo que ha generado internet son facilidades para el usuario para buscar información, encontrar entretenimiento de cualquier tipo o reencontrarse con aquellas personas que hace tiempo que no ve: existe otro lado oscuro de internet que también evoluciona al mismo ritmo o incluso más rápido, ya que, al igual que hay gente que hace buen uso de la red, como hemos mencionado anteriormente, también hay un resquicio de la sociedad que ha aprendido a usar estas nuevas tecnologías para lucrarse de manera ilícita a costa del desconocimiento de muchos otros, generando un nuevo estilo de delincuencia, la ciberdelincuencia, de la que hablaremos con más detalle a lo largo del trabajo.

Tras este concepto histórico vamos a entrar en detalle de cómo internet y los internautas pueden originar diversas situaciones en las que la red se convierte en una verdadera "selva" donde la gente puede estafar y ser estafada, robar y ser robada, traficar y ser parte de ese tráfico, etc. Comprobaremos cómo existe un mundo mucho más allá del internet convencional, un mundo donde todo puede ser objeto de peligro y delincuencia, el mundo de la Deep Web y sus consecuencias. Todo esto lo iremos desarrollando a medida que avancemos por los distintos epígrafes del trabajo. En concreto, en el apartado 2 veremos que es la ciberdelincuencia y que es lo que la caracteriza para que sea tan común actualmente. En el apartado 3 veremos como España se blinda ante todas estas nuevas formas de cometer delitos y como asegura

mediante su Ordenamiento Jurídico, la protección de los ciudadanos ante este tipo de delincuencia, etc. En concreto, en el apartado 2 […]. En el apartado 3, […], etc.

2. EL CRIMEN EN LA RED DEL SIGO XXI

No es de extrañar que a medida que avanza la sociedad a un terreno más digitalizado también lo haga la forma de socializar y de gestionar nuestro día a día delante de una pantalla.

Ya hablé de todo esto anteriormente en mi TFG "Los ciberdelitos"[7] y es que, a medida que la sociedad se globaliza y va adentrándose más y más en un mundo digitalizado donde internet es la base de todo lo que hacemos en nuestro día a día, también avanzan consigo las nuevas formas que tienen los delincuentes para cometer sus actos delictivos y lucrarse a costa de los demás.

¿Qué es el cibercrimen? Es una pregunta muy común para aquellas personas que no están acostumbradas a los términos virtuales. Para empezar, podemos decir que el cibercrimen y la ciberdelincuencia son todos aquellos delitos que los delincuentes comenten de manera general en la calle; robos, estafas, etc., pero llevados a un entorno virtual, es decir, internet. Cuando un delincuente comete un delito a través de internet, este está cometiendo un cibercrimen y por tanto una acción ilegal castigada por la ley.

En los últimos años se ha ido modificando la denominación de delitos informáticos por la de cibercrimen y cibercriminalidad. La utilización del término

[7] GALÁN AHUMADA, JAVIER, Los ciberdelitos, Tutor: Carlos García Valdés. Universidad de Alcalá de Henares, 2020, páginas 5-6.

cibercrimen viene de una traducción del término anglosajón Cybercrime, el cual procede de la unión del prefijo cyber (que viene a su vez del término cyberspace -ciberespacio-) y el término crime, utilizado en países como Estados Unidos, Inglaterra o Australia. En estos países utilizan esta expresión para hacer referencia a todo lo que tenga que ver con los ciberdelitos y la ciberdelincuencia, ya que no suelen hablar de Cybercriminality, ni de Ciberdelinquency. En España se utilizan en reiteradas ocasiones los términos ciberdelincuencia, cibercriminalidad y cibercrimen para referirse a un mismo significado, pese a ser unos términos que pueden, en muchas ocasiones, distanciarse entre sí.[8]

Miró Llinares, en su libro titulado "El cibercrimen", diferencia distintas fases en la evolución de la ciberdelincuencia a lo largo de los años, y las separa en forma de tres "generaciones". Una primera generación donde la cibercriminalidad se caracteriza por el uso de ordenadores para cometer delitos, una segunda donde la característica central es que el delito se comete a través de internet y, una tercera en la que los delitos están absolutamente determinados por el uso de internet y las TIC (tecnologías de la información y la comunicación).[9]

A su vez Miró Llinares también separa el cibercrimen en dos conceptos distintos, un concepto de cibercrimen amplio y otro más restringido. En el sentido más amplio del cibercrimen, Miró Llinares nos lo define como cualquier comportamiento delictivo realizado en el ciberespacio, mientras que en el sentido más restringido nos quiere dar a entender que para hablar de cibercrimen deberíamos acudir a la propia idea de la realización del delito por medio de las TIC.

[8] MIRÓ LLINARES, FERNANDO. *El cibercrimen.* Edit. Marcial Pons 2012, pág. 33, 37.
[9] Ídem, pág. 37.

Teniendo en cuenta esto, nos da a entender que solo se considerarían cibercrímenes aquellos comportamientos delictivos realizados en el ciberespacio cuya esencia de injusto no podría haberse cometido de ninguna otra forma fuera de él[10], es decir, un acto delictivo que única y exclusivamente se pudiese haber cometido a través de internet y el ciberespacio.

Los delincuentes han encontrado en internet un filón muy importante a la hora de cometer crímenes, ya que han pasado de una criminalidad local, centrada únicamente en su círculo de influencia más cercano, o nacional, donde los delincuentes más profesionales actúan en todo el territorio del Estado, a poder cometer sus actos en un entorno que engloba a todo el mundo, un entorno en donde con un simple click de ratón, el delincuente puede ganar dinero sin mucho más esfuerzo que el de engañar a su víctima.

Otros de los problemas que nos encontramos en la red son los propios internautas. Un entorno digital y libre de cualquier control, donde cualquier persona puede colgar o comentar cualquier cosa sin ningún tipo de limitación y acompañándolo de la capacidad de anonimato que proporciona internet, produce que las personas creen contenido de dudosa ética, basados en destruir conceptos tan básicos como el honor y el respeto de los demás internautas, produciéndose amenazas y cyberbullying entre los distintos individuos de la red. Como bien dijo

[10] MIRÓ LLINARES, FERNANDO. *El cibercrimen.* Madrid: Edit. Marcial Pons, 2012, pág. 41-42.

Thomas Hobbes en su obra "Leviatán" de 1651: "El hombre es un lobo para el hombre"[11].

Existen infinidad de delitos que se pueden cometer a través de la red, y nuestro Ordenamiento Jurídico a lo largo de los años ha ido modificándose y actualizándose para dar cabida a todas estas nuevas formas de cometer actos ilícitos. En el siguiente apartado vamos a ofrecer una panorámica general de los principales delitos, aclarando el bien jurídico protegido en cada uno de los casos, para posteriormente, en los epígrafes posteriores, profundizar en dos de ellos en concreto, los delitos más comunes: (i) la estafa y sus distintas modalidades, entre ellas el phishing, y (ii) la pornografía infantil; la cual es fácil de encontrar de encontrar si navegamos más allá de lo que nos proporcionan nuestros navegadores convencionales y nos adentramos en el mundo más allá del internet convencional, es decir, nos adentramos en la popularmente conocida Deep Web.

[11] ARRIETA, EVER. *"*El hombre es un lobo para el hombre (homo homini lupus)*" Cultura genial*. Recurso disponible en: https://www.culturagenial.com/es/el-hombre-es-un-lobo-para-el-hombre/ [Consulta: 16 de febrero de 2022]

3. El ORDENAMIENTO JURÍDICO EN LA CIBERDELINCUENCIA

España, en materia de ciberdelincuencia, ha optado por regularla mediante una serie de reformas en el propio Código Penal, dejando de lado la creación de una Ley penal especial para esta serie de delitos. Sin embargo, ni el código penal de 1995 o sus sucesivas reformas han destinado un Título específico para dedicarlo a los delitos informáticos[12].

El abogado Moisés Barrio Andrés en su monografía "Ciberdelitos: amenazas criminales del ciberespacio" nos hace una clara clasificación de los diversos tipos de ciberdelitos que podemos encontrar en nuestro Código Penal, dividiéndolos en distintos apartados, a saber[13]:

3.1. Delitos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos[14]:

En este apartado nos encontramos los delitos de intrusismo recogidos en el artículo 197.1 y ss del Código Penal, así como la protección de datos, los daños y sabotajes (cracking) y el abuso de sistemas informáticos (phreaking)

En el artículo 197 bis y siguientes, destinados a condenar los accesos no autorizados a sistemas informáticos así, podemos encontrar lo siguiente:

[12] BARRIO ANDRÉS, MOISÉS. *Ciberdelitos: amenazas criminales del ciberespacio.* Edit. Reus. Madrid. 2017. *Revista de las Cortes Generales*, 83, 2011, pág.[las páginas no son correctas, pues este artículo tiene páginas numeradas dentro de la revista]56-57.
[13] BARRIO ANDRÉS, MOISÉS. *Ciberdelitos: amenazas criminales del ciberespacio.* Edit. Reus. Madrid. 2017. *Revista de las Cortes Generales*, 83, 2011, pág.62.
[14] Idem.

197 bis: *"1. El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.*

2. El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses."

197 ter: *"Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:*

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información."[15]

[15] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Relativo a los Daños y sabotajes, el cual Moisés Barrio Andrés lo denomina "vandalismo digital"[16], se integran en esta categoría todas aquellas anomalías que perjudiquen el correcto funcionamiento de un medio digital e informático (virus, worms, crackings, etc), esto nos lo encontramos en el Código Penal en su artículo 264:

"1. El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años…"[17].

A si mismo, el articulo 256 del Código penal castiga a todo aquel que haga un uso de cualquier equipo o terminal de telecomunicación sin consentimiento para el titular y causando a este un perjuicio económico (phreaking)[18]:

"1. El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, y causando a éste un perjuicio económico, será castigado con la pena de multa de tres a doce meses…"[19].

[16] BARRIO ANDRÉS, MOISÉS. *Ciberdelitos: amenazas criminales del ciberespacio.* Edit. Reus. Madrid. 2017. Pág. 82.
[17] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
[18] BARRIO ANDRÉS, MOISÉS. *Ciberdelitos: amenazas criminales del ciberespacio.* Edit. Reus. Madrid. 2017. pág.91.
[19] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

3.2. Delitos asociados a la informática[20]:

Entran en esta categoría todas las estafas y fraudes cometidos en internet tipificados en el artículo 248 del código penal[21].

Este grupo de delitos son aquellos delitos tradicionales que se han visto actualizados a las nuevas tecnologías por parte de los delincuentes para poder lucrarse a costa del resto de personas, utilizando internet para ampliar el alcance de sus delitos hasta lugares incalculables, delitos como la estafa, el carding o el phishing entran dentro de esta categoría, por ello el articulo 248 estipula lo siguiente:

"1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

[20] BARRIO ANDRÉS, MOISÉS. *Ciberdelitos: amenazas criminales del ciberespacio.* Edit. Reus. Madrid. 2017. Pág. 94.
[21] Idem.

c) Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero."[22].

De entre todos estos delitos, vamos a dedicar un apartado concreto al Phishing donde lo analizaremos en el siguiente epígrafe con mucho más detalle, junto con algunos otros delitos como la estafa nigeriana o las estafas a través de compras online, todo esto debido que son delitos que están cogiendo cada vez más ventaja en internet con respecto al resto gracias a la facilidad de "gancho" que tienen frente a los internautas.

3.3. Delitos de contenido y relativos a las infracciones contra la propiedad intelectual.[23]:

Pertenecen a esta categoría todos los delitos que persiguen la creación, publicación y distribución de contenidos ilegales[24], como son la pornografía infantil, el grooming y como infracciones contra la propiedad intelectual, la piratería.

Los abusos sexuales a menores vienen recogidos en el articulo 183 del Código penal, pero es el articulo 183 ter, el que recoge todo lo que atañe a este mismo delito dentro de un entorno en red:

"1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga

[22] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
[23] BARRIO ANDRÉS, MOISÉS. *Ciberdelitos: amenazas criminales del ciberespacio.* Edit. Reus. Madrid. 2017. Pág 101.
[24] Idem.

concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.

2. El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años."[25]

Sin embargo, no es el articulo 183 el que recoge todo lo relativo a la pornografía infantil, este delito tiene su propio artículo del Código penal, ya que no solo se castiga a quien realice el contenido ilegal, sino también a quien lo posea y lo distribuya mediante cualquier medio de difusión, este artículo es el 189, el cual nos detendremos y analizaremos con algo más de detalle en el siguiente apartado del trabajo.

Por parte de la difusión de contenidos que están protegidos por la ley de propiedad intelectual, es el artículo 270.1, 270.2 y ss del Código Penal el encargado de velar por este bien jurídico protegido:

"1. Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo

[25] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios."[26]

Como podemos ver, las leyes españolas también protegen aquello que va más allá de los delitos comunes, la sociedad avanza y con él las maneras de cometer delitos por parte de los delincuentes, es por ello que los Ordenamientos Jurídicos tienen que actualizarse también para poder proteger en todo momento los intereses de sus ciudadanos, bien mediante reformas o bien por medio de leyes especiales concretas creadas para dicho fin.

