Trabajo Fin de Grado

INTERNET OSCURA E INTERNET PROFUNDA

Presentado por:

Ainara Aguirreburualde de Dios

Tutor:

Filiberto Pla Bañón

Grado en Criminología y Seguridad

Curso académico 2021/22

RESUMEN

Al hablar de la *Dark Web*, o *Internet Oscura*, nos referimos a todos aquellos sitios de Internet a los que solo se puede acceder mediante un navegador especializado. Así, se garantiza el anonimato. No obstante, aunque es cierto que ciertas personas la usan para evadir la censura del Gobierno, la mayoría de usuarios que se adentran en la *Dark Web* realizan actividades ilegales.

Por otra parte, cuando hablamos de la *Deep Web*, o *Internet Profunda*, nos referimos a toda la información que se encuentra en la Web, pero que no se ha indexado por los buscadores tal y como los conocemos. Así, es todo el contenido público que se encuentra de manera online, pero que no es encontrado ni rastreado por el usuario.

Además, decir que la *Deep Web* engloba tanta información, que es imposible que se pueda determinar de manera exacta cuántos sitios web se encuentran activos en un determinado momento. La *Deep Web* incluye lo que hemos definido anteriormente como *Dark Web*.

Para acceder a la *Deep Web* existen varios niveles de dificultad, añadiendo mayor seguridad cada vez que se pasa de nivel y, por tanto, dependiendo del nivel, se requieren programas específicos para el acceso. Por último, esta zona oculta comprende y esconde el 90 % de la información que está en Internet, la cual puede ser confidencial y personal de cada usuario.

Palabras clave: *Internet Oscura*, *Internet Profunda*, anonimato, información.

ABSTRACT:

When talking about the *Dark Web*, or *Dark Internet*, we refer to all those Internet sites that can only be accessed through a specialized browser. Thus, anonymity is guaranteed. Nevertheless, although it is true that certain people use it to evade government censorship, most users who enter the *Dark Web* engage in illegal activities.

On the other hand, when talking about the *Deep Web*, we refer to all the information found on the Web, but that has not been indexed by search engines as we know them. Thus, it is all the public content that is found online, but is not found or crawler by the user.

Furthermore, to say that the *Deep Web* encompasses so much information that it is impossible to determine exactly how many websites are active at a certain time. The *Deep Web* includes what we have previously defined as the *Dark Web*.

To access the *Deep Web* there are several levels of difficulty, adding greater security every time you change to a higher level, and, therefore, depending on the level, specific programs are required for access. Finally, this hidden area comprises and hides 90 % of the information that is on the Internet, which can be confidential and personal to each user.

Keywords: *Dark Web*, *Deep Web*, anonymity, information.

EXTENDED SUMMARY

To begin with, I have decided to choose this work because of the importance that should be given to the *Deep Web*, since I consider that it is one of the greatest resources offered by freedom of expression on the Internet today.

There is no doubt that technology is advancing according to the change of society, that is, each change implies, directly or indirectly, advocates and detractors, fears due to lack of knowledge, great expectations for the future, etc. Thus, human beings face such changes in a satisfactory way, depending on their values, beliefs, interests, social status, etc. However, it should be kept in mind that "*science can be used for good or evil; this is one of the meanings of the neutrality of science (or technology); in itself it is neither good nor bad*" *(Echeverría,1998)*. In addition, we must also bear in mind what Arandojo pointed out: "*Technology is a neutral element, it is neither bad nor good, we just have to learn how to use it*" *(Arandojo, 2016)*.

Thus, it is not unusual that, despite the benefits offered by the Internet in all senses, there are users who use these benefits as a means to carry out certain illegal activities, such as drug trafficking, pornography, pedophilia, sexual abuse, etc. All these activities are usually carried out, in general, on the so-called *Deep Web* or *Deep Internet*. Such Web is characterized by its anonymity, which, according to Vélez *(2015, 20)*, offers advantages such as:

- The expression of ideas in a free manner, without being recorded by the government.

- Access to valuable information that, in a public way, could not be traced or found.

- The possible access to databases, such as in the area of engineering, science, etc.

- The collection of financial information.

- Cultural manifestations (digital advertising, photography, forums, etc.).

Therefore, having no limit when searching for information, the *Deep Web* is a place to perform both licit and illicit activities, which include "*valuable information such as: Electronic journals, doctoral theses, statistics and reports, dictionaries and encyclopedias, recordings, also generate money without paying tax and you can make some transactions but one to one*" *(Murillo & Díaz, 2018)*.

Special reference should also be made to Bautista's quote: "*The obscure practices of the Deep Web deterritorialize the previous concepts of humans with respect to space, gesture and the concept of self in terms of the conformation of a personality and establish new categories of movement, of interpretation of the body of the other, of staging, of phantasmagoria, of use and acquisition of forms and also of goods and accessories to put themselves on stage and make them reckless, to trap the curious*".

For all these reasons, today's technologies have changed the way we communicate and live, but also the way we do business. For example, in the past, we had to search for the model of glasses we wanted to buy in every store. Nowadays, you only need to search the Internet for what you want to buy, and order it. The same goes for illegal activities, where in the past you had to prepare a more elaborate plan, where people had to specify a day and time to carry out, for example, a drugs o arms deal, as well as an exchange of people.

This topic is something that I have been thinking about for a long time, such as: ¿What exactly is sold on the *Deep Web*?; ¿Who are the buyers?; ¿How did the *Deep Web* come about?; ¿What are the prices of the goods?; ¿Who finances it?; Among and endless list of questions that go around in the head of anyone interested in the subject. These are the objectives that, at first instance, I want to capture in my work, since I believe that they are the most appropriate to solve for any interested person.

In this work we are also going to talk, in depth, about the *Dark Web*, which is a part of the *Deep Web*, characterized as all those Internet sites that can only be accessed through a specialized browser.

In addition, before going completely into this topic, I wanted to go deeper into Computer Security itself, since, if the characteristics contained in any type of security in the technological field are not understood, it is impossible to go into the dark side of computer navigation.

Moreover, I have also focused on the consequences and the main problems of handling personal and confidential information on the Internet. Once the problems and their consequences have been analyzed, I have exposed the main websites as tools for the extraction of users personal information on the Internet.

Once these points have been analyzed, I have started with the general explanation of the *Dark Internet* and the *Deep Internet*, prioritizing the definition of both networks, as well as their main characteristics. From here, I have tried to answer in the clearest and most concise way the questions described above, in order to give a real and current approach of what is nowadays this dark navigation.

Another objective of this work is the explanation of the similarities and differences of both Webs, since, currently, there are still several gaps to refer to these terms. Therefore, I have tried to follow the scheme of the iceberg, in which it is said that the top, what protrudes on the surface, is the web that is known as such (*Surface Web*); Everything below the water is what is called *Deep Web*, and the deepest part of the sea is the *Deep Web* and *DarkNets*.

However, the iceberg scheme is too simple, since, in my opinion, the *Deep Web* is much more than what is not indexed in search engines, and next to the *Dark Web* another term should be introduced, the *DarkNet*. For all these reasons, I believe that this is an important point to discuss, in order to know how to differentiate between when we talk about the *Dark Web* and when we talk about the *Deep Web*.

At a practical level, and simplifying the whole process, there are three different levels of the Internet:

- *Surface Internet*: It is comprised of web pages in which the contents can be indexed by conventional search engines.

- *Deep Internet*: It is comprised of web pages in which the contents cannot be accessed by conventional search engines, as is the case with some databases that require a username and password.

- *Dark Internet*: It is comprised of hidden pages, without any link between them, and by private networks in which access must be made by non-conventional means.

Formerly, these differences were not taken into account, but with the arrival of the NSA and the existence of TOR, a private virtual network whose purpose is to preserve anonymity on the network against government intrusions, has led to the term *Deep Internet* being linked to the *Dark Internet*, which in turn has to be linked to the concept of illegality, since it can be found:

- Black markets of uncontrolled substances.
- Sale of bladed weapons, black weapons, etc.
- Leaks of confidential information.
- Money laundering.
- Impersonation to commit crimes of swindle, fraud, etc.