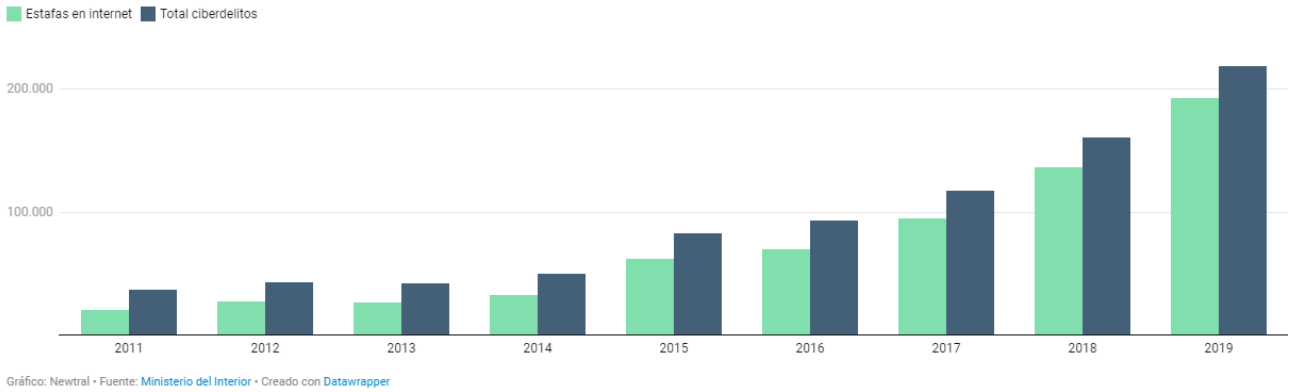
[26] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

4. LA ESTAFA Y SUS FORMAS DENTRO DE LA RED

Con el paso de los años, los distintos distribuidores de servicios de internet han estado trabajando duro para poder suministrar al usuario un internet libre y seguro, para proporcionar un entorno al internauta que pueda disfrutar sin mayor preocupación que la de encontrar lo que está buscando. Esto ha producido que con el paso de los años y acompañado de mucho desconocimiento por parte de algunos miles de usuarios de internet, muchos de ellos hayan podido ser víctimas de alguna estafa o robo de información en internet, creyendo que la información que están proporcionando al sitio web es segura o que lo que están comprando por internet es real.

En España uno de los delitos más comunes en internet es la estafa, que engloba miles y miles de actividades delictivas, entre ellas una que está cogiendo cada vez más fuerza y se está poniendo más y más de moda por parte de los delincuentes gracias a su fácil utilización y los rápidos beneficios que proporciona: el Phishing, una práctica habitual en la que el delincuente se hace pasar por otra persona o entidad con el propósito de conseguir datos sensibles de su víctima, tales como cuentas de acceso a redes sociales, donde conseguir infinidad de información, o incluso a cuentas bancarias, con los perjuicios que ello conlleva. El Sistema Estadístico de Criminalidad (SEC), gestionado por el Ministerio del Interior, recogió que, en el año 2019, el 88% de los delitos denunciados correspondían a fraudes online[27].

[27] PASCUAL María "Las estafas por internet representan más del 80% de los ciberdelitos" *Newtral*, 06 de agosto de 2021. Recurso disponible en: https://www.newtral.es/estafas-internet-ciberdelitos/20210806/ [Consulta: 16 de febrero de 2022]



(Figura 3: Evolución de los ciberdelitos registrados en España desde 2011)[28]

Como se puede ver en la gráfica anterior, extraída del medio web Newtral y con datos proporcionados por el Ministerio del Interior, en los últimos 9 años, las denuncias por fraudes online se han multiplicado exponencialmente desde 2011, pasando de 21.075 en 2011 a 192.375 en 2019. En los años posteriores, y con la pandemia del Covid-19 en auge, cuando se sufrió un confinamiento masivo de la sociedad y se multiplicaron los accesos a internet y utilización de servicios en línea tanto como método de entretenimiento como en forma de consumo con las compras on-line, este tipo de denuncias se mantuvo más o menos en las mismas cifras; Jorge Chinea, responsable de Ciberseguridad en Servicios Reactivos del Centro de Respuesta a Incidentes de Seguridad del Instituto Nacional de Ciberdelincuencia (INCIBE-CERT), explicó al medio web Newtral.es que se registraron más de 130.00 incidentes de ciberdelincuencia, de los cuales un 32% correspondían a fraudes[29].

[28] Fuente de la imagen: PASCUAL María "Las estafas por internet representan más del 80% de los ciberdelitos" *Newtral*, 06 de agosto de 2021. Recurso disponible en: https://www.newtral.es/estafas-internet-ciberdelitos/20210806/ [Consulta: 16 de febrero de 2022]

[29] PASCUAL María "Las estafas por internet representan más del 80% de los ciberdelitos" *Newtral*, 06 de agosto de 2021. Recurso disponible en: https://www.newtral.es/estafas-internet-ciberdelitos/20210806/ [Consulta: 16 de febrero de 2022]

Desde 2011, la cantidad de detenciones e investigaciones por prácticas de este tipo ha crecido exponencialmente. En 2019 se produjeron 8.914 detenciones por ciberdelitos en internet, según el Ministerio del Interior, más de la mitad fueron a causa de fraudes informáticos, seguido de otros delitos como amenazas y coacciones, y delitos de índole sexual[30].

Teniendo en cuenta todos estos datos, podemos comprobar cómo internet, aunque parezca un entorno seguro y los proveedores de servicios de este tipo trabajen continuamente para que esto sea así, no es cien por cien seguro, y es necesario también una labor de concienciación e información por parte del usuario, no hay mejor escudo ante este tipo de actos que el conocimiento y la precaución del propio usuario.

A continuación, vamos a desglosar un poco en qué consiste la estafa dentro de internet, así como algunas de las prácticas utilizadas por los ciberdelincuentes para poder realizar estos delitos de estafa y robos de información.

La estafa es uno de los delitos más antiguos del mundo, y al igual que la sociedad avanza, los estafadores y las estafas avanzan con ella para adaptarse y seguir pudiendo lucrarse de los demás. Los estafadores han encontrado en internet un mundo completamente nuevo donde poder expandir su capacidad de engaño a límites prácticamente imposibles de controlar.

La estafa está regulada en el Código Penal español en su artículo 248 y ss., el cual castiga a aquella persona que, "*con ánimo de lucro, utilizare engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio*

[30] PASCUAL María "Las estafas por internet representan más del 80% de los ciberdelitos" *Newtral*, 06 de agosto de 2021. Recurso disponible en: https://www.newtral.es/estafas-internet-ciberdelitos/20210806/ [Consulta: 16 de febrero de 2022]

o ajeno". En su apartado segundo a), el articulo 248 estipula que "*también es reo de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro."*[31]

Los estafadores han combinado su capacidad de engaño que ya utilizaban anteriormente en sus delitos en el "entorno físico" fuera de la red, con el desconocimiento y la inocencia de muchas personas del uso de internet, para poder acceder a unos beneficios ilícitos rápidos y eficaces sin necesidad de hacer un gran sobre esfuerzo ni un gran despliegue de medios para poder cometer dichos delitos, simplemente un ordenador y paciencia.

Existen distintos tipos de estafa dentro de internet, pero las más comunes y que se puede encontrar cualquier persona en su día a día simplemente navegando por su buscador web de confianza o revisando sus correos electrónicos son: las distintas modalidades de estafa nigeriana utilizadas por los delincuentes para engañar a la víctima con una recompensa, por regla general económica, a cambio de datos o una pequeña suma de dinero; las compras on-line, donde el cliente compra un artículo en alguna web y jamás recibe el mismo o lo que recibe no se adapta a aquello que ha comprado, el phishing y otras muchas más. A continuación, expondremos las tres primeras.

[31] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 [Consulta: 16 de febrero de 2022]

4.1.1. Estafa nigeriana.

Las estafas nigerianas son los tipos de estafa más comunes en la red, sobre todo desde la existencia de los correos electrónicos "modernos" tal y como los conocemos actualmente.

Todo el mundo ha debido recibir alguna vez en su correo electrónico, ya sea de empresa o personal, algún correo extraño de alguien que no conoce pidiéndole ayuda para algo u ofreciéndole una suma de dinero alta, a cambio de un ingreso previo en una cuenta bancaría de una suma de dinero ínfima o muy inferior a la ofertada. Este es el modus operandi básico de las estafas nigerianas, también conocidas como timo 419; que hace referencia al artículo del código penal nigeriano al que se refiere este tipo de delitos[32].

Con el paso de los años las variantes de este tipo de estafa han ido cambiando y adaptándose a los distintos medios que han ido saliendo a la luz dentro de la red, pasando por estafas en herencias, intentando hacer creer a la víctima que ha ganado una herencia millonaria y que, para recibirla, debe hacer un ingreso "X" en una cuenta bancaría en concreto; estafas amorosas, de venta de vehículos, etc.

Hay un ejemplo claro de este tipo de estafas que está cogiendo mucha fuerza en redes sociales en los últimos meses y que se realiza a través de medios como el correo electrónico o medios de mensajería instantánea tales como WhatsApp o Telegram, donde el estafador intenta hacerse pasar por algún familiar cercano de la víctima que lleva años sin ver ni tener ningún tipo de contacto, engañando a la misma para que le

[32] EQUIPO AYUDALEY "La estafa nigeriana o timo 419" *Ayudaley*. Recurso disponible en: https://ayudaleyprotecciondatos.es/2021/01/18/estafa-nigeriana-timo-419/ [Consulta: 16 de febrero de 2022].

diga un nombre de algún familiar con la intención de ganarse su confianza para después poder poner en marcha la estafa.

Mediante esta estafa, el delincuente hace creer al usuario que está de vuelta al país de residencia de esta, pero en el trayecto pierde el vuelo, y sus maletas parten con el avión destino al país donde vive la víctima. El delincuente pide a su objetivo que se haga cargo de dicho equipaje, ya que no quiere perder el contenido del mismo en el cual, normalmente, hay alguna suma de dinero; para ello le comunica que se va a poner en contacto con él un agente del aeropuerto para poder cogerle los datos y una pequeña cantidad de dinero en concepto de "fianza" por dichas maletas.

Esta es una práctica que se ha estado dando en muchos puntos geográficos de España y Latinoamérica, y respecto de la cual muchos usuarios en redes sociales han ido posteando sus experiencias.

En el Anexo I al final de este trabajo estarán algunos ejemplos de esta modalidad de estafa nigeriana, imágenes posteadas en la red social Twitter y cedidas para este trabajo por el usuario *"Kalipo de melocotón (@Kalipo20206");* en dicho anexo se puede observar el "modus operandi" de estos delincuentes y, aunque el propio usuario los responde de manera paródica, puesto que es consciente de que se trata de una estafa, es una buena manera de ilustrar la forma de trabajo que tienen los mismos y advertir de las consecuencias que se puedan derivar en caso de que el delincuente consiga su objetivo.

Otro ejemplo de este tipo de estafas, bastante común en internet, es la estafa de las herencias, donde el estafador escribe a su objetivo por medio de alguno de los métodos de comunicación de la red, para hacerle saber que quiere transmitirle todo su

patrimonio por medio de una herencia de manera totalmente desinteresada, para ello pide a la víctima una serie de datos personales y bancarios para poder realizar el "testamento" o el ingreso del capital prometido, con el simple objetivo de conseguir datos sensibles del usuario para poder acceder a cuentas bancarias o contenidos personales de esta.

En el Anexo II al final de este trabajo estarán las imágenes que ilustran este tipo de estafa, imágenes cedidas por el creador de contenido online "*Tamayo (@Tamayostuff)"* y posteadas en su red social Instagram.

Con estos métodos el estafador va consiguiendo pequeñas cantidades de dinero, que dependiendo de la estafa nigeriana son de unas cantidades u otras, a costa de la ingenuidad y el desconocimiento de su víctima.

Por regla general son cantidades de dinero pequeñas para que no salten las alarmas frente a los cuerpos de seguridad del Estado; esto hace que, gracias a la capacidad que proporciona internet de poder compartir y extender cualquier noticia o información de manera rápida y a cualquier parte del mundo en muy poco espacio de tiempo, los estafadores consigan una suma de capital bastante elevada sin ningún tipo de esfuerzo y con los mayores beneficios posibles.

4.1.2. Compras On-Line.

Muchísimos usuarios han ido adaptando su forma de comprar con el paso de los años, pasando de realizar sus compras de manera física en los comercios existentes en su zona de influencia, a realizar compras de manera telemática u online; esto se ha visto incrementado en gran medida desde que existen plataformas de comercio puramente virtuales como los Marketplace de Amazon o Aliexpress, donde cada día reciben

millones de pedidos de millones de usuarios que realizan sus compras por dichas plataformas.