Having analyzed all of the above, we move on to the part that, in my opinion, is the most interesting part of the work. It deals with the most relevant crimes that can be found on the *Deep Web*. However, it must be said that the *Deep Web* and *Dark Web* are always thought of as darks webs, where all kinds of illegalities are committed, which, in another browser, could not be committed.

This is not entirely true. For example, in the *Deep Web* there is also useful and, above all, legal content, which is made to evade governmental opinion and censorship. Moreover, some of the videos that can be seen on the *Deep Web* can also be found on public browsing, such as YouTube or some social networks (for instance drug trafficking, which can be observed on the *Dark Web*, although it is also continuously observed on conventional social networks, such as Instagram).

Going even further, on too many occasions the saying that reality surpasses fiction is fulfilled, and what supposedly in the *Dark Webs* are myths, become something real in the conventional and public Internet. In this instance we are talking about Red Rooms[1], supposed pages where you can watch live or even participate in a real murder or torture. These are myths that in reality are non-existent, but have become real facts by the retransmission, in known social networks, of killings and terrorist acts.

---

[1] These are supposed pages where, in exchange for bitcoins, you can watch or participate in a torture or murder. Something like being able to see and interact in first person with a snuff film. But fortunately these types of sites are once again an urban legend. There are no sites that stream murders. Or, at least, that is the majority opinion.

We can also talk about the 4chan portals[2], which was originally created to upload any type of anime and manga, but ended up becoming a portal where any kind of content is uploaded, from gore images to real executions.

In conclusion with respect to this section, it should be noted that in the criminal field of computer crime, it should be borne in mind that once a specific activity has been punished, cybercriminals adapt to the different environments they have, so that they carry out what has not been foreseen, or invent new techniques to commit the activity in question. Therefore, on many occasions, in practice they end up finding ways to end up executing the actions that have been prohibited by taking advantage of legal and technical "vulnerabilities" in the regulations in force.

Finally, we move on to the topic of conclusions. The first conclusion to cite is how little knowledge people have about the Deep Web and the *Dark Web*. Nowadays, I have the impression that people surf the Internet without any kind of care, and this is because they are not aware that many of our personal data, due to our lack of responsibility and experience, are in some of the pages of the *Surface Web*.

Statistically speaking, it is shown that the easiest way to find personal information is on the *Surface Web*, however, it should be noted that it is believed, although not entirely true, that the *Deep Web* is the place where illegal activities are continuously taking place. Therefore, personal data found within the *Deep Web* may be used to commit illegal activity, and therefore, it is said that the degree of danger of personal data stored on the *Deep Web* is much greater than on the *Surface Web*.

From a personal perspective and knowledge, this work has given me great knowledge about a part of the Internet, which, in my opinion, at this time I consider more important than public browsing, as it is where there may be greater danger to your own information. This is the knowledge it has given me about the *Deep Web* and *Dark Web*.

On the other hand, not only I have learned about this more anonymous browsing, but this work has helped me to know the main problems you can have about what you publish and upload on the networks, especially if personal information is published.

---

[2] 4Chan was born in 2003 as a site where Internet users could discuss manga and anime. But soon it ceased to be that place on the web to become a place where all kinds of content could be found and where many of the memes that you have ever seen circulating on the Internet were born. There are anonymous users who upload all kinds of images and other users can respond to that image with text or with other images or photographs.

I have also been able to realize that we have at our disposal a multitude of tools that can help you maintain the confidentiality of personal information on the Internet.

In summary and as a conclusion, it has been a work with great contributions both on a personal and profesional level, since apart from solving certain doubts that I had about the *Deep Web* and *Dark Web*, it has helped me to know certain problems and their direct and indirect consequences of the use that you give to your personal information on the Internet, and that there are also several tools that facilitate the security and confidentiality of your personal data.

For all the above reasons, this project has been one of the most important for my academic experience and, to date, the work that has given me more knowledge for future experiences.

ÍNDICE GENERAL:

1. INTRODUCCIÓN.

1.1. MOTIVACIÓN DEL PROYECTO.

Internet como tal está presente en nuestra vida cotidiana desde hace ya muchos años. Aunque los servidores de Internet van aumentando de manera continua y, por tanto, la información contenida en la Red, aún no es posible establecer su tamaño, ya que una gran parte del contenido de la Red no es de acceso público.

Para iniciar el tema, se ha de hablar sobre qué es el concepto de la *Surface Web*. Así, a rasgos generales, se puede definir como la Web que puede ser conocida por cualquier persona en el mundo, y que, por ende, para acceder a ella sólo es necesario cualquier tipo de navegador web. En esta parte del Internet se encuentran las páginas que se conocen mundialmente, como puede ser Facebook, Twitter, Google, etc *(Kaspersky, 2021)*.

Por otro lado, se debe dar especial relevancia al término conocido como *Deep Web*. La *Web Profunda* o *Deep Web* consiste en toda la información que se encuentra en la Web, pero que no se ha indexado por los buscadores tal y como los conocemos. Ello es así gracias a varios factores, los cuales se comentan más adelante.

Por ello, en la *Deep Web* se encuentran informaciones que, de manera general, no están permitidas ni encontradas en la *Surface Web* (por ejemplo libros prohibidos, información personal, números de cuentas, mercancías ilegales, etc.). Así, la *Deep Web* se ha definido como el sitio donde se refugia la delincuencia, aunque dicha afirmación no es del todo cierta.

No obstante, en la *Surface Web* también se puede encontrar información personal, ya que la mayoría de las personas, sin ser consciente de ello, publican sus datos personales de manera pública, por ejemplo en sitios como Facebook o Instagram.

Por último, se ha de citar el concepto *Dark Web*, ya que, en muchas ocasiones, se suelen confundir estos tres conceptos si no se analizan de la manera adecuada. Así, la *Dark Web* se define como el conjunto de sitios que permanecen de manera oculta, por lo que para acceder a esta parte del Internet, se ha de utilizar un navegador web especializado, como puede ser, por ejemplo, TOR (The Onion Router). Con ello, se garantiza de una manera segura el anonimato en Internet. Además, la *Deep Web* incluye en su concepto el término de *Dark Web*, pero no son términos idénticos, existen diferencias entre ellos, como se comenta a lo largo del trabajo.

No obstante todo lo comentado, se debe insertar un cuarto término de especial relevancia, término casi similar al concepto de *Dark Web*, pero con unos pequeños matices que lo hacen distintivo a él. Se trata del concepto denominado *DarkNet*. Así, se dice que la *Dark Web* es toda la información o contenido que permanece oculto en Internet, mientras que las *DarkNets* son esas redes específicas que hacen que ese contenido esté oculto, como puede ser, por ejemplo, la citada red TOR (The Onion Router). Por tanto, el contenido que compone todo el conjunto de la *Dark Web* es ocultado por las diferentes *DarkNets*.

La principal motivación para llevar a cabo este proyecto es la poca conciencia que se tiene acerca de lo que se publica en Internet, ya que no sólo se puede encontrar información personal en la *Deep Web*. En la *Surface Web* también están presentes estos datos personales, y solo se necesitan ciertos conocimientos para saber encontrarlos.

Otro de los motivos son las constantes preguntas que se suelen tener acerca de la *Deep Web* y *Dark Web*, preguntas que a día de hoy se han esclarecido a nivel académico. Por último, también suele llamar la atención los delitos que se pueden cometer mediante dichas páginas, ya que existen bastantes mitos arraigados a la sociedad acerca de este ámbito de Internet, mitos que, en la mayoría de ocasiones, no son del todo acertados.

1.2. OBJETIVOS DEL PROYECTO.

Los objetivos que se han tenido en cuenta para la elaboración del proyecto son:

- Objetivos de la Seguridad Informática y definición de la Criptografía para entender la importancia de la navegación por Internet.

- Definición de la *Deep Web* y *Dark Web*, diferencias y similitudes entre ellas, y también entre la *Surface Web*.

- Estudiar los problemas y las consecuencias de una navegación no segura por Internet, donde podemos dar información personal.

- Mostrar las herramientas disponibles para una navegación segura y confidencial por Internet.

- Analizar los posibles delitos que se pueden cometer en la *Deep Web* y *Dark Web*, aunque aclarando que no sólo se cometen ilegalidades en dichas redes.

1.3. METODOLOGÍA SEGUIDA.

La metodología que se ha seguido al desarrollar este proyecto se basa en los siguientes aspectos:

- Revisión bibliográfica y fuentes de información, sobretodo utilizando la página Web “Xataka".

- Análisis de métodos sobre Seguridad Informática.

- Estudio de herramientas de navegación web seguras y confidenciales.

- Análisis de las relaciones de estas funcionalidades con la comisión de delitos.

- Estudio de casos ejemplo.

2. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA.

La seguridad informática se define como una parte de la informática, encargada de mantener y proteger la privacidad de toda la información que contienen los equipos informáticos. Además, dicha seguridad se basa en unas normas y procedimientos, que tienen como objetivo garantizar la integridad, confidencialidad y el uso correcto de la información que se contiene en un sistema de información.

Los objetivos *(Pla Bañón, 2021)* a tener en cuenta son:

- Confidencialidad: Se debe lograr que la información sólo sea visible por las personas autorizadas. Esto quiere decir que se ha de conseguir la privacidad de los datos que se encuentran y procesan en un sistema informático, para así protegerlos de invasiones y entradas de personas o programas no autorizados. Todo ello se puede alcanzar mediante medidas de índole distinta (como puede ser, por ejemplo, la seguridad física, es decir, tener los equipos en un lugar seguro). De manera física es bastante factible proteger la información, lo difícil es proteger la información en la transmisión de datos, ya que es en este momento cuando éstos son vulnerables (por ello se emplea la técnica matemática de la criptografía, que consiste en

desarrollar métodos para que la información, cuando se desplace a través de Internet, no sea visible).

- Disponibilidad: Se trata de que la información debe estar disponible en el momento en el que se necesita, y, por tanto, se ha de mantener de manera continua el acceso a la información almacenada y procesada en un sistema informático. Por ejemplo, los ataques DOS van dirigidos a vulnerar la disponibilidad (se trata de colapsar un servicio determinado para que éste no pueda mostrar la información).

- Integridad: Se trata de intentar que la información sólo pueda ser cambiada por las personas que estén autorizadas para ello, y así mantener la validez de los elementos de información almacenados. Además, se debe evitar pérdidas accidentales. Por tanto, para evitar dichas pérdidas, se elaboran técnicas que permiten la aportación de redundancia (por ejemplo teniendo varios discos duros sincronizados).

- Autenticidad: Está relacionada con la integridad, y sirve para conocer el origen de los datos. Por tanto, se ha de garantizar la integridad respecto al origen de los datos, con el fin de comprobar si dichos datos provienen de manera real de la fuente o persona que dice ser.

Además, los sistemas informáticos se ven en numerosas ocasiones afectados por distintas amenazas, que se aprovechan de las vulnerabilidades de los ordenadores. Estas amenazas se clasifican en: Físicas o naturales (se pone en peligro los elementos del hardware del sistema); Involuntarias (uso indebido, negligente o descuidado); Intencionadas.

Para defenderse de estas amenazas se utilizan las contramedidas, que se definen como las acciones que se implementan para la prevención de amenazas, y que pueden ser no sólo soluciones y reglas, sino que también es la toma de conciencia por parte de los usuarios. Estas contramedidas se clasifican en varios niveles:

- Físicas: Se trata del primer medio de protección, y consisten en la protección física de los equipos a través de ventiladores, vigilancia, etc.

- Lógicas: Se encuentran como segundo escalón, y se refiere al software, por ejemplo el usuario y contraseña.

- Administrativas: Se trata del tercer escalón, y se refiere a las normas de seguridad que han de cumplir todas las entidades públicas.

- Legales: Se trata del último escalón, y se utilizan cuando el resto de contramedidas han fallado, refiriéndose a medidas judiciales.

Por último, hay que destacar los principios de la seguridad *(Pla Bañón, 2021)*, de los cuales destacan:

- El principio del menor privilegio: A cualquier usuario se le ha de comentar y proporcionar la información necesaria (privilegios de uso y de acceso) para realizar su trabajo.

- El principio de la oscuridad: La seguridad no se basa en el secretismo, es decir, el ocultar defectos y vulnerabilidades no va a garantizar la seguridad del sistema.

- El principio de la defensa en profundidad: Se trata de usar distintas formas de protección, de manera que, si falla alguna, se debe tener más medios de protección. Por tanto, cualquiera que pretenda atacar un sistema, tiene que superar distintas barreras para acceder al sistema, por lo que generalmente lleva a desistir de su objetivo inicial.

- El principio del eslabón más débil: Se trata de establecer todos los puntos de ataque, por lo que no sólo basta con establecer unos mecanismos muy complejos y fuertes en algún punto concreto, dejando otros puntos desprotegidos.

- El principio de la existencia de seguridad en caso de fallo: En el caso de que falle algún mecanismo de seguridad, el sistema debe continuar en un estado seguro.

- El principio de participación universal: En caso de detectar alguna vulnerabilidad o amenaza, el usuario debe comunicarlo al administrador para que lo intente arreglar lo mas rápido posible.

2.1. CRIPTOGRAFÍA.

La criptografía *(Pla Bañón, 2021)* es la manera más satisfactoria para proteger la confidencialidad de los mensajes. Así, se trata de una técnica mediante la protección de documentos y datos, la cual funciona a través de la utilización de cifras o códigos para codificar datos y documentos confidenciales, de manera que la información original no puede ser accesible. Se utilizan dos sistemas:

- **Sistema simétrico.**

También se conoce como "*criptosistema de clave privada*", ya que su principal característica es que se usa una sola clave, que es la misma para codificar y descodificar. Ello supone un problema, ya que si no se tiene la clave, no se puede comprender el mensaje, de forma que dos personas que se comuniquen mediante el sistema simétrico, deben tener ambas la clave. Además, los cifrados de clave privada se basan en el principio de Kerkhoff, que trata de mantener la clave secreta de todos modos, ya que es lo que no permite descifrar los mensajes por usuarios con mala intención.

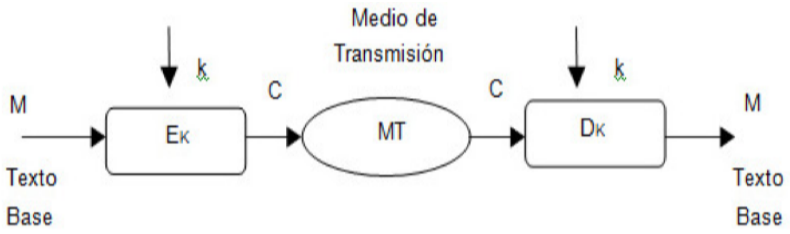


Figura 1. Funcionamiento del criptosistema de clave privada.

En la "*Figura 1*" se muestra el esquema que sigue dicho sistema, de manera que con Ek se cifra el mensaje original aplicando la clave k, y con Dk se descifra, aplicando la misma clave k. Por tanto, la confidencialidad y la integridad se logran si se protegen las claves en el cifrado y en el descifrado.

Algunos ejemplos que destacan dentro de este sistema son: DES o "*Data Encryption Standard*" (actualmente está en desuso); RC4 o "*Rivest Cipher 4*" (se usa para cifrar las wifis); AES o "*Advanced Encryption Standard*", que es uno de los algoritmos de cifrado más usados y seguros en la actualidad, ya que casi todos los dispositivos electrónicos lo soportan y es de acceso público, y se trata del cifrado que la NSA ("*National Security Agency*") usa para asegurar los documentos que tienen la consideración de "top secret".

- **Sistema asimétrico.**

En este caso, la principal característica es la clave pública. Los criptosistemas asimétricos se utilizan para la protección de archivos y unidades completas contra los accesos no autorizados, y para intercambiar mensajes confidenciales. Así, se usan claves para cifrar y descifrar los datos. Además, tienen 2 tipos de claves distintas siempre existentes, una privada y otra pública.

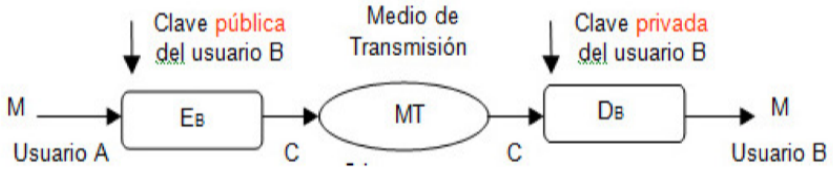


Figura 2. Esquema del criptosistema de cifrado con clave pública y descifrado con clave privada.