Este tipo de comercio está en auge a día de hoy, y se ha visto incrementado aún más desde el comienzo de la pandemia en 2020, donde el confinamiento de la sociedad en sus domicilios impulsó que el comercio electrónico se viese incrementado en un 46% en 2020 con respecto a años anteriores, promovido también por el cierre de establecimientos y comercios no esenciales.[33] En este periodo el mayor número crecimiento de ventas fueron a parar a la compra de prendas de vestir, grandes almacenes, suscripción de plataformas de entretenimiento, etc..

(Figura 4: Las 10 actividades con mayor % de transacciones del comercio electrónico)[34]

Este incremento en el comercio electrónico también abre las puertas a los delincuentes para aprovecharse de la situación e intentar lucrarse económicamente de los usuarios de internet, intentando enganchar a estos con anuncios falsos y jugosos

[33] EQUIPO ITRESELLER "El comercio electrónico aumentó casi un 50% en el año de la pandemia" *Itreseller*, 21 de julio de 2021. Recurso disponible en: https://www.itreseller.es/al-dia/2021/07/el-comercio-electronico-aumento-casi-un-50-en-el-ano-de-la-pandemia [Consulta: 16 de febrero de 2022]

[34] Fuente de la imagen: CNMC "El comercio electrónico superó en España los 12.400 millones de euros en el primer trimestre de 2021, casi un 2% más que el año anterior" *Cnmc*, 08 de octubre de 2021. Recurso disponible en: https://www.cnmc.es/prensa/ecommerce-1T-20211008 [Consulta: 16 de febrero de 2022]

para que piquen y compren algo que no les va a llegar nunca, o que no se adapta en ninguno de los casos a lo que el usuario compró en realidad.

Los ciberdelincuentes se caracterizan por su gran capacidad de adaptación al medio en el que van a delinquir, es así que saben qué es lo más óptimo en cada situación y aprovechan eso para intentar engañar al usuario; utilizando periodos de rebajas o acontecimientos relevantes como San Valentín, Navidades o el Black Friday para colocar ofertas jugosas para la víctima y que esta muerda el anzuelo de la estafa. Durante los primeros meses de pandemia, por ejemplo, los incidentes más habituales de fraude estaban enfocados sobre todo en productos sanitarios, servicios de mensajería y plataformas digitales, así como los relacionados con los ERTE, como explica Jorge Chinea en el medio online Newtral.es[35]

Para evitar este tipo de prácticas por parte de los ciberdelincuentes es necesario por parte del usuario que ponga atención a aquello que está comprando y en qué web lo está haciendo, haciendo una labor de investigación para saber si esa web es de confianza o es una página de dudosa procedencia, si tiene algún tipo de valoración por parte de otros usuarios y sobre todo no dejarse engañar por ofertas de dudosa legitimidad.

También es recomendable no pagar mediante el uso de tarjeta de crédito y utilizar métodos alternativos de pago, tales como PayPal, ya que así evitamos el posible robo de nuestros datos bancarios en caso de estafa.

[35] PASCUAL María "Las estafas por internet representan más del 80% de los ciberdelitos" *Newtral*, 06 de agosto de 2021. Recurso disponible en: https://www.newtral.es/estafas-internet-ciberdelitos/20210806/ [Consulta: 16 de febrero de 2022]

4.1.3. Phishing.

El phishing es uno de los métodos más conocidos en el entorno virtual de robo de información que utilizan los delincuentes en la actualidad para hacerse con información personal y sensible de sus víctimas de una manera sencilla y efectiva.

El ciberdelincuente utiliza entidades muy conocidas o "ganchos" de atracción mediante correos, spam, o mensajería SMS, entre otras, para conseguir engañar al usuario y que así introduzca sus datos en los enlaces web que crean los estafadores para este propósito; estas páginas web suelen ser clones prácticamente perfectos de las páginas web legitimas para generar así un sentimiento de confianza por parte de la víctima y conseguir así que caiga en la estafa de manera más sencilla.

Para tratar todo este apartado de Phishing voy a usar como referencia una conferencia pública de más de 20 minutos, del instituto nacional de ciberdelincuencia (INCIBE), publicado en la plataforma YouTube y protagonizada por Josep Albors, un profesional con más de 12 años de experiencia en el mundo de la ciberseguridad.

A lo largo de los años los casos de Phishing han ido creciendo y evolucionando de manera exponencial, engañando y estafando a miles de millones de usuarios de internet en todo el mundo. En 2018 del porcentaje total de correos electrónicos que llegaban a las bandejas de entrada de los internautas, el 55% de dichos correos tenían algún contenido Phishing, con intención de comprometer la seguridad del usuario.

Estos datos son recogidos por la empresa Microsoft y expuestos en la conferencia de Josep Albors donde se puede apreciar un aumento significativo de los correos destinados al phishing desde enero de 2018 a diciembre de ese mismo año, aunque los datos sean de 2018 hay que destacar que todo este contenido ha ido

creciendo cada vez más en los años posteriores, creandose por parte de los estafadores metodos cada vez más innovadores y mejor conseguidos para sobreponerse al aumento de conocimientos que consiguen los usuarios los cuales, aunque sean cada vez más desconfiados, siguen cayendo una y otra vez en este tipo de estafas tan comunes[36].

(Figura 5: porcentaje de correos Phishing en 2018)[37]

Existen multitud de ejemplos de phishing en internet, donde el estafador utiliza la confianza del usuario en alguna entidad concreta para poder acceder a sus datos personales; un claro ejemplo de este phishing es el phishing bancario.

El estafador por medio de un correo electrónico envía a la víctima una supuesta vulneración de datos de su clave y contraseña, y solicita a este el cambio de la misma haciendo click en un enlace que proporciona el mismo correo; una vez dado click en el

[36] ALBORS, JOSEP. "¿Por qué el phishing sigue siendo tan efectivo?" *INCIBE, #CyberCamp19* [Vídeo en línea]. Publicado el 29 de enero de 2020. Disponible en: https://www.youtube.com/watch?v=1gNhHmM1tdQ&t=120s

[37] Fuente de la imagen: ALBORS, JOSEP. "¿Por qué el phishing sigue siendo tan efectivo?" *INCIBE, #CyberCamp19* [Vídeo en línea]. Publicado el 29 de enero de 2020. Disponible en: https://www.youtube.com/watch?v=1gNhHmM1tdQ&t=120s

enlace, este redirige a una web prácticamente idéntica a la de tu banco de confianza para que introduzcas tu usuario y contraseña, una vez introducidos el estafador ya tiene total acceso a tu plataforma de banca online.

Para evitar este tipo de situaciones hay que mirar detenidamente la dirección desde donde se envía dicho correo y desconfiar si no es una dirección oficial del Banco; a su vez, cabe resaltar que ningún banco suele pedir ningún tipo de información confidencial de esa índole al usuario precisamente para evitar este tipo de situaciones, ni tampoco ningún enlace donde tenga que acceder el usuario.

Otro tipo de phishing que nos podemos encontrar es el phishing en servicios de almacenamiento en la nube, tales como Dropbox, iCloud, OneDrive o Google Drive; donde el estafador utiliza el mismo método que con el phishing bancario para poder acceder a los datos en la nube de tu cuenta, normalmente para luego usarlos como método de extorsión y conseguir un beneficio económico de ello. Otros métodos de phishing conocidos son el Phishing de servicios online como Netflix o Disney+ o phishing por mensajería instantánea tales como WhatsApp o Telegram, aprovechando algún "gancho" al usuario como cupones gratis o descuentos elevados.

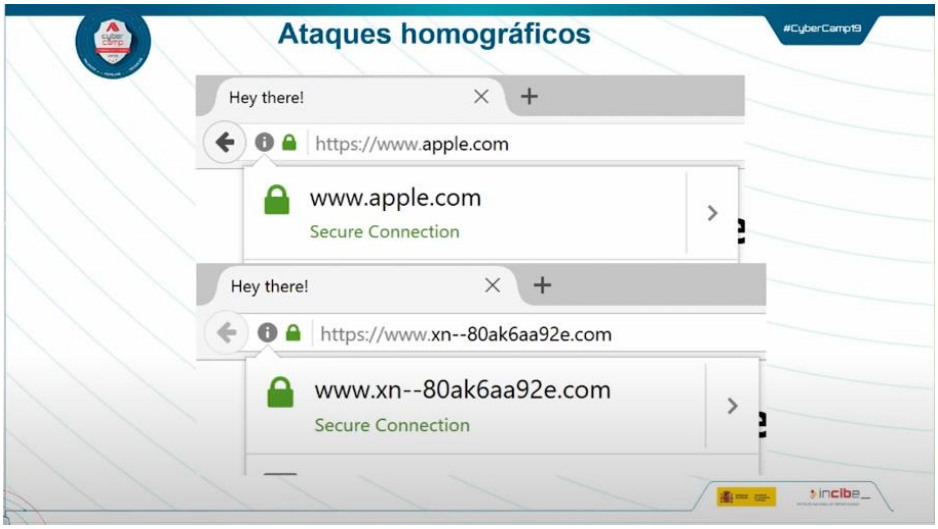
(Figura 6: Phishing en WhatsApp)[38]

Este problema se ve aún más incrementado cuando el usuario no cambia sus claves con asiduidad o cuando tiene la misma contraseña para más de un servicio: con solo conseguir de manera efectiva que la víctima caiga en un caso de phishing, podría tener acceso a multitud de servicios de la persona, incluyendo en algunos casos acceso a cuentas de empresa de esta.

Cada vez es más y más difícil diferenciar una página web real de una fraudulenta debido a que los estafadores cada vez innovan más en cómo gestionar una web para que parezca lo más real posible para así conseguir engañar al usuario y futura víctima. Así es como los delincuentes utilizan programas y métodos de escritura digital como por ejemplo caracteres Unicode, para simular una dirección web real donde en realidad contiene una web fraudulenta destinada al robo de información personal o datos de tarjetas bancarias de las víctimas; esto se conoce como ataques homográficos.

[38] Fuente de la imagen: INCIBE, 2020. ¿Por qué el phishing sigue siendo tan efectivo? – Josep Albors #CyberCamp19. En *YouTube* [Video en línea]. Publicado el 29 de enero de 2020. Disponible en: https://www.youtube.com/watch?v=1gNhHmM1tdQ&t=120s

Los distintos proveedores de navegación web tales como Chrome o Firefox, cada vez proporcionan más información al usuario del enlace web al que están accediendo dificultando la codificación de estos lenguajes especiales y alertando al internauta de manera más sencilla, pero dependiendo de que navegador utilices estas funciones no están disponibles, sobre todo si el acceso es desde un dispositivo móvil.



(Figura 7: Ejemplo Ataque homográfico con codificación Unicode)[39]

El phishing va mucho más allá del robo de información por parte del estafador a su víctima. En multitud de ocasiones este phishing también es utilizado como medio de extorsión para conseguir alguna cantidad económica por parte de la persona estafada, donde el delincuente consigue robar, o no, información sensible del usuario para posteriormente amenazarle con hacerla pública o eliminarla si no realiza un ingreso a una cartera cripto en un plazo determinado de tiempo. Para este tipo de extorsiones se

[39] Fuente de la imagen: INCIBE, 2020. ¿Por qué el phishing sigue siendo tan efectivo? – Josep Albors #CyberCamp19. En *YouTube* [Video en línea]. Publicado el 29 de enero de 2020. Disponible en: https://www.youtube.com/watch?v=1gNhHmM1tdQ&t=120s

utilizan las carteras cripto y las transferencias en criptomoneda gracias a la seguridad y la imposible trazabilidad que proporcionan dichas transacciones[40].

Para evitar todo este tipo de situaciones, los proveedores de servicios digitales y todas las páginas web están empezando a implementar las verificaciones de identidad en dos o incluso tres pasos, donde para acceder al sitio donde el usuario está intentando entrar ya no es necesario solo el introducir el usuario y la contraseña, sino también otra serie de autentificadores externos que aseguren que el que accede a dicho sitio web es el usuario legítimo; se trata de verificaciones como códigos mediante correo electrónico o mediante SMS al móvil que el usuario debe introducir en la web para acceder, o como la utilización de programas externos que guardan un código o semilla (seed) como Google Authenticator.

Las entidades bancarias, para evitar la posible utilización de los sistemas online para comprar fraudulentamente por parte del estafador que haya podido hacerse con los datos bancarios de algún usuario, piden la autentificación y la autorización por parte del usuario de dicha transacción por medio del acceso a su plataforma de banca online en su teléfono móvil.