En la "*Figura 2*" se muestra cómo el cifrado con una clave pública solo puede ser descifrado con su correspondiente clave privada. Así, se cifra con la clave pública del destinatario, de forma que se consigue que solo él, al tener su clave privada, pueda acceder al mensaje original y real respetando la confidencialidad.

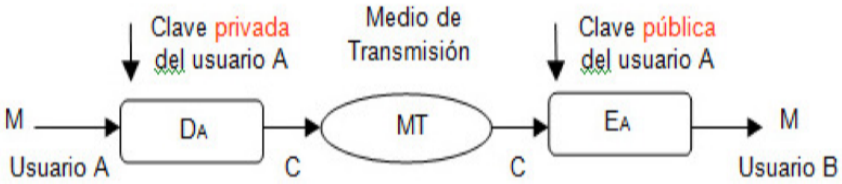


Figura 3. Esquema del criptosistema de cifrado con clave privada y descifrado con clave pública.

En la "*Figura 3*" se muestra el esquema que sigue dicho sistema, en el cual se realiza el cifrado del mensaje con la clave privada del emisor y se descifra con la clave pública del emisor. Por tanto, cualquiera puede descifrar el mensaje, pero se sabe que si se puede descifrar con la llave pública, es porque se cifró con la clave privada correspondiente, con lo cual el mensaje es auténtico, aunque no confidencial.

Así, las dos formas de utilizar el sistema asimétrico para preservar la confidencialidad y la autenticidad del mensaje son, por un lado, que lo cifrado con la clave pública de un usuario solo puede descifrarse con la clave privada de ese

usuario, y, por otro lado, que lo cifrado con la clave privada de un usuario solo puede descifrarse con la clave pública de ese usuario.

3. NAVEGACIÓN SEGURA EN INTERNET.

3.1. RIESGOS DE MANEJAR INFORMACIÓN PERSONAL EN INTERNET.

A día de hoy, existen numerosas redes sociales que te permiten conocer a gente nueva de manera continua. Dichas redes te permiten conocer a infinidad de personas alrededor del mundo, pero también sirven para dar la opinión personal, o para compartir imágenes y vídeos. No obstante, estas redes tienen unos riesgos altos relacionados con la seguridad de nuestra información personal, entre los cuales hay que destacar *(Jiménez, 2021)*:

- Autorización de ciertas aplicaciones: Se trata de un problema, ya que se da el permiso a la recopilación de información personal en el dispositivo, y se puede utilizar en contra nuestra.

- Compartir información personal: La redes nos dan la opción de compartir nuestro nombre, lugar de trabajo, número de teléfono, etc. Hay que tener cuidado con lo que se publica, no es necesario exponer tantos datos personales.

- Caer en trampas y ataques cibernéticos: Por ejemplo, los ataques Phishing, mediante los cuales se roban claves e información personal. Por ello se ha de tener herramientas de seguridad, además de tener los sistemas actualizados.

- Cambios en los permisos de privacidad: Hay que tener claro qué complementos tenemos en las redes sociales, y sus correspondientes servicios.

- Los bots en redes sociales: Los bots se refieren a softwares o programas informáticos que mediante inteligencia artificial realizan tareas automatizadas a través de Internet. Así, pueden realizar un número bastante grande de tareas a la vez (editar textos, responder preguntas, enviar correos electrónicos, etc.). Lo mas común es que se hagan pasar por usuarios reales, pero en estos casos se detectan fácilmente.

3.2. PROTEGER NUESTROS DATOS PERSONALES EN INTERNET.

Lo primero que hay que tener en cuenta es que no se debe proporcionar nuestra información personal a páginas que consideremos poco seguras, por ejemplo, porque te piden más información de la que realmente se necesita.

Además, antes de que se introduzcan datos personales, se ha de asegurar que la página web tenga una política de privacidad, en la cual se detalle de manera explícita qué se va a hacer con nuestra información.

No se debe poner disponible en Internet lo que no queremos que se comparta con otra persona, ya que una vez se ha subido a la nube, es prácticamente imposible eliminar ese contenido. Para aclarar dicho apartado, se ha de definir qué es la nube. Así, la nube se define como un conjunto de servidores alrededor de todo el mundo que están conectados para su funcionamiento como un ecosistema único, y, además, ello permite que cualquier información esté a nuestra disposición en cualquier momento. Además, si se utilizan tarjetas de crédito o similares, se debe ejecutar en un protocolo de Internet seguro (como por ejemplo https[3] o a través de plataformas de pago fiables como PayPal).

Para proteger la identidad de uno mismo, podemos crear una cuenta que esté destinada a utilizar los servicios que necesitamos, sin que esté vinculada a datos personales reales.

Además, se debe asegurar cerrar las sesiones que se hayan abierto. Hay que dejar claro que no basta con cerrar el navegador, ya que a veces las sesiones se siguen quedando abiertas. Por otra parte, el problema puede aumentar si la sesión se ha abierto en un ordenador que no es el nuestro, ya que, por razones obvias, hay más probabilidad de que accedan a los datos de nuestra cuenta.

Por último, hay que administrar las contraseñas de un modo inteligente, por ejemplo, no hay que usar para todos los sitios la misma contraseña. Lo más sensato es tener una contraseña distinta para cada sitio, y, de manera obvia, hay que utilizar contraseñas con significado personal, y cuanto mas compleja sea, mayor seguridad *(Security, 2019)*.

---

[3] Es un protocolo que consigue una conexión de manera segura entre el servidor y el cliente, la cual no puede ser interceptada por personas no autorizadas. Es la versión segura del http (Hyper Text Transfer Protocol).

3.3. WEBS QUE PERMITEN OBTENER INFORMACIÓN PERSONAL.

Existen diversos sitios Web que se dedican a proporcionar datos privados a toda persona que lo solicite, y, además, la mayoría de ellos de manera anónima y gratuita. Las Webs más conocidas son *(Coll, 2015)*:

Indexeus: Buscador que proporciona datos personales que han sido robados de bases de datos[4]. Indexa contraseñas y registros de usuarios aprovechándose de brechas de seguridad, por ejemplo, de algunos servidores famosos como Adobe o Yahoo. También se muestra la lista negra en la que aparecen los usuarios.

Los creadores de dicho buscador han asegurado que el objetivo no es publicar esta información para que se use de una manera ilegal o fraudulenta, sino que se ha creado para concienciar y sensibilizar a la sociedad en general. Además, según su opinión, una Web como Indexeus sirve para ayudar a las autoridades y aumentar la seguridad en Internet.

No obstante, este buscador es bastante cuestionable en torno a su legalidad, ya que, además de robar tus datos personales sin tu consentimiento, se ha de pagar para poder verlos. Por tanto, la mayoría de opiniones aseguran que Indexeus es, además de ilegal, inmoral.

Dateas: Buscador de información personal que, mediante servicios de gestión, búsqueda y localización, te permite encontrar documentos y registros públicos. El funcionamiento de dicha Web es, simplemente, poner el nombre y apellidos de la persona que se quiere encontrar, y, para una mayor precisión de búsqueda, introducir también su DNI. Es un buscador de pago, y te permite obtener información como el domicilio de la persona, sus familiares, estado civil, etc.

Infobel: Es una guía telefónica de particulares y empresas del mundo. Cuantos más datos proporciones de la persona o empresa que quieres buscar, más técnica y comprometida será la búsqueda. Por último, dicha Web permite encontrar nombre completo, número telefónico y dirección.

Buscardatos: No está disponible en España (sólo funciona en Chile, Paraguay y Argentina). Funciona buscando por nombre y apellidos, dirección, DNI, teléfono y Código Postal, por tanto, una vez introducidos los datos, el buscador devuelve la información que está disponible acerca de éstos.

---

[4] ANEXO I. Cuentas de correo y contraseñas robadas en Indexeus. Página 50.

Cuitonline: Es un buscador originario de Argentina, y, en este caso, cuando se introduce un nombre o DNI (cuit), funciona devolviendo direcciones, deudas, trabajo reciente, etc. Es un buscador gratuito y abierto a todo el mundo, en el cual se obtiene información de las personas que se quiere.

Spokeo: Se encuentra en Estados Unidos, y es un buscador que utiliza la información que se encuentra en redes sociales para realizar la búsqueda de la persona en cuestión. La manera de realizar la búsqueda es introduciendo el nombre, email, teléfono o una dirección, en lo que mediante todos los datos descritos, se localiza un mapa y se devuelve toda la información necesaria. El buscador es de pago, mediante una subscripción mensual.

Pipl: Es el buscador de datos personales en la *Deep Web*. Funciona buscando un nombre, nombre de usuario, teléfono, email, y, si se dispone de la información necesaria, también introduciendo la localidad. Mediante estos datos, el buscador rastrea en archivos oficiales, registros criminales, redes sociales, etc.

Por tanto, es un buscador similar a los descritos anteriormente, pero con la característica única de que es capaz de obtener información de la *Deep Web*. El funcionamiento es:

1) Se realiza la consulta de un email, nombre, usuario o teléfono.

2) El crawler (pequeño programa informático que, de manera automática, analiza las páginas web) entra en la *Deep Web* para buscar lo relacionado con la información que se ha solicitado.

3) La información extraída se guarda, de manera temporal, para posteriormente analizarla.

4) Un conjunto de algoritmos inteligentes filtran la información extraída para devolver un resultado que se ajuste más a lo que buscamos.

5) Se devuelven los datos obtenidos al usuario.

Estos buscadores se encuentran en la parte visible de Internet. No obstante, en la *Deep Web* también se encuentran portales que, a cambio de dinero, proporcionan todo tipo de información personal y confidencial (números de cuentas bancarias, cuentas PayPal, tarjetas de crédito, etc.). Para llegar hasta ellos es bastante costoso, ya que

de manera oficial no existen, ni los buscadores los tienen indexados, pero una vez se ha conseguido entrar, se observa lo habitual que es el tráfico de información confidencial.

Por tanto, cualquier medida que se tome para protegernos es, a veces, inútil. Siempre hay que vigilar dónde se introducen nuestros datos, ya que cualquier persona que consiga entrar en la *Deep Web* puede hacerse con ellos, o incluso falsificarlos, ya sea por diversión o por algún tipo de beneficio.

3.4. WEBS DONDE PODEMOS CONFIGURAR NUESTROS DATOS PERSONALES.

Algunos sitios de Internet permiten ocultar o prescindir de información que se quiere mostrar a los demás, sobretodo las redes sociales. No obstante, aunque la información no se muestre a los demás usuarios, los creadores de estos servicios de Internet sí tienen acceso, por lo que pueden proporcionar esos datos a terceros.

Facebook: Es la red mas famosa de todo el mundo, y permite ocultar casi en un 100% la información a los demás, es decir, es la opción que permite proteger de manera casi completa nuestros datos, pero se dice que se está cerrado al mundo en sí. Es decir, ciertas críticas que tiene Facebook se debe a que, al tener tantas opciones de privacidad, no te das a conocer de manera completa al mundo exterior, ya que, por ejemplo, se puede tener una cuenta sólo para que la pueda ver la persona en sí, sin existir la opción de que sea visible para los demás, y eso es lo que genera esa sensación de no permitir conocer a toda la comunidad en su estado puro. Así, existe la opción de tener cerrado el perfil, sólo pudiendo verse una foto y el nombre. Además, existe la opción de que, a través del buscador, no puedan buscar nuestra información y si, por algún casual la encuentran, que no se puedan enviar ni mensajes ni petición de amistad.

En este caso, las opciones básicas de privacidad son: *Público* (se puede ver el perfil por cualquier persona); *Amigos de amigos* (el perfil se puede ver por los agregados como amigos, y los amigos que tengan nuestros amigos); *Amigos* (el perfil sólo puede verse por los agregados como amigos); *Solo yo* (el perfil sólo lo puede ver el propietario de la cuenta).

Dichas opciones se pueden configurar, y, por tanto, a cada elemento de la página se le puede poner una opción diferente. Por ejemplo, si una persona quiere que su foto sea vista por todo el mundo, se marca la opción de "*público*" en el álbum, y si la misma

persona quiere que sus publicaciones sean sólo leídas por sus amigos y los amigos de sus amigos, se marca la opción de "*amigos de amigos*" en la privacidad del muro.

Twitter: En este caso, aunque no se proporcionan muchos datos personales, se centra en lo que se escribe de las empresas, ya que se han creado programas que rastrean dicha red para extraer esta información. Por tanto, lo que se ha de lograr es proteger los tweets mediante los cuales las empresas puedan lucrarse del contenido de éstos.

Existen dos opciones de privacidad: *Público* (nuestro contenido está al alcance de cualquier persona); *Abierto* (el perfil sólo lo puede observar la gente que uno elige).

Linkedin: Es una red que, de manera mayoritaria, se centra en un uso profesional, no personal. Por defecto, esta red permite a Google que pueda indexar toda nuestra información, por lo que aparece todo nuestro perfil en el buscador. Muchas empresas eligen la opción por defecto, ya que les interesa mostrar toda su información. No obstante, existen cuentas que prefieren mantener su privacidad, por lo que se pueden personalizar su perfil, desmarcando lo que no se quiere mostrar (fotografía, lugar de trabajo, actividad que se muestra, etc.).

Por ejemplo, si se tiene asociado el Twitter a Linkedin, se puede establecer la opción de que los tweets no aparezcan. Otra característica de dicha red es que, si se entra en el perfil de otra persona, a dicha persona le aparece una notificación de que ha sido visitado (dicha opción también es modificable para ocultarse de los demás). Por último, también está la opción de no mostrar los contactos que se tengan.

Google+: La red se ideó con la idea de llegar al mismo nivel de Facebook, aunque no ha sido capaz de derrotar a la red social más conocida a nivel mundial. En Google+, de forma obligatoria, se ha de compartir con todo el mundo la foto de perfil y la de portada, y el nombre.

El resto de opciones se pueden configurar (por ejemplo los contactos con los que se tiene relación). Además, los datos personales son configurables, al igual que Facebook, en cuatro tipos de opciones (cualquier persona en la web, círculos ampliados, tus círculos o sólo tu). Por último, aunque no es recomendable, también se puede compartir la ubicación actual.

Google (Buscador): El buscador también permite controlar la privacidad, ya que, además de guardar el historial, también dicho buscador almacena las búsquedas, lugares visitados, vídeos vistos y búsquedas en YouTube.

Aunque se puede tener la opción de que no se guarden los datos, no se garantiza de manera completa que lo que se ha almacenado se borre, aunque parezca que ya no esté. Además de guardar las búsquedas, también almacena a qué hora se han realizado, las veces que se han buscado, etc.

3.5. HERRAMIENTAS PARA EVITAR DEJAR RASTRO EN INTERNET.

3.5.1. ENVIAR CORREOS ELECTRÓNICOS DE FORMA SEGURA.

Hay que destacar que todos los correos electrónicos (emails) existentes en el mundo son interceptados y almacenados en la base de datos de la National Security Agency (NSA) de Estados Unidos. Por tanto, si se quiere tener una cierta precaución respecto a los emails, con el objetivo de que éstos no acaben en manos de terceras personas, se ha de tomar una serie de medidas.

La primera solución es elaborar un servicio propio de correo electrónico, aunque, además de la complejidad que acarrea, otras redes de correo electrónico pueden ignorar los mensajes o considerarlos como *spam* (correo basura).

Otra opción es encontrar un proveedor de correo electrónico que no venda a sus clientes y que, además, no se encuentre en Estados Unidos. Los correos más conocidos en España, como Gmail o Outlook, tienen situados sus servidores en territorio norteamericano. Por tanto, algunas alternativas que conocemos, aunque no siempre sean gratuitas, son:

HushMail: Es un servicio seguro tanto para empresas como para particulares, en el cual existe una versión gratuita (sólo se puede utilizar 25MB de espacio). Existe también un servicio de pago (se aumenta la capacidad de almacenamiento, según la versión escogida, de 1GB a 10GB).