Como hemos podido comprobar, internet es un entorno muy enriquecedor para cualquier persona, pero hay que usarla con cuidado, pues con el suficiente desconocimiento y desinformación del internauta acerca de lo que pasa en la red,

[40] ALBORS, JOSEP. "¿Por qué el phishing sigue siendo tan efectivo?" *INCIBE, #CyberCamp19* [Vídeo en línea]. Publicado el 29 de enero de 2020. Disponible en: https://www.youtube.com/watch?v=1gNhHmM1tdQ&t=120s

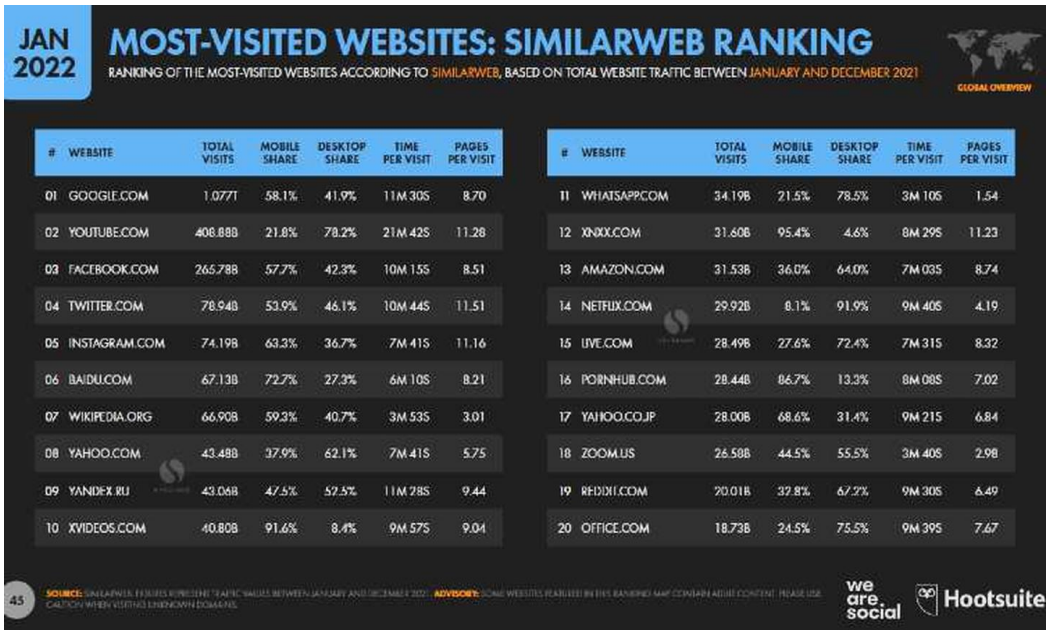
cualquier persona con intenciones poco loables puede tener acceso a infinidad de información y poder utilizarlos para su beneficio personal.

Para finalizar este apartado, cabe señalar que internet no solo está en lo que vemos y navegamos en el día a día: existe un mundo mucho más allá de la red convencional que se usa de manera cotidiana, donde ya no existe un control por parte de servicios y entidades destinadas a ello; hay un entorno mucho más grande fuera de la red estándar, utilizado por los delincuentes para poder realizar sus operaciones delictivas y mucho más: esta es la Deep Web, la cual explicaremos y analizaremos con mucha más profundidad en los epígrafes siguientes.

5. LA PORNOGRAFÍA COMO DELITO

La pornografía en sentido estricto no esta penada por ningún Ordenamiento Jurídico, ya que esta de por sí no es delito, siempre y cuando se realice entre personas con mayoría de edad y se realice de manera consentida y consensuada entre todos los que formen parte de las escenas realizadas.

La pornografía en sí nace como un medio para satisfacer una necesidad fisiológica de una persona sea hombre o mujer, y por esta misma razón siempre podemos encontrar páginas de carácter pornográfico, entre el top veinte de más visitas en todo el mundo, es así como por ejemplo en enero de 2022 páginas web como xvideos.com o pornhub.com se colocaron entre las 20 páginas web más vistas en el mundo, la número 10 y la 16 más concretamente.



(Figura 8: páginas más visitadas en el mundo en enero de 2022)[41]

El momento en el que la pornografía pasa de ser una forma de satisfacción a una sociedad a un delito, es cuando se vulneran los derechos inalienables de cualquier persona; pero ello no por la realización de porno, sino por la comisión para su realización de delitos como amenazas, coacciones, lesiones, abusos sexuales y violación, entre otros.

Sin embargo, existe una situación donde la pornografía sí es delito en sí misma, y es cuando para la realización de la misma entran en escena personas menores de edad o determinadas personas con discapacidad; en ese preciso momento la pornografía pasa a denominarse pornografía infantil y es aquí donde verdaderamente existe delito castigado por el Código Penal, delito con penas muy severas.

El delito de pornografía infantil está regulado en el artículo 189 del Código Penal, el cual condena en todos sus apartados a aquellas personas que difundan, almacenen,

[41] Fuente de la imagen: Equipo FayerWayer "Porno en la web se posiciona en el Top Ten de Internet con XVideos.com" *FayerWayer*, 25 de marzo de 2022. Recurso disponible en: https://www.fayerwayer.com/internet/2022/03/25/porno-en-la-web-se-posiciona-en-el-top-ten-de-internet-con-xvideoscom/ [Consulta: 1 de julio de 2022]

vendan, produzcan o exhiban cualquier medio de pornografía infantil con una pena de prisión de uno a cinco años. Este artículo también nos da una concepción bastante detallada de lo que se considera pornografía infantil para el Ordenamiento Jurídico, estipulando la siguiente definición citada textualmente del código penal:

"A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.

b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.

c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales."[42]

[42] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 [Consulta: 1 de Julio de 2022]

El articulo 189.2 en todos sus apartados está dedicado a su vez, a agravar las penas recogidas en el 189.1 cuando concurran una serie de circunstancias, estas circunstancias son las siguientes:

"2. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:

a) Cuando se utilice a menores de dieciséis años.

b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio, se emplee violencia física o sexual para la obtención del material pornográfico o se representen escenas de violencia física o sexual.

c) Cuando se utilice a personas menores de edad que se hallen en una situación de especial vulnerabilidad por razón de enfermedad, discapacidad o por cualquier otra circunstancia.

d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

e) Cuando el material pornográfico fuera de notoria importancia.

f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

g) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, de la persona menor de edad o persona con discapacidad necesitada de

especial protección, o se trate de cualquier persona que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.

h) Cuando concurra la agravante de reincidencia."[43]

Los siguientes puntos del articulo 189 están dedicados a proteger todos aquellos puntos donde el menor se pueda ver vulnerado de cualquier manera, siendo por ejemplo potestad de fiscales y jueces y de los tutores de los menores, la capacidad y obligación de actuar frente a aquellas acciones donde el menor se haya visto o pudiese haberse visto perjudicado:

"3. Si los hechos a que se refiere la letra a) del párrafo primero del apartado 1 se hubieran cometido con violencia o intimidación se impondrá la pena superior en grado a las previstas en los apartados anteriores

4. El que asistiere a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de seis meses a dos años de prisión.

5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

[43] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 [Consulta: 1 Julio de 2022]

La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación.

6. El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o una persona con discapacidad necesitada de especial protección y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o persona con discapacidad necesitada de especial protección, será castigado con la pena de prisión de tres a seis meses o multa de seis a doce meses.

7. El Ministerio Fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.

8. Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español.

Estas medidas podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal."[44]

[44] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín oficial del Estado*, 24 de noviembre 1995. Recurso disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 [Consulta: 1 de Julio de 2022]

Como vemos, todas las actividades de índole sexual donde forme parte un menor de edad o una persona con discapacidad necesitada de especial protección están castigadas por la ley y son duramente perseguidas por los cuerpos de Seguridad del Estado en los distintos países del mundo. Un niño o niña menor de edad requiere de una protección especial por parte del resto de la sociedad ya que estos no son plenamente capaces de tomar decisiones personales ya que o no entienden muchos conceptos o no son capaces de diferenciar, en muchos casos, lo que está bien de lo que está mal; siendo necesario que sea la sociedad quien los proteja hasta que alcancen dicha madurez intelectual que les dé la posibilidad de elegir sus propias decisiones y consentimientos.

Hay que tener en cuenta que la mayoría de edad no se alcanza en todos los países a la misma franja de edad, sino que varía según el Estado y su Ordenamiento Jurídico, en España por ejemplo la mayoría de edad se alcanza con los dieciocho años, pero en países como Estados Unidos, esta mayoría no se adquiere hasta los veintiuno.

El Ordenamiento Jurídico no solo considera que cometen delito de pornografía infantil a aquellas personas que realicen el acto ilícito en concreto, sino también a todas aquellas personas que alberguen y distribuyan dichos contenidos.

Teniendo en cuenta todo lo anterior, bien es cierto que en el internet convencional, el que usamos en nuestro día a día (bien en nuestros ordenadores o bien en nuestros smartphones) es prácticamente imposible encontrar este tipo de contenidos, puesto que la red está vigilada en su totalidad por los cuerpos de seguridad del Estado en ayuda de todos los suministradores de internet del país y en el momento en el que se encuentran este tipo de contenidos son prácticamente eliminados al segundo y la persona que lo difunde detenida y pasada a control judicial casi al instante.

Sin embargo, existe un entorno donde este tipo de contenido aún se puede encontrar de manera más o menos fácil si una persona se pone a investigar a conciencia; un entorno donde la seguridad escasea y el control es mucho mas complicado, estamos hablando de la Deep Web.

En los epígrafes siguientes vamos a explicar que es esto de la Deep Web y qué clase de fenómenos y contenidos podemos encontrarnos en la misma y cómo este entorno es idóneo para muchas personas a la hora de poder distribuir y almacenar muchos contenidos ilegales que en la "Surface web" serían eliminados y castigados en milésimas de segundos.

6. LA DEEP WEB, CONCEPTOS GENERALES

¿Qué es la Deep Web, y la Dark Web? ¿Son sinónimos? ¿Hay que tenerles miedo? Las respuestas a estas preguntas las iremos resolviendo poco a poco a medida que profundicemos en los siguientes epígrafes de este trabajo.

En todo momento, cuando hablamos de internet, el mundo lo define como una "red de redes", un sistema descentralizado donde miles de ordenadores de todo el mundo comparten información entre sí para poder brindar un entorno estable y didáctico para todo aquel que quiera navegar o buscar información. Pero internet va mucho más allá de eso, existen entornos más allá de lo que convencionalmente podemos encontrar en un navegador web, sitios cuyo acceso es más complicado de lo habitual, en algunos casos, encriptados o con más de una capa de seguridad para proteger información o servicios que se realizan en ellos, legales o incluso en algunos casos ilegales. Todos estos lugares, no accesibles con un simple click y un buscador, se

engloban en varios entornos virtuales dependiendo de la finalidad de los contenidos de estos sitios web, a saber: la Deep Web y la Dark Web.

La forma más habitual de utilizar internet hoy es abrir el navegador (Internet Explorer, Opera, Google Chrome, etc.) y teclear en la barra del buscador de Google aquello que queremos encontrar. En cuestión de segundos, obtenemos cientos de miles de resultados y solo hay que entrar en el enlace que deseemos.

Google es una empresa, creada en 1997 por dos estadounidenses, Larry Page y Sergey Brin, cuyo primer y más famoso producto fue un motor de búsqueda de Internet, el mismo que seguimos utilizando hoy en día y el más utilizado por todo el mundo en la actualidad[45], desbancando a todos sus competidores en todo momento. Sin embargo, Google no es internet, esta apenas rasca la superficie de lo que hay dentro de la red, hay mucho más allá de lo que Google nos puede proporcionar si sabemos cómo buscar y acceder.

Para conocer el funcionamiento de la Deep Web y la Dark Web y por qué no está al alcance de los navegadores convencionales debemos conocer cómo funciona Google y su método de "encontrar páginas".

Google utiliza, en primer lugar, una herramienta llamada "crawler", popularmente conocida como "reptador" o "araña", un Bot virtual que se dedica a recorrer la red sin descanso, captando términos relevantes, para lo que utiliza una serie de patrones informáticos conocidos como "algoritmo Google"[46]. Todos estos datos son enviados a unos ordenadores que los recopilan y los ordenan como si de un índice

[45] CASAS HERRER, EDUARDO. *La red oscura.* Edit. La esfera de los libros, 2017, pág. 17.
[46] CASAS HERRER, EDUARDO. *La red oscura.* Edit. La esfera de los libros, 2017, pág. 17.

bibliográfico se tratase, que posteriormente son clasificados según importancia para así, cuando el usuario final teclee en el buscador un término, este muestre los resultados más cercanos a lo que el usuario ha escrito en primer lugar.

Precisamente esta manera de trabajar del buscador de Google también es su "punto débil" a la hora de gestionar las búsquedas de información de su herramienta "crawler". Por mucho que recopile su Bot virtual, la capacidad de encontrar información es limitada y siempre habrá sitios o páginas que jamás podrá encontrar y recopilar, ya que internet va mucho más allá de la capacidad finita que puede llegar a tener un Bot o I.A. De esta manera Google tiene la entrada vetada a diversas páginas o entornos de red como pueden ser las redes privadas de empresas y complejos y aquellos sitios donde Google y otros buscadores no pueden alcanzar al utilizar encriptaciones y métodos de accesos ajenos a donde puede llegar "crawler". Para acceder a estos sitios es necesario conocer el enlace concreto y entrar mediante navegadores especiales capaces de descompilar enlaces web concretos.