CounterMail: Se considera como uno de los mejores servicios para utilizar de manera segura el correo electrónico, aunque sea de pago. Dicho servicio utiliza memoria RAM y LiveCDs, y los mensajes se cifran mediante OpenPGP, el cual se trata de un estándar de código abierto, que se basa en el cifrado PGP, con el fin de proteger la información distribuida por Internet, como por ejemplo por correo electrónico,

mediante el sistema de criptograma de clave pública y de firmas digitales, que usan parejas de claves pública - privada para cifrar y firmar la información. Además, para una mayor seguridad, se ofrece la opción de comprar una llave USB para almacenar la clave y poder utilizar dicho servicio en cualquier momento.

NeoMailBox: Es un servicio de pago proveniente de Suiza, donde los mensajes son cifrados con OpenPGP. Además, se protege la IP del usuario mediante el anonimato, y se admite la migración de un dominio al servicio. La capacidad más económica es de 1 GB, aunque pagando un poco más se puede obtener 5GB o 10GB.

Por último, citar que existe la forma de enviar correo-e encriptado, y por tanto confidencial, a través de servidores habituales como Google, pero mediante aplicaciones de clientes de correo-e que permitan realizar esta función, como por ejemplo Thunderbird, el cual se trata de un cliente de correo y chat gratuito que se puede utilizar de manera fácil, por su simpleza a la hora de configurarlo y personalizarlo.

3.5.2. NAVEGACIÓN SEGURA.

Actualmente, casi todos los navegadores tienen incorporados el modo de navegación privada, como es el caso de Mozilla Firefox y Google Chrome. Así, en estos casos el navegador no almacena ni rastrea nada de lo que se busca (historiales, usuarios, contraseñas, etc.), y las cookies, es decir, los datos que un navegador guarda automáticamente en el ordenador cuando un usuario visualiza una página web, se borran al cerrar la ventana. No obstante, que no se rastree lo que se busca no significa que la navegación sea segura, ya que, aunque la información no se almacene en el ordenador, seguramente sí que se esté almacenando en las webs que se visitan.

Además, también se puede configurar el navegador para que se pueda utilizar sin tener que usar la navegación privada (por ejemplo deshabitar los scripts de JavaScript para que los navegadores que se visiten no puedan ejecutar ningún código de rastreo o que se bloquee el acceso a páginas que pueden ser destructivas para el ordenador).

Para que una navegación sea privada, segura y sin registro alguno, se utiliza, por ejemplo, el navegador TOR, el cual es un sistema que protege la comunicación entre el ordenador del usuario y el servidor al que se le hace las peticiones. Su funcionamiento se basa en utilizar una red voluntaria para que cada petición que se haga siga una ruta diferente y no se pueda rastrear su recorrido. Así, antes de usar la ruta más corta, se hacen varios saltos hasta llegar al usuario. No obstante, mientras se

está utilizando TOR, la conexión a Internet se va a ralentizar, aunque no significa un problema real para el funcionamiento del ordenador. Aunque TOR permite que no se pueda rastrear las peticiones, no funciona correctamente si el usuario no tiene cuidado en sus movimientos, ya que no sirve de nada que se mueva anónimamente por Internet si, acto seguido, se rellenan formularios con datos personales.

Por último, si se quiere realizar búsquedas en las que no se registre nada, se utiliza, por ejemplo, el buscador DuckDuckGo, donde todas las búsquedas que se realizan son privadas y confidenciales, es decir, nadie tiene acceso a los resultados que se obtengan excepto la persona que realiza la búsqueda. Un buscador similar a DuckDuckGo, que ejecuta la misma tarea, es StartPage (antiguamente se denominaba Ixquick), que trata de un metabuscador provisto en Holanda, el cual su característica principal y distintiva es su privacidad.

3.5.3. SISTEMAS OPERATIVOS SEGUROS.

En este caso, hay que destacar el sistema operativo Tails, una distribución GNU / Linux, que se basa en Linux y en el LiveCD. Si lo usamos en un Pendrive, cuando se pone en el Ordenador, carga el sistema operativo y la RAM, lo que permite que una vez se desconecte el Ordenador, desaparezca cualquier tipo de rastro. Dicho sistema operativo mantiene anónimo hasta quienes lo crearon, con el fin de ayudar a mantener el programa lejos de los Gobiernos. La particularidad es que está diseñado para forzar todas las conexiones salientes mediante la red TOR. Así, se garantiza la privacidad y anonimato en la red.

Por último, Tails usa tecnologías como: Sistemas PGP; El sistema KeePassX (sistema de gestión de contraseñas); Para acabar, el plugin Off-The-Record (cifrado de chats).

4. LA RED OSCURA.

La *Red Oscura*, o *Dark Web*, forma parte del conjunto que engloba la *Deep Web* (*Internet Profunda*), y son servicios y páginas web mediante los cuales no es posible acceder a través de los buscadores públicos y que todo el mundo conoce, como puede ser DuckDuckGo, Google, etc. Así, la *Dark Web* se compone de un conjunto de páginas ocultas, a las cuales sólo se puede acceder mediante ciertos buscadores, como puede ser, por ejemplo, TOR. Por tanto, los usuarios pueden acceder a este tipo de redes mediante ciertos buscadores anónimos, pero también, una vez accedido al navegador, se mantiene una navegación de manera confidencial y anónima, ya que

estos navegadores usan servidores proxy (equipo informático que hace de intermediario entre las conexiones de un servidor y un cliente, filtrando los paquetes entre ambos) para que su IP sea casi imposible de rastrear.

Gracias a su difícil rastreo, la *Dark Web* es la forma de navegación web de muchos criminales, que usan dicho sistema para la oferta de servicios y actividades ilegales (un ejemplo a citar, la Europol en 2020 expuso los resultados de la operación llamada "DisrupTor" *(Europol, 2021)*, encaminada a vendedores y compradores de productos ilegales en la *Dark Web*).

En relación a los peligros que puede suponer el acceso a la *Dark Web*, se sitúa en que los ciberdelincuentes se mueven por este tipo de páginas con su anonimato impoluto, y ello supone que sea más accesible el realizar ciberataques, creando riesgos para el usuario que navega por dicha página, como puede ser: Infección a través del malware, es decir, un programa que se ejecuta en los equipos informáticos con el fin de tomar el control del sistema o robar información, y que, además, se instala sin que se pueda conocer, y realiza determinadas funciones sin que el usuario se dé cuenta; Phishing, el cual es un ciberataque que consiste en robar los datos de los usuarios, como puede ser el número de la tarjeta de crédito; Espionaje y secuestro de cámaras Web; Robo de identidad o credenciales; Entre otros *(Soto, 2021)*.

No obstante, aunque se considere que la *Dark Web* es el sitio ilegal para los criminales, esta afirmación no es del todo cierta, ya que también posee un ámbito positivo dentro de ella. Así, se producen navegaciones totalmente legales en países donde existe la censura, por el acceso a una navegación privada sin que el Gobierno pueda rastrear dicho servicio. Además, también permite la fácil navegación de manera anónima, respetando en todo momento la privacidad del usuario.

Por tanto, en la *Dark Web* se encuentra tanto servicios comerciales y financieros, como servicios de mensajería, blogs, webs de venta de productos, servicios criminales, etc.

Para comprender mejor dicho concepto, a continuación se expone un ejemplo que puede servir de modelo. Así, se debe de imaginar que tenemos en nuestro dominio una página web de destino, sin enlace entrante ni saliente. Por tanto, nuestra página sólo puede ser vista por los usuarios que sepan de la dirección URL exacta. De este modo, sólo se puede acceder a la página con el conocimiento de la URL exacta, pero ello no significa que la página no sea pública, es decir, sigue permaneciendo pública pero de manera oculta, siendo accesible sólo para los usuarios con dicha información.

Esta explicación ocurre a menudo con los blogs que no han sido publicados, pero que siguen existiendo en Internet, considerándose como parte de la *Dark Web (Archanco, 2014)*.

Por otro lado, las redes privadas virtuales también podrían considerarse parte de la *Dark Web*, como es el caso de TOR (The Onion Router), consistente en una red privada con el objetivo de garantizar el anonimato de los usuarios, que necesita de un software específico para poder navegar por dichas páginas.

4.1. THE ONION ROUTER (TOR).

Hasta hace poco, no se conocía de manera consciente y real la existencia de la *Deep Web* y la *Dark Web*. No obstante, gracias al descubrimiento de la red virtual privada denominada TOR, “The Onion Router” o “La Red Cebolla”, que se encarga de preservar el anonimato en la navegación frente a las intromisiones de los Estados, desencadenó a que el término de *Deep Web* se arraigue intensamente con la *Dark Web*. Aunque esto no es del todo correcto, se ha ligado a acciones ilegales, ya que, en ésta, se puede observar: Venta de armas; Mercados negros de sustancias ilegales; Filtraciones de información secreta; Suplantaciones de identidad para el robo de tarjetas de crédito, DNI, etc.; Lavados de dinero; Entre otras actividades de escasa legalidad.

Figura 4. Estructura del cifrado de la red TOR.

Mencionar que TOR es una red completamente gratuita, creada para evadirse de las medidas de control que ejercen los Gobiernos hacia los usuarios. Para garantizar el secreto de la información consultada y el anonimato, TOR cuenta con nodos de salida y nodos intermedios, mostrados en la “*Figura 4*”. No obstante, hay que tener en cuenta que el anonimato en Internet de manera perfecta, es decir, al 100 %, no existe, siempre se deja algún rastro, incluso dentro de TOR, aunque puede ser extremadamente complicado rastrear la información en este tipo de sistemas.

De este modo, TOR permite traducir las URLs de la *Dark Web*, caracterizadas por la combinación de 16 caracteres, que carecen de sentido lógico entre ellos, formados

por letras y dígitos que comiencen por 2 y terminen en 7, acabándose con el pseudo dominio ".onion" (a modo de ejemplo podemos citar los sitios de la *Hidden Wiki*, como puede ser http://kl4gp72mdxp3uelicjjslqnpomqfr5cbdd3wzo5klo3rjlqjtzhaymqd.onion *(Fernández, 2021c))*.

Además, la red TOR basa su funcionamiento en un sistema de distribución, aunque no se puede decir que sea una red P2P donde las partes actúan de manera autónoma, respondiendo a un protocolo de comunicaciones y consenso común, ya que se cuenta con los clientes de la red, con los usuarios que hacen posible el tráfico de TOR, y con algunos usuarios que cumplen la función de servicio de directorio para la navegación por TOR *(Academy, 2022)*. Así, los integrantes de la red pueden intercambiar información sin intermediarios y de manera directa.

Existen diversos motivos por los que se puede utilizar la red TOR, siendo algunos legales, y otros muchos ilegales. No obstante, existen varias ventajas que se pueden resumir en *(Espinosa, 2019)*:

- Libertad: Lo más característico de TOR es la navegación por Internet sin censura. A día de hoy, los Gobiernos intentan la ocultación de información privada a sus ciudadanos, restringiendo el acceso a diferentes sitios webs.

- Vigilancia: Si algún usuario consigue infiltrarse en nuestra red local doméstica, puede extraer (ver lo que realizamos, consultar nuestra actividad, etc.) toda la información y actividad que se realiza online, lo que se ha de relacionar con la actividad relacionada con la navegación web, no con otros temas relacionados con el hackeo de un sistema o una red. Utilizando la red TOR, si alguien ha conseguido infiltrarse, no puede saber lo que se está haciendo en Internet.

- Bloqueo de rastreadores: En una navegación cotidiana y pública, cuando se busca un producto en Internet, tiempo después nos aparece publicidad relacionada con esos productos. Si se utiliza TOR, cada sitio web consultado es aislado, y, por tanto, los rastreadores de publicidad no pueden seguir tu rastro, y, por ende, no mostrar publicidad.

- Seguridad: Ello es así ya que sus navegadores basan su funcionamiento en cifrar varias veces cualquier paquete de información transmitido y recibido cuando se está navegando, pasando por varios nodos de TOR, en los cuales se añaden varias capas de seguridad.

No obstante, añadir que, mientras existen numerosas ventajas al utilizar dicha Red, también nos podemos encontrar aspectos de escasa moralidad, como puede ser: Tráfico de drogas; Filtraciones privadas; Asesinos a sueldo, etc. Además, es común el uso de dicha Red para la comunicación entre sectas y grupos terroristas, por lo que la Policía está continuamente pendiente de cualquier movimiento, con el fin de detectar cualquier movimiento relacionando con estos actos ilegales.

5. LA RED PROFUNDA.

La *Red Profunda*, o lo que es conocido como *Deep Web*, es todo el contenido de Internet que no puede ser indexado por los buscadores comunes públicos, como pueden ser Yahoo, Google, etc. *(D., & D., 2015)*.

Al contrario de la *Surface Web*, o *Internet Superficial*, que engloba todo el contenido que se conoce, es decir, todas las páginas y webs a las que se acceden de manera habitual, la *Deep Web* se encuentra oculta para los navegadores y buscadores cotidianos, y, por tanto, no puede ser localizada de una manera sencilla.

¿Por qué no pueden ser indexadas las páginas de la *Deep Web*? Generalmente, se resume en que la información contenida en la *Deep Web* se observa en sitios generados de manera dinámica, por lo que es muy complicado que pueda ser encontrada por los buscadores. Además, un motivo puede ser que la página esté protegida por una contraseña, por lo que tiene el acceso restringido, o que para acceder a la web sea necesario la utilización de un software específico *(Rochina, 2017)*.

Dentro de la *Deep Web*, se encuentran todo tipo de actividades ilegales *(Araújo, 2019)*: Compra de armas; Hackeos de cuentas PayPal; Blanqueo de Bitcoins; Trata de personas; Prostitución; Tráfico de libros, música, películas, etc.; Entre otras. No obstante, no hay que acudir al mito de "*La Deep Web siempre se utiliza para la realización de actos ilegales e inmorales*". En la *Deep Web* también se observan actos legales, a modo de ejemplo, citar los protocolos de seguridad para banca y seguros.

Por último, se debe citar los factores que hacen posible que la *Deep Web* no sea indexada por los buscadores tradicionales, los cuales son:

- La *Deep Web* contiene en su programación un archivo *robots.txt* (código *Disallow*), el cual actúa impidiendo que entre toda araña que respete las normas de

éste. La instrucción Disallow es capaz de restringir el acceso a una ruta. Así, haciendo un Disallow, los robots no son capaces de acceder a la página web.

- La programación de la página se realiza mediante *Flash* (imposibilita la lectura por los buscadores). Además, de manera general, Flash es independiente del sistema operativo y navegador, aunque el usuario debe tener instalado Adobe Flash.

- La *Deep Web* es protegida mediante algo tan simple como una contraseña, pero la característica es que es desconocida para los robots que la intentan indexar.

- Cuando una araña consigue acceder a la página, no llega a encontrar información a indexar, ya que la *Deep Web* se genera de forma dinámica.

5.1. NIVELES DE LA RED PROFUNDA.

Hay que hacer especial mención a los niveles[5] que se pueden encontrar en la *Deep Web*. A día de hoy, se conocen 7 niveles *(YouTube, 2019, sobre los niveles de la Deep Web)*, los cuales mediante más te adentres en ellos, más oscura se tornará la navegación. Dicho de otra manera, cada nivel es mucho más peligroso que su antecesor:

- Nivel 0: Es el nivel mas sencillo de todos ellos. Prácticamente, es aquel nivel que ves la primera vez que entras. Es de fácil acceso y contiene páginas con información básica, con temáticas suaves o páginas sin sentido, las cuales dicen tener contenido impresionante, pero no es del todo cierto. Simplemente son placebos para llamar la atención de la gente y obtener visitas. Básicamente encuentras lo que puedes tener de manera sencilla y sin riesgos buscando en Google.

- Nivel 1: Este nivel nos permite acceder a la *Deep Web* de manera fácil, pero las páginas están un poco ocultas, es decir, debes llegar a ellas por medio de enlaces. Se pueden observar temáticas como pornografía, foros, páginas abandonadas pero que aún funcionan, etc. Por tanto, se comienza a observar temas específicos, como por ejemplo la afición a “hacer gárgaras con leche”, la cual trata de una afición en la que ciertas personas se graban cantando una canción mientras hacen gárgaras con leche, obteniendo numerosas visitas por dicha acción.