Para aclarar la diferencia entre la Surface Web, de una parte, y la Deep Web y Dark Web, de otra, por regla general se utiliza un símil de internet con un iceberg, donde el 20% del mismo es lo que podemos ver en el día a día y acceder mediante buscadores web, y el 80% restante que está bajo el agua y lo que no vemos o no podemos acceder de manera convencional, siendo este 80% de lo que en realidad está compuesto internet. Si bien es cierto que la imagen es muy genérica, puesto que no nos proporciona una diferenciación entre Deep Web y Dark Web, las cuales explicaremos un poco más adelante, sí que es una pieza clave para entender de manera básica el funcionamiento de internet

(Figura 9: comparación análoga de internet con un iceberg)[47]

Tras este símil podemos hacer una diferenciación más concreta entre Deep Web y Dark Web. Ambas cosas están centradas en la misma premisa, aquello que no podemos acceder mediante un buscador convencional como Google, etc. Pero con connotaciones completamente distintas en ambos casos.

7. DEEP WEB, DARK WEB Y SU RELACIÓN CON EL MUNDO DELICTIVO

Habiendo explicado de una manera general cómo funcionan los buscadores web como Google y por qué podemos dividir internet en distintas capas como si fuese un iceberg, es momento de explicar qué es la Deep Web y la Dark Web y qué podemos encontrar en cada una de ellas.

La Deep Web es todo aquel entorno donde un navegador convencional no puede acceder mediante un motor de búsqueda estándar, es decir, un entorno en la red donde no siempre puedes acceder simplemente buscando en Google o Yahoo! Estos

[47] Fuente de la imagen: LOPEZ José María "Deep Web, Dark Web y DarkNet: los rincones más ocultos de internet". *Hipertextual*, 15 de abril de 2022. Recurso disponible en: https://hipertextual.com/2022/04/deep-web-dark-web-darknet [Consulta: 20 de abril de 2022]

entornos son accesibles desde cualquier navegador, ya sea Chrome, Firefox, Internet Explorer, etc. Y obviamente, no todos los contenidos que existen en la Deep Web son ilegales, de hecho, cualquier persona está navegando continuamente en la Deep Web en su día a día, cuando consultas tu correo desde el navegador, miras tu cuenta bancaria, accedes a grupos privados de Facebook o perfiles restringidos de Instagram, cuando entras a un foro de internet… Todo este contenido forma parte de la Deep Web y es perfectamente legal[48].

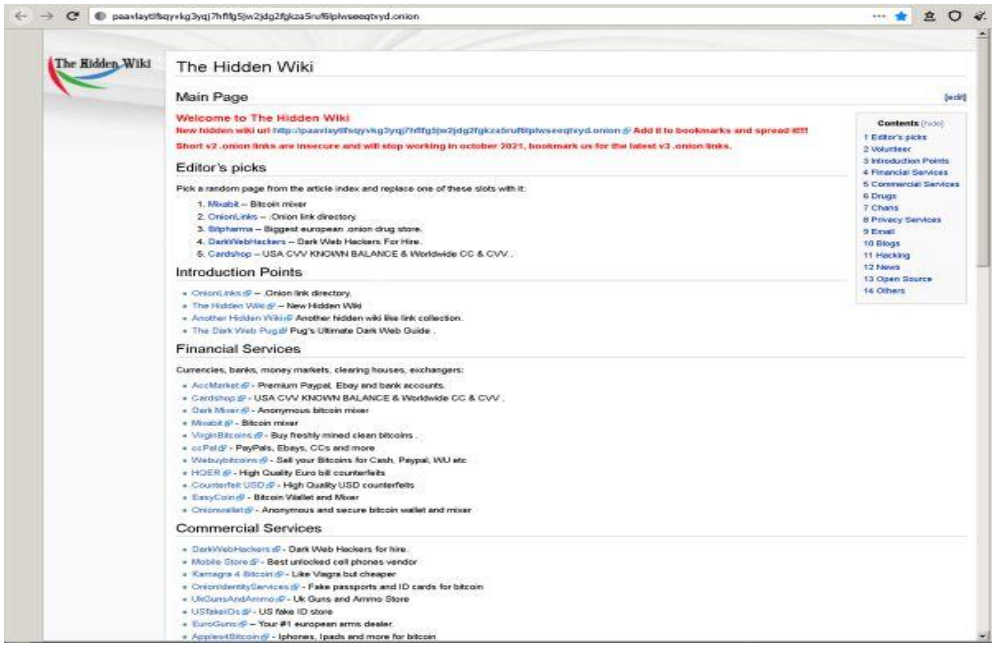
El contenido alojado en este tipo de "Internet profunda" suelen ser foros privados, intranet de empresas, webs privadas y todo aquel contenido que suele estar fuera del alcance de la gente cotidiana, aunque muchos de estos contenidos son accesibles siempre y cuando sepas la dirección completa o URL y, en algunos casos, la contraseña de acceso a dichos sitios.

La gran diferencia viene cuando intentas profundizar mucho más en ese "iceberg" metafórico e intentas entrar a contenidos algo más turbios e ilegales, es decir, te adentras en los contenidos de la Dark Web. Este entorno no es accesible mediante un navegador estándar: para acceder a contenidos de la Dark Web se han creado navegadores específicos capaces de navegar por aquellas URLs específicas, las cuales solo se pueden ejecutar mediante estos navegadores y con unas encriptaciones específicas para garantizar el anonimato; estas URLs tienen una extensión web concreta, la extensión .onion. Algunos de los navegadores más comunes para acceder a este tipo de contenido son por ejemplo TOR, Freenet, I2P o Zeronet.

[48] LOPEZ José María "Deep Web, Dark Web y DarkNet: los rincones más ocultos de internet" Hipertextual, 15 de abril de 2022. Recurso disponible en: https://hipertextual.com/2022/04/deep-web-dark-web-darknet [Consulta: 10 de mayo de 2022]

Lo primero que debemos hacer para acceder a la DarkNet es descargar alguno de los navegadores mencionados anteriormente, entre los cuales el más común para este tipo de accesos es TOR (The Onion Router); este navegador se caracteriza por enmascarar las direcciones I.P y los enlaces de acceso del usuario y la página web en diversas capas de información para que su rastreo y su identificación sea más compleja de lo normal, como si de las capas de una cebolla se tratase, de ahí el nombre del navegador. Además, también cuenta con un buscador web, al propio estilo de Google, llamado DuckDuckGo, capacitado para buscar, aparte de cualquier contenido de la Surface Web, enlaces .onion propios de la DarkNet.

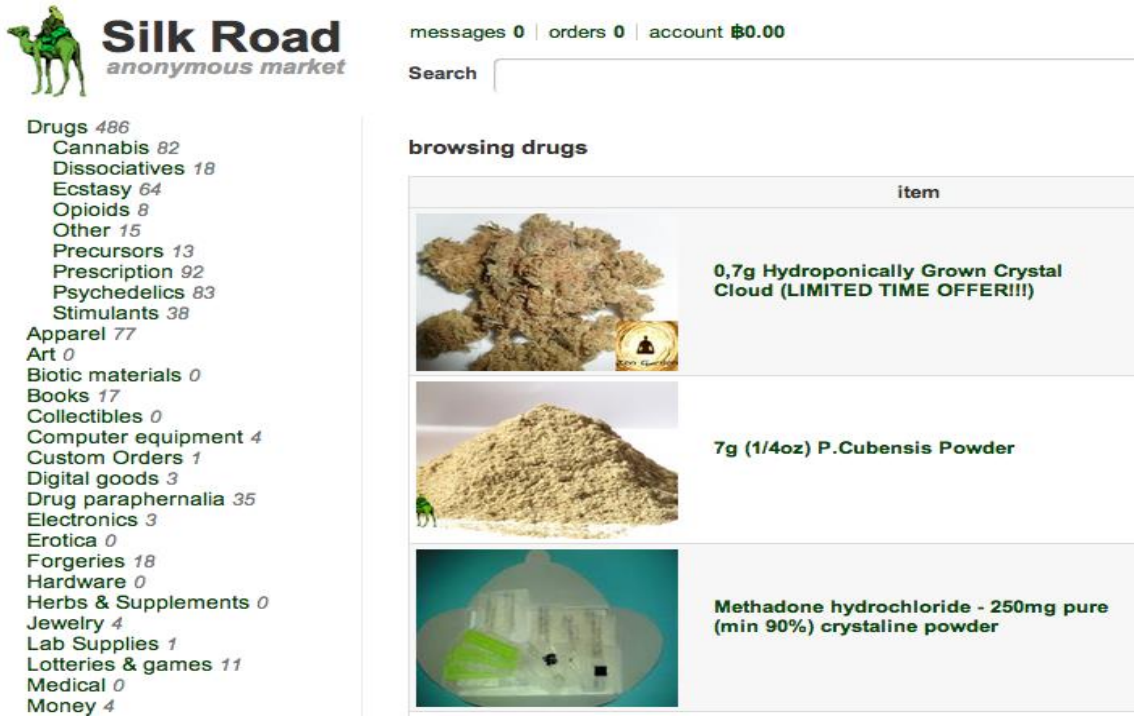
Una buena forma de comenzar a navegar por la Dark Web es buscar la biblioteca de enlaces por antonomasia de la Dark Web "The Hidden Wiki". Aquí se pueden encontrar una gran cantidad de páginas .onion y su descripción en inglés ordenadas por temáticas, algunas de contenido lícito y otras no tanto; sí que es cierto que muchas de estas webs con contenido ilegal han ido desapareciendo poco a poco debido a que todos estos enlaces están muy controlados por los cuerpos de seguridad de los diferentes Estados del mundo.



(Figura 10: The Hidden Wiki)[49]

Dentro de los contenidos de esta Hidden Wiki podemos encontrar servicios financieros, comerciales, foros de opinión, investigación… pero también podemos encontrar enlaces a webs de venta de drogas y armas. Una de las páginas de este tráfico ilegal de sustancias y armamento fue Silkroad, actualmente cerrada por el FBI pero que ha sido sucedido por miles y miles de páginas en la Dark Web con la misma temática y capacidad de venta de sustancias estupefacientes, armas y otros bienes de carácter ilegal; todo este contenido lo explicaremos con mucho más detalle en el apartado siguiente.

[49] Fuente de la imagen: The Hidden Wiki. Recurso disponible en: https://thehiddenwiki.org/ [Consulta: 10 de mayo de 2022]



(Figura 11: Pagina web Silkroad antes de su cierre definitivo)[50]

Aparte de venta de drogas y tráfico de armas, también podemos encontrar otra serie de contenidos ilegales dentro de la Dark Web, contenidos tales como pornografía infantil, pedofilia, zoofilia y otros muchos contenidos ilegales de índole sexual; también podemos encontrar contenidos de venta de productos robados, etc.

Una de las transacciones que podemos encontrar dentro de la Dark Web y que está cogiendo popularidad en los últimos tiempos es la contratación de servicios tales como el espionaje, el hackeo de grandes multinacionales o incluso la falsificación de identidades y pasaportes. Dentro de la Dark Web, el mayor tráfico de material y la mayor ganancia de dinero que existe es la venta de información personal de cualquier persona, los datos personales que se pueden extraer mediante estafas y robos de identidades en la Surface Web son motivo de compra venta y tráfico de información dentro de la Dark

[50] Fuente de la imagen: PENALVA, Javier "Ser creador de una web de tráfico de drogas ya tiene pena: cadena perpetua". *Xataka*, 30 mayo de 2015. Recurso disponible en: https://www.xataka.com/servicios/ser-creador-de-una-web-de-trafico-de-drogas-ya-tiene-pena-cadena-perpetua [Consulta: 10 de mayo de 2022]

Web, mucha gente paga cantidades ingentes de dinero por información clasificada o por datos personales de algún individuo concreto.

Cabe destacar que los accesos a las URLs de la Dark Web, por regla general, se realizan de manera anónima y siempre enmascarando la identidad del usuario por medio de VPNs o similares que ocultan las direcciones y las informaciones personales de los usuarios y de los aparatos electrónicos que utilizan para acceder a estos lugares, pero esto no siempre es cien por cien fiable; a medida que más profundizas en la Dark Web e intentas acceder a entornos más comprometidos o "peligrosos" más difícil es enmascarar tu información personal, puesto que está bajo el control de muchísima gente cuya capacidad de obtener información (Hackers) va más allá de la que el propio navegador puede ocultar, aparte del control policial que tienen este tipo de lugares, los cuales cuentan con tecnología suficiente para poder desenmascarar una dirección IP en el menor tiempo posible aunque esta esté oculta bajo una VPN remota difícil de localizar.

Hay que señalar que no todo lo que se encuentra en la Dark Web es de contenido ilegal: si el usuario sabe buscar correctamente, se puede encontrar muchísimo contenido que no está dentro de los contenidos ilegales propios de la Dark Web, contenidos tales como foros de opinión, recursos electrónicos como pueden ser investigaciones médicas, arqueológicas, etc. Y muchísimo contenido intelectual donde el que sepa buscar puede nutrirse de información muy valiosa y que no se puede encontrar fácilmente en la Surface Web.

También existen otros contenidos para los usuarios más fanáticos de lo paranormal y el ocultismo, donde se pueden encontrar distintos archivos multimedia,

ya sean vídeos, audios, fotos o simplemente textos donde se intenta dar por verídica la existencia de entidades extraterrestres o paranormales; en este tipo de foros, es común encontrarse supuestos archivos desclasificados del área 51 de EE.UU donde se corrobora la existencia de vida alienígena más allá de la atmosfera terrestre y muchos otros contenidos audiovisuales de carácter paranormal.

Como podemos ver, el contenido que podemos encontrar en la Dark Web es del todo variado, no todo es malo, pero tampoco todo es bueno, cada usuario es libre de navegar por un contenido que no está prohibido o castigado, ya que navegar por la Dark Web no es ilegal. Pero sí que tiene que ser consciente de que busca o qué quiere encontrar, ya que el hilo que separa el contenido legal del ilegal es tan fino, que en cualquier momento el usuario puede ser cómplice o autor de algún acto ilegal o víctima de una estafa o robo de información dentro de esta “Web profunda”.

8. SILKROAD Y EL TRÁFICO DE DROGAS POR LA DARK WEB

Cuando hablamos de Dark Web, lo primero que pensamos siempre es en peligrosidad y actuaciones al margen de la ley y en parte es cierto, o lo era hasta el cierre de una de las plataformas ilegales más grandes de toda la "Web profunda", estoy hablando de Silk Road.

Ya hemos hablado un poco en el epígrafe anterior de qué era Silk Road y de su principal funcionabilidad dentro de la Dark Web, el tráfico de drogas. En este epígrafe vamos a conocer mucho más el entorno web de Silk Road, así como la vida y detención de su autor Ross Ulbricht, ya que ambas cosas son importantes para conocer el funcionamiento de la Dark Web hasta el cierre de la plataforma y el fin del mayor tráfico de drogas y armas de EE.UU. mediante esta plataforma.

Ross Ulbricht nació en Austin, Texas, el 27 de marzo de 1987 y en su vida de estudiante asistió a la Westlake High School, conocida por ser una de las mejores 200 preparatorias más grandes de Estados Unidos. Tras graduarse, Ross empezó su carrera universitaria en la universidad de Texas, donde se graduó en 2006 tras completar sus estudios de Física. Tras esto Ulbricht comenzó a asistir a la universidad de Pensilvania, donde obtuvo un Máster en ciencias materiales e ingeniería, donde también estudio cristalografía[51].

Durante un tiempo tras su graduación en la universidad de Pensilvania, Ulbricht intentó empezar su propio negocio, pero en todos ellos siempre acaba fracasando. Su último intento fue un portal online de venta de libros conocido como "Good Wagon

[51] EQUIPO BIT2MEACADEMY "¿Quién es Ross Ulbricht?". *Bit2meacademy*. Recurso disponible en: https://academy.bit2me.com/quien-es-ross-ulbricht/ [Consulta: 25 de mayo de 2022]

Books”[52], proyectó que también fracasó, desplomando la moral de Ulbricht. Sobre esta época, Ulbricht estaba bastante endeudado y no tenía muchas expectativas sobre su futuro; después de un tiempo de pensar en cómo mejorar su situación actual decidió empezar a desarrollar lo que se conocería como el primer gran dark market del mundo, Silk Road.

La idea principal de Ulbricht con Silk Road era simple, un mercado digital donde podías comprar lo que quisieras, de manera totalmente anónima y cuyo pago se realizaría con una moneda difícil de rastrear, Bitcoin. Teniendo en cuenta esta idea Ulbricht comenzó el desarrollo de Silk Road hasta su lanzamiento en febrero de 2011[53].

Aunque la idea original de Ulbricht era conseguir crear el “Amazon” de la DarkNet donde poder comprar de manera anónima y sin que nadie pudiese registrar tu información en el intento, la realidad es que Silk Road empezó a llenarse de ofertas “fuera de la ley”, llenándose la página de ofertas de drogas, armas, carnets falsos, etc., tanto de EE.UU. como del resto del mundo, con una simple premisa, el anonimato. Por esta misma razón era tan difícil rastrear por parte de los cuerpos de inteligencia de los Estados más importantes del mundo. Detrás de todo esto había un seudónimo común: “Dread Pirate Roberts”, alías que Ross Ulbricht usaba como dueño de la página[54].

Por los motivos previamente mencionados (anonimato y pagos con Bitcoins), Silk Road era un sitio prácticamente inexpugnable, donde rastrear la identidad de su autor no fue tarea fácil para el FBI: hicieron falta dos divisiones distintas para conseguir

[52] Ídem.
[53] EQUIPO BIT2MEACADEMY “¿Quién es Ross Ulbricht?”. *Bit2meacademy*. Recurso disponible en: https://academy.bit2me.com/quien-es-ross-ulbricht/ [Consulta: 25 de mayo de 2022]
[54] PEREZ Hanna, “Ross Ulbricht”. *Diariobitcoin*, 29 agosto 2020. Editado el 20 de febrero 2021. Recurso disponible en: https://www.diariobitcoin.com/personajes/ross-ulbricht/ [Consulta: 25 de mayo de 2022]

avanzar en la investigación de Silk Road, el FBI y la DEA. El agente de la DEA Carl Force y el especialista de la división de cibercrimen Chris Tarbell del FBI fueron los encargados de encabezar la investigación[55].

Para conseguir avanzar en la investigación contra Silk Road y Ulbricht, ambos agentes tuvieron que encaminar la misma de maneras completamente distintas: Force se infiltró en Silk Road haciéndose pasar por un narcotraficante de la Republica Dominicana para entablar comunicación con Dread Pirate Roberts y ganarse su confianza, mientras que Tarbell intentaba localizar el servidor donde se alojaba la página web y la localización donde se conectaba el administrador de la misma[56].

Según algunas fuentes, Ulbricht finalmente cometió dos errores fundamentales que le costaron el fin de Silk Road y su detención por parte del FBI: el primero fue caer en el engaño de Force y auto incriminarse al pedirle que realizará un asesinato por encargo, aunque finalmente esto no pudo ser demostrado en su totalidad. El segundo fue tener mucho ego y confianza en que nadie podría acabar pillándole nunca[57].

En estos momentos Ulbricht ya estaba fuertemente vigilado por parte del FBI y ya tenían muchas pruebas de peso para poder encausarle y poner fin a Silk Road, solo necesitaban que Ulbricht se loguease en la página web para tener una prueba firme de que formaba parte de la misma, es así como Ulbricht fue detenido en la biblioteca

[55] ESTEVES Ricky, "La Historia de Silk Road". *Regiamag*, 2 de mayo de 2017. Recurso disponible en: https://regiamag.com/ross-ulbricht-cadena-perpetua/ [Consulta: 25 de mayo de 2022]
[56] EQUIPO VOZ POPULI "El caso 'Silk Road': la misión policial que acabó con el Temible Pirata Roberts". *Voz Populi*, 9 de mayo de 2015. Recurso disponible en: https://www.vozpopuli.com/internacional/silk_road-ross_ulbricht-temible_pirata_roberts-ruta_de_la_seda-caso-caso_silk_road-detencion-fbi-chris_tarbell-dea-carl_force_0_832716729.html [Consulta: 25 de mayo de 2022]
[57] ESTEVES Ricky, "La Historia de Silk Road". *Regiamag*, 2 de mayo de 2017. Recurso disponible en: https://regiamag.com/ross-ulbricht-cadena-perpetua/ [Consulta: 25 de mayo de 2022]

pública de Glen Park, en San Francisco, mientras estaba conectado a Silk Road creyendo que estaba charlando con una de las administradoras de la página, cuando en realidad estaba hablando con un agente de investigaciones encubierto que había tomado control de la cuenta de la administradora[58].

Ulbricht fue condenado en 2015 cadena perpetua y finalmente se dio fin al mayor mercado de drogas "legal" existido en el mundo localizado en la Deep Web, el mercado conocido como "El camino de la seda" o Silk Road.

9. LAS CRIPTOMONDEDAS, EN ESPECIAL BITCOIN.

La principal ventaja que tiene la Deep Web en comparación con la Surface web es el anonimato que proporciona tanto navegando por ella como realizando cualquier transacción. En el caso de la navegación, el anonimato se lo da el propio navegador donde accedes a todo el entorno de la Deep Web: el navegador TOR. Por parte de las transacciones seguras y anónimas que se producen en la Deep Web entra en escena toda una nueva tecnología que ha ido cogiendo muchísima fuerza poco a poco, es el caso de las criptomonedas, en este caso concreto, el BitCoin.

¿Qué es BitCoin y que son las criptomonedas? Esta pregunta a día de hoy es algo bastante difícil de explicar si no tienes algún conocimiento básico de finanzas e informática, pero vamos a intentar explicar de manera sencilla qué son las criptomonedas y por qué el BitCoin es tan importante a día de hoy.

[58] PEREZ Hanna, "Ross Ulbricht". *Diariobitcoin*, 29 agosto 2020. Editado el 20 de febrero 2021. Recurso disponible en: https://www.diariobitcoin.com/personajes/ross-ulbricht/ [Consulta: 25 de mayo de 2022]

Las criptomonedas son herramientas que, basándose en los principios de la criptografía, permiten que un grupo de personas unidas por la red y que no se conocen entre sí generen "dinero" y lo hagan circular, sin que haya una autoridad central que pueda validar las transacciones que se realicen.[59] Con estas acciones se garantiza la titularidad de esta "moneda virtual" y se puede controlar la creación de nuevas monedas por parte de los usuarios, evitando también que se puedan hacer copias de las monedas ya existentes como podríamos hacer con, por ejemplo, un dibujo o una foto. Estas monedas no existen de forma física, se almacenan todas en un entorno virtual, comúnmente conocido como "cartera digital"[60].

Estas criptomonedas funcionan de manera muy distinta respecto a los sistemas convencionales, no están reguladas ni controladas por ninguna institución bancaria y no requieren de estos como intermediarios para validar las transacciones que realiza la gente.

Para comprender mejor cómo funciona este sistema de transacciones, se puede hacer una comparativa de cómo se realizan actualmente las transacciones en moneda digital, es decir, sin pagar con dinero físico y en efectivo: cuando pagamos por un artículo con nuestra tarjeta de débito, lo que estamos haciendo es enviar un aviso a nuestro banco, dándoles la orden de transferir la cantidad de dinero concreta que vale dicho artículo, desde nuestra cuenta bancaria a la cuenta de la tienda en cuestión. En nuestro registro bancario figurará que se ha retirado "X" cantidad de dinero, mientras que en el

[59] VAGO Claudia, VILLANO Domenico "Historia del Bitcoin: cómo nació y en qué se ha convertido.". *Valor Social*, 21febrero 2021. Recurso disponible en: https://valorsocial.info/historia-del-bitcoin-como-nacio-y-en-que-se-ha-convertido/ [Consulta: 01 de junio de 2022]

[60] EQUIPO SANTANDER "Guía para saber qué son las criptomonedas." *Santander*, 24 de mayo 2022. Recurso disponible en: https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas [Consulta: 01 de junio de 2022]

de la tienda que se ha ingresado “X” cantidad. En estas transacciones, es la entidad financiera quien actúa como intermediario y verifica la transacción realizada entre el comprador y el vendedor.

Las criptos se inventaron para realizar esta misma función pero sin necesidad de que una entidad financiera haga de intermediaria y garantice la veracidad de dicha transacción, esto garantiza un anonimato cien por cien real a la hora de realizar transacciones con criptomonedas, ya que el usuario que paga y el que recibe la cripto no tienen que verificar dicha transacción por medio de entidades físicas bancarias, sino que son los usuarios de la red dedicados a verificar dicha transacción que no tienen “nombre y apellidos” los que dan por correcto el pago.

Bitcoin fue la primera criptomoneda existente en el mercado, creada en 2008 por el inventor Satoshi Nakamoto presentando el protocolo base de la criptomoneda a expertos en criptografía mediante la Cryptography Mailing List[61]. En 2009 el BitCoin estaba ya listo para salir a la red y convertirse en una de las criptos más importantes actualmente.

El valor de las criptomonedas va fluctuando según la oferta y la demanda de los usuarios que invierten en ellas, es como invertir en bolsa, pero en vez de con acciones de compañías existentes, con “monedas virtuales”. El valor actual del Bitcoin a día de hoy está en torno a los 27.920,83 euros, este valor puede ir variando a cada minuto[62].

[61] S. Jesús “¿Quién es Satoshi Nakamoto y por qué puede ser una amenaza al bitcoin?” *Economia3*, 11 de marzo 2022. Recurso disponible en: https://economia3.com/satoshi-nakamoto-bitcoin/ [Consulta: 01 de junio de 2022]

[62] GOOGLE. Recurso disponible en: https://cutt.ly/7JCCwu8 [Consulta: 01 de junio de 2022]

Por todas estas razones de descentralización de la moneda, el anonimato y la seguridad que proporciona el BitCoin en la época de Silk Road o cualquier criptomoneda actual, las transacciones que se realizan en la Deep Web se hacen mediante pago por criptomoneda haciendo que sea seguro tanto para el comprador como para el vendedor, así como difícil de rastrear en el caso de que se realicen transacciones "ilegales" como las que se realizaban en Silk Road para el tráfico de drogas y armas como en la venta de papeles ilegales o contratación de hackers, etc. En la Deep Web.

CONCLUSIONES

1. Internet y la tecnología han evolucionado de manera drástica en los últimos años, pasando de comunicarnos mediante telégrafos o teléfonos cuya centralita de gestión de llamadas estaban operadas por personas físicas en una central de una gran empresa a poder teclear cualquier cosa en un teclado con palabras y encontrar cualquier información prácticamente al instante o llamar a cualquier persona con un sistema de comunicación que tenemos en el bolsillo en cualquier momento.
2. La delincuencia, al igual que la tecnología, se ha visto actualizada y evolucionada de manera drástica en muy poco tiempo, pasando de ser algo típico de la calle a moverse en un entorno virtual donde el límite de la delincuencia se encuentra en si el usuario final tiene acceso a internet o no.
3. La escala a la que un ciberdelincuente puede llevar sus delitos se extiende en la misma proporción en la que lo hace internet, siendo prácticamente infinitas las posibilidades de un delincuente de estafar o robar a una víctima en cualquier parte del mundo.
4. El Ordenamiento Jurídico español, así como los Ordenamientos Jurídicos de prácticamente todos los estados del mundo se han ido actualizando y modernizando para adaptarse a los cambios tan repentinos que ha proporcionado internet, siendo necesario nuevas formas de protección frente a nuevas formas de cometer delitos. Algunos como el Ordenamiento Jurídico español, han extrapolado y adaptado sus artículos ya existentes para dar cabida

a estas nuevas formas de delinquir, otros Estados han creado leyes especiales destinadas a proteger estos vienes jurídicos.

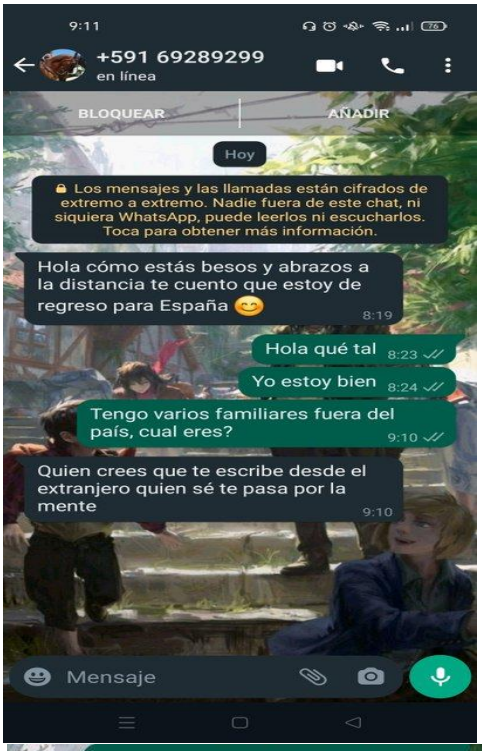
5. El phishing está a orden del día en la navegación de todos los usuarios de internet. Seguramente recibimos miles de correos catalogados como spam o phishing a lo largo del día, así como miles de intentos de estafa y robos de información cada vez que intentamos navegar por internet.
6. Al igual que el phishing, las estafas de todo tipo, así como otros delitos como el carding también son comunes en internet y son el mayor motivo de robo de información que hay en la red actualmente
7. La pornografía infantil es un delito castigado muy duramente por todos los Ordenamientos Jurídicos de todos los Estados, la idea siempre es proteger a los menores de cualquier "mal" debido a que estos aún no poseen la suficiente capacidad jurídica y de obrar como para protegerse a si mismos de estas situaciones.
8. Las entidades bancarias y las distintas páginas web donde requiere un log in por parte del usuario están implementando miles de métodos de autentificación para evitar así el robo de información por parte de los delincuentes.
9. Navegar por la Deep Web no es ilegal, pero sí que hay que tener mucha precaución de los entornos en donde accedemos ya que puedes ser víctima de robos de información o acceder a sitios que los cuerpos de inteligencia de muchos Estados controlan constantemente.
10. La Deep Web tiene mucha historia de delincuencia, pero no todo lo que podemos encontrar en ella es "ilegal", podemos encontrar muchas páginas de interés e

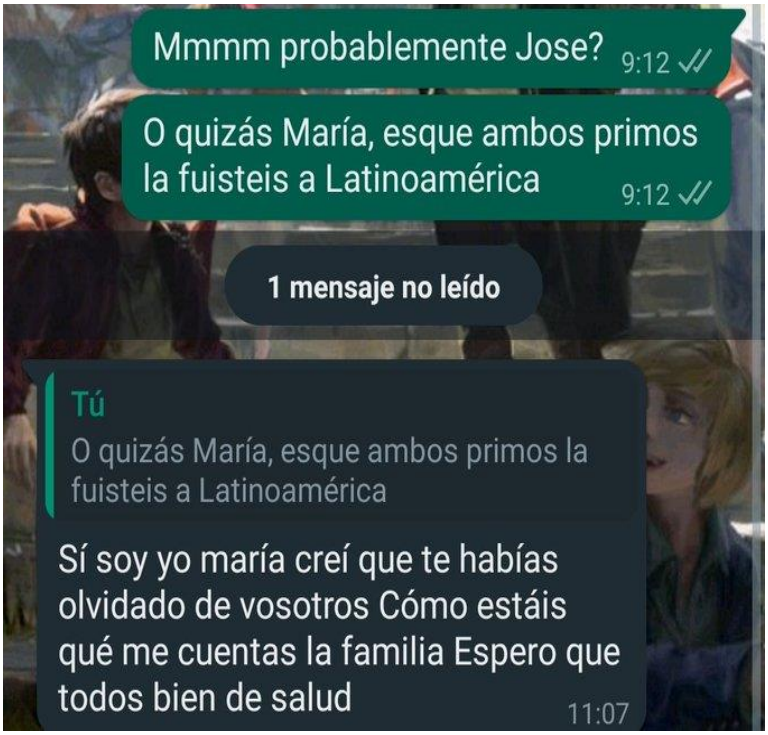
investigación capaces de satisfacer la curiosidad y el interés de todo tipo de personas.

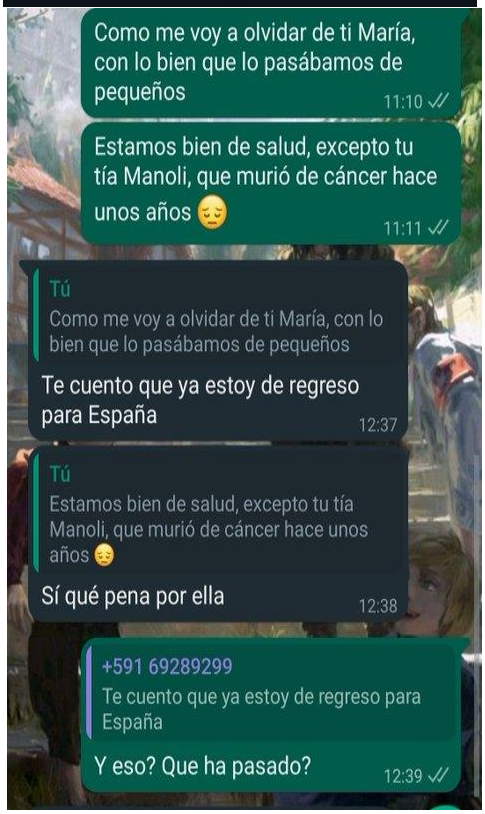
11. Las criptomonedas es algo novedoso pero que ha ido cogiendo fuerza con el paso de los años, convirtiéndose en la actualidad en uno de los métodos de pago e inversión más comunes en la actualidad.
12. La volatilidad de una criptomoneda depende de la oferta y la demanda de la misma en el mundo "cripto". Es así que hay que tomar muchas precauciones a la hora de invertir en criptomonedas, un día pueden valer una fortuna y al día siguiente no valer absolutamente nada.
13. Los Ordenamientos Jurídicos se van adaptando a la vez que va evolucionando la sociedad, es así como el Código Penal español ha ido sufriendo ligeras modificaciones a lo largo de los años para poder adaptar todo lo que son los delitos informáticos y la ciberdelincuencia y así poder proteger todos los bienes jurídicos de los ciudadanos, ya sea de manera "física" como de forma "virtual".

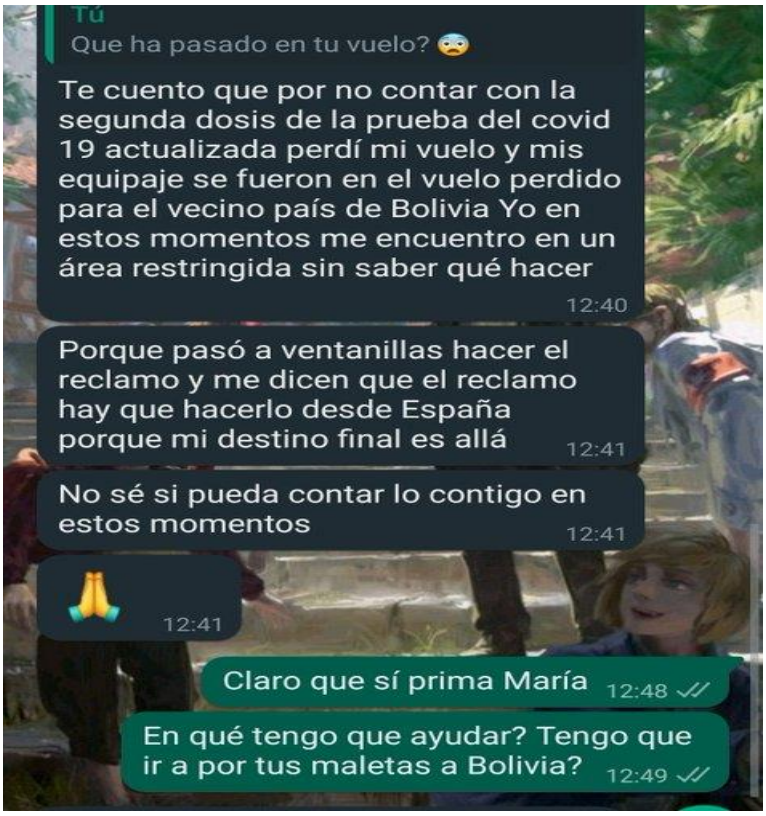
ANEXOS:

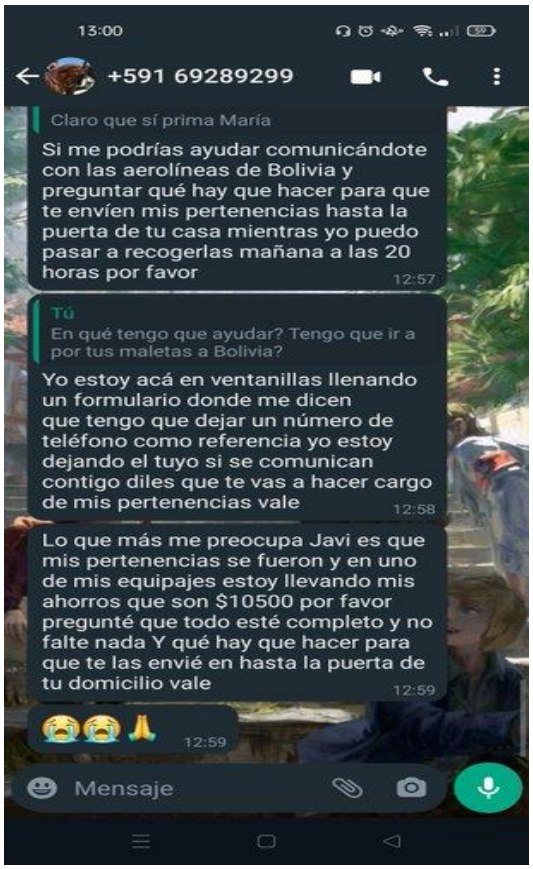
Anexo I:



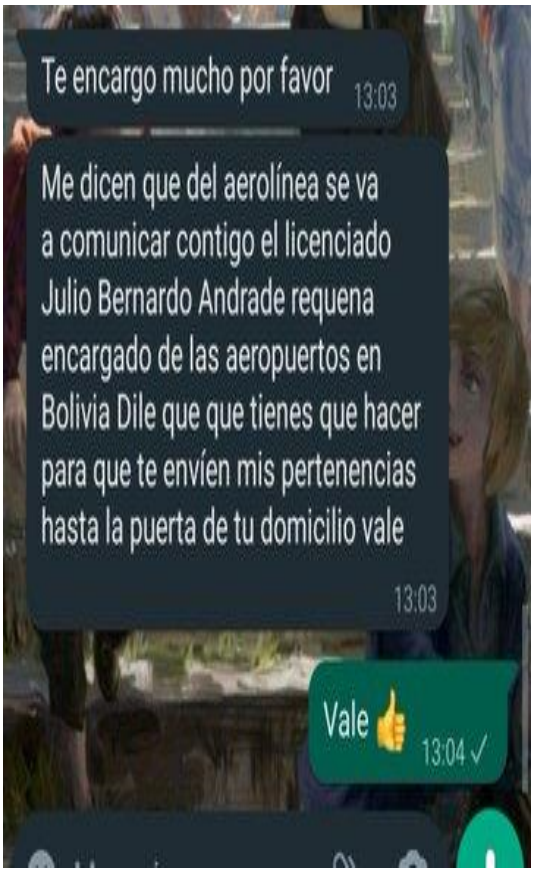


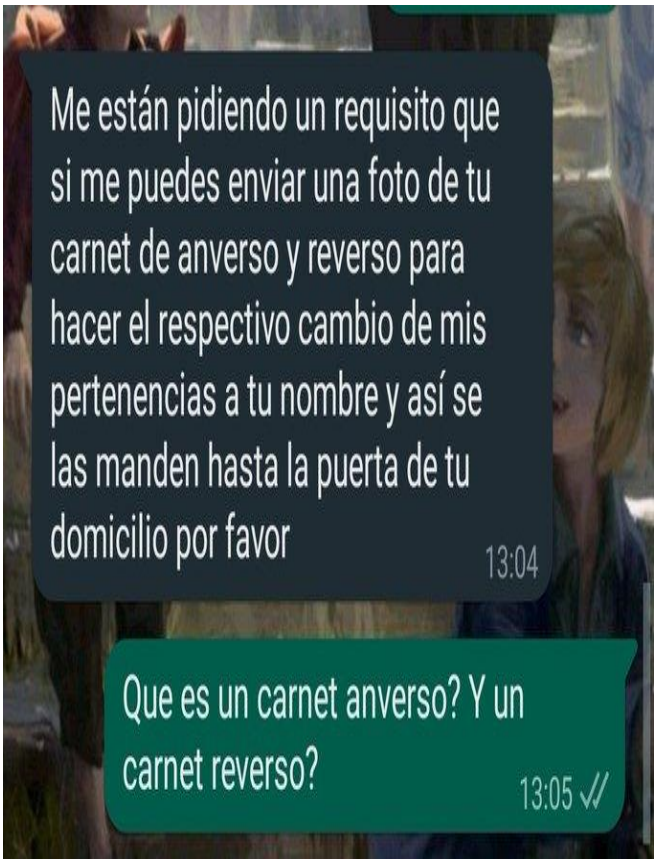





13:00
+591 69289299
Claro que sí prima María
Si me podrías ayudar comunicándote con las aerolíneas de Bolivia y preguntar qué hay que hacer para que te envíen mis pertenencias hasta la puerta de tu casa mientras yo puedo pasar a recogerlas mañana a las 20 horas por favor
12:57
Tú
En qué tengo que ayudar? Tengo que ir a por tus maletas a Bolivia?
Yo estoy acá en ventanillas llenando un formulario donde me dicen que tengo que dejar un número de teléfono como referencia yo estoy dejando el tuyo si se comunican contigo diles que te vas a hacer cargo de mis pertenencias vale
12:58
Lo que más me preocupa Javi es que mis pertenencias se fueron y en uno de mis equipajes estoy llevando mis ahorros que son $10500 por favor pregunté que todo esté completo y no falte nada Y qué hay que hacer para que te las envié en hasta la puerta de tu domicilio vale
12:59
12:59
Mensaje


13:03
+591 69289299
escribiendo...
tu domicilio vale
12:59
12:59
Vale
13:01
Si te preguntan el número de vuelo es el 503
13:02
Y el código de mis equipaje son
13:02
Vale
13:02
PASE DE ABOR
KRL-246
KRL-245
KRL-247
LATA
LATAM
13:03
Vale
13:03
Mensaje


Te encargo mucho por favor
13:03
Me dicen que del aerolínea se va a comunicar contigo el licenciado Julio Bernardo Andrade requena encargado de las aeropuertos en Bolivia Dile que que tienes que hacer para que te envíen mis pertenencias hasta la puerta de tu domicilio vale
13:03
Vale
13:04


Me están pidiendo un requisito que si me puedes enviar una foto de tu carnet de anverso y reverso para hacer el respectivo cambio de mis pertenencias a tu nombre y así se las manden hasta la puerta de tu domicilio por favor
13:04
Que es un carnet anverso? Y un carnet reverso?
13:05

Anexo II:

Hola
Nos disculpamos por contactarlo de esta manera. Solo miré tu perfil y pensé que eras la persona que necesitaba. En definitiva, mi nombre es Carine Lemer, de origen austriaco y vivo en Francia. Sufro una grave enfermedad que me ha condenado a una muerte segura, a saber, el cáncer de garganta, y tengo una cantidad de 387 000 euros que me gustaría dar a una persona fiable y honesta que lo utilice bien.
Soy dueña de una empresa que importa aceite rojo a Francia y perdí a mi esposo hace 6 años. Estaba muy impresionada y no pude casarme hasta que tuve hijos ese día. Me gustaría donar esta suma antes de mi muerte, para que mis días estén contados por la ausencia de esta enfermedad, para la cual no tenía cura, pero sí una garantía en Francia, por lo que no quiero saber si puede beneficiarse de esta donación. Si desea recibir una donación de € 387,000, puede contactarme a través de mi correo electrónico de donación: [redacted]

lemer carine 11:17
per a Carles

Hola
Está bien, te entiendo completamente. Para confirmar que te hemos elegido para ser el heredero de mi patrimonio, haz lo que prometes. En cambio, solo pido una oración para dormir con mi esposo, a quien he amado tanto en el pasado. Te doy este regalo desde el corazón. Favor de contactarme primero por correo electrónico con mi notario para solicitar la donación que tengo por teléfono. Está esperándote. Gracias y no olvides la promesa una vez que el dinero esté en tu cuenta. Así que por favor póngase en contacto con la oficina del maestro. Correo electrónico: [redacted]

.

Saludos cordiales, escriba a mi notario a la siguiente dirección de correo electrónico: [redacted]

y sigue sus instrucciones para que, como te dije, tengas 387.000 euros en poco tiempo. Gracias por avisarme tan [redacted]nga en contacto contigo.

Hola.

Soy dicho abogado de la Sra. Carine Lemer.

Con respecto a su donación, por favor envíeme la siguiente información para dejarme saber su identidad.

APELLIDO: .....

Primer nombre: .....

PAÍS: .....

CIUDAD: .....

NÚMERO DE TELÉFONO: .....

CÓDIGO POSTAL: .....

INFORMACIÓN BANCARIA: .....

NÚMERO DE CUENTA: .....

COSTILLA / SWIF; ..... (Para favorecer la transmisión)

PD: Necesito un extracto de su documento de identidad o de su pasaporte para ponerlo en contacto con el banco de la Sra. Carine para que pueda recibir rápidamente su donación.

BIBLIOGRAFÍA Y WEBGRAFÍA

(1) ARRIETA, Ever. *"*El hombre es un lobo para el hombre (homo homini lupus)*"* *Cultura genial*. Recurso disponible en: https://www.culturagenial.com/es/el-hombre-es-un-lobo-para-el-hombre/

(2) EQUIPO AYUDALEY. "La estafa nigeriana o timo 419" *Ayudaley*. Recurso disponible en: https://ayudaleyprotecciondatos.es/2021/01/18/estafa-nigeriana-timo-419/

(3) BAHILLO, Luis. "Historia de internet: como nació y cuál fue su evolución" *Marketing4commerce*. Recurso disponible en: https://marketing4ecommerce.net/historia-de-internet/

(4) BARRIO ANDRÉS, Moisés. *Ciberdelitos: amenazas criminales del ciberespacio.* Edit. Reus. Madrid. 2017

(5) EQUIPO BIT2MEACADEMY. "¿Quién es Ross Ulbricht?". *Bit2meacademy*. Recurso disponible en: https://academy.bit2me.com/quien-es-ross-ulbricht/

(6) CASAS HERRER, Eduardo. *"La red oscura"* Edit. La esfera de los libros, España, 2017.

(7) MIRÓ LLINARES, Fernando. "El cibercrimen" Edit. Marcial Pons, España, 2012.

(8) FORERO, Tatiana. "conoce la historia de internet desde su nacimiento hasta lo que es hoy". *Rockcontent*. Recurso disponible en: https://rockcontent.com/es/blog/historia-del-internet/

(9) GOOGLE (Análisis Bitcoin). Disponible en: https://cutt.ly/7JCCwu8

(10) PEREZ, Hanna. "Ross Ulbricht". *Diariobitcoin*, Recurso disponible en: https://www.diariobitcoin.com/personajes/ross-ulbricht/

(11) EQUIPO ITRESELLER “El comercio electrónico aumentó casi un 50% en el año de la pandemia” *Itreseller*. Recurso disponible en: https://www.itreseller.es/al-dia/2021/07/el-comercio-electronico-aumento-casi-un-50-en-el-ano-de-la-pandemia

(12) S. Jesús. “¿Quién es Satoshi Nakamoto y por qué puede ser una amenaza al bitcoin?” *Economia3*. Recurso disponible en: https://economia3.com/satoshi-nakamoto-bitcoin/

(13) LOPEZ, José María. “Deep Web, Dark Web y DarkNet: los rincones más ocultos de internet” *Hipertextual*. Recurso disponible en: https://hipertextual.com/2022/04/deep-web-dark-web-darknet

(14) ORELLANA, Rodrigo. “Qué fue de GeoCities, el desaparecido Beverly Hills de internet”. *Digitaltrends.* Recurso disponible en: https://es.digitaltrends.com/computadoras/que-fue-geocities/

(15) PASCUAL, María. “Las estafas por internet representan más del 80% de los ciberdelitos” *Newtral*. Recurso disponible en: https://www.newtral.es/estafas-internet-ciberdelitos/20210806/

(16) ESTEVES, Ricky. “La Historia de Silk Road”. *Regiamag*. Recurso disponible en: https://regiamag.com/ross-ulbricht-cadena-perpetua/

(17) EQUIPO SANTANDER. “Guía para saber qué son las criptomonedas.” *Santander*. Recurso disponible en: https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas

(18) VAGO Claudia, VILLANO Domenico. “Historia del Bitcoin: cómo nació y en qué se ha convertido”. *Valor Social*. Recurso disponible en: https://valorsocial.info/historia-del-bitcoin-como-nacio-y-en-que-se-ha-convertido/

(19) EQUIPO VOZ POPULI. “El caso ‘Silk Road’: la misión policial que acabó con el Temible Pirata Roberts”. *Voz Populi*. Recurso disponible en: https://www.vozpopuli.com/internacional/silk_road-ross_ulbricht-temible_pirata_roberts-ruta_de_la_seda-caso-caso_silk_road-detencion-fbi-chris_tarbell-dea-carl_force_0_832716729.html

BIBLIOGRAFÍA DE FIGURAS

(1) BAHILLO, Luis. "Historia de internet: como nació y cuál fue su evolución" *Marketing4commerce*. Recurso disponible en: https://marketing4ecommerce.net/historia-de-internet/

(2) PASCUAL, María. "Las estafas por internet representan más del 80% de los ciberdelitos" *Newtral*. Recurso disponible en: https://www.newtral.es/estafas-internet-ciberdelitos/20210806/

(3) CNMC. "El comercio electrónico superó en España los 12.400 millones de euros en el primer trimestre de 2021, casi un 2% más que el año anterior" Cnmc. Recurso disponible en: https://www.cnmc.es/prensa/ecommerce-1T-20211008.

(4) . "¿Por qué el phishing sigue siendo tan efectivo?" *INCIBE, #CyberCamp19* [Vídeo en línea]. Recurso Disponible en: https://www.youtube.com/watch?v=1gNhHmM1tdQ&t=120s

(5) Equipo FayerWayer. "Porno en la web se posiciona en el Top Ten de Internet con XVideos.com" *FayerWayer*, 25 de marzo de 2022. Recurso disponible en: https://www.fayerwayer.com/internet/2022/03/25/porno-en-la-web-se-posiciona-en-el-top-ten-de-internet-con-xvideoscom/

(6) LOPEZ, José María. "Deep Web, Dark Web y DarkNet: los rincones más ocultos de internet". *Hipertextual*. Recurso disponible en: https://hipertextual.com/2022/04/deep-web-dark-web-darknet

(7) The Hidden Wiki. Recurso disponible en: https://thehiddenwiki.org/

(8) PENALVA, Javier "Ser creador de una web de tráfico de drogas ya tiene pena: cadena perpetua". *Xataka*, Recurso disponible en: https://www.xataka.com/servicios/ser-creador-de-una-web-de-trafico-de-drogas-ya-tiene-pena-cadena-perpetua