[5] *ANEXO 2. Clasificación de los niveles de la Deep Web (Ugaz, 2020). Página 51.*

- Nivel 2: Ya se hace un poco mas complicado para acceder a este nivel. Así, se necesita de un buen navegador y hacer uso de proxies. Aquí comienza la parte ilegal de la *Deep Web*, con ventas de armas, drogas, contrabando, entre otros.

- Nivel 3: Dicho nivel es definido en varias webs como el nivel donde empieza la artillería pesada. En este nivel, ya se considera importante el saber cómo entrar de forma anónima a la *Deep Web* (como puede ser mediante el buscador alternativo TOR). Se encuentra pornografía infantil, secretos del Gobierno, contratos, hackers que saben que ingresaste a ese nivel y que quieren hackearte y, evidentemente, también rastrearte, etc.

- Nivel 4: Es definido como el nivel donde la censura no existe. Puedes ver los vídeos más escabrosos de asesinatos, de torturas, venta de órganos, etc. Se trata del nivel donde cualquier petición de hackeo es muy probable que se lleve a cabo, todo ello bajo el riesgo de ser una víctima. A partir de dicho nivel, el BitCoin es la moneda por defecto, por lo que es difícil rastrear las transacciones.

- Nivel 5, 6 y 7: Son niveles desconocidos, especialmente porque son de difícil acceso incluso para los hackers más experimentados del mundo. Se puede encontrar secretos gubernamentales, seres de otros planetas, ilumnatis, diseños de tecnología futurista, experimentos, etc. Se dice que para poder acceder al último nivel se necesita una máquina cuántica, además de saber de programación y hacking cuántico.

Por lo comentado en este apartado, podemos observar que es muy importante que, antes de adentrarnos en la *Deep Web* y *Dark Web*, hay que tener en cuenta que somos usuarios en terreno desconocido, por lo que es conveniente formarse antes de abordar este tema tan complejo.

5.2. RECURSOS DE LA RED PROFUNDA.

Entre los recursos que nos proporciona la *Deep Web*, podemos destacar los siguientes (*Archanco, 2014*):

- Recursos científicos de la *Deep Web*: Por ejemplo, la Web del Conocimiento, que es una de las mayores bases de datos de citas mundiales con mas de 54 millones de registros.

- Recursos estadísticos de la *Deep Web*: A modo de ejemplo citar Eurostat, definida como fuente estadística de todos los países de Europa.

- Recursos sobre legislación de la *Deep Web*: Destacar Eurolex, la cual incluye cualquier disposición e información legal sobre la legislación actual y los Tratados Europeos.

5.3. LAS MARIANAS WEB.

Se dice que dicho concepto se encuentra en el sexto nivel de la *Deep Web*, y debido a su dificultad, no se puede acceder mediante TOR *(B., 2020)*. Así, se especula que en esta parte de la *Deep Web* comienzan las especulaciones acerca de la utilización de una herramienta denominada "*Closed Shell Systems*" (Sistemas Cerrados), de manera adicional a otra denominada "*Polymeric Falcighol Derivation*" (Derivación Polimérica Falcighol).

Sin embargo, todo ello son herramientas y nombres ficticios, es decir, originados de la nada, sólo algunos usuarios terminan por creérselo. No obstante, como se ha comentado, para acceder a varios sitios web, se necesitan de programas y configuraciones más técnicos y avanzados que TOR. Estos sitos son los que forman las *Marianas Web*, la cual se divide en capas (quinto, sexto y séptimo nivel), en el cual más alto el acceso, más avanzado el usuario y el cómo acceder a la capa.

¿Por qué es tan secreto las *Marianas Web* que deben ser escondidas de tal forma? No hay una respuesta científica y exacta a dicha pregunta, aunque nos podemos guiar de foros especializados en la *Deep Web* y de usuarios experimentados.

Así, algunas personas comentan que existen sitios en los que se puede disponer de un sicario, así como de compañías especializadas en venta de armas prohibidas y militares. Además, existe el comercio con seres humanos, órganos y animales exóticos *(De Softonic, 2021)*.

No obstante, también hay partes "legales" en las *Marianas Web*, ya que algunos foros están controlados por el Partido Pirata Chino (*Manuel Fernández, 2019)*, grupo con la finalidad de abogar por la libertad de expresión dentro de su país.

Otra buena acción a comentar es el intercambio de información que se efectúa entre los grupos de hackers, los cuales se han unido en la lucha contra la pedofilia,

tema que se puede observar de manera continua en este tipo de niveles de la *Deep Web*.

6. DIFERENCIAS Y SIMILITUDES ENTRE AMBAS REDES.

El término que a día de hoy es conocido como *Deep Web*, fue establecido por la empresa de alto rango en indexados denominada “Bright Planet”, el cual lo usaron para poder detallar contenidos no indexables *(YouTube, 2018)*, como por ejemplo los paywalls (barrera de pago digital configurada por los editores para cierto tipo de ofertas digitales), las solicitudes de bases de datos dinámicas, entre otros elementos que, mediante el uso de buscadores básicos, se hace complicado encontrarlos. No obstante, posteriormente se encontraron con “*Silk Road*”, referida a una página web relacionada con la droga, la cual sólo es posible acceder si navegas mediante el uso de TOR, por lo que se garantiza el anonimato. Si se hace un encargo, sólo puedes pagar mediante BitCoin. Por tanto, no queda rastro de quién compra la droga ni de cómo se hace el pago. Gracias a Silk Road, los medios de comunicación comenzaron a utilizar el término *Deep Web* para referirse a otros términos, como la *Dark Web*.

Por tanto, debido a estos malentendidos, Bright Planet defendió que el término *Deep Web* es inexacto para referirse a la *Dark Web* y *DarkNet*. No obstante, el malentendido ya estaba arraigado a la sociedad, y distinguir estos elementos se ha convertido en una tarea realmente costosa *(Fernández, 2021a)*.

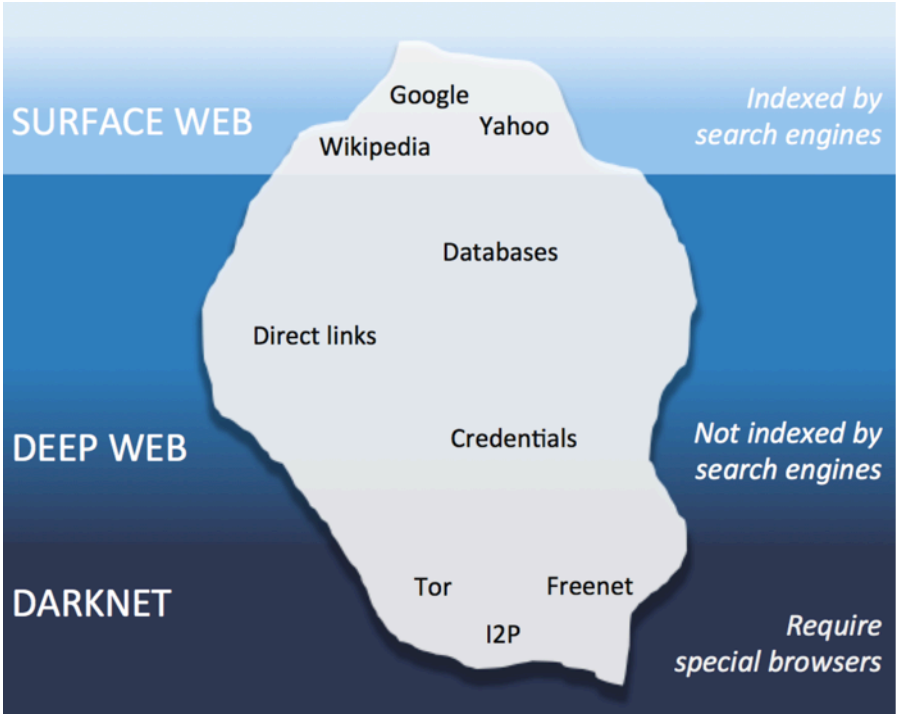


Figura 5. Esquema del Iceberg.

De manera general, para distinguir los términos de *DarkNet*, *Dark Web*, *Deep Web* y *Surface Web* se utiliza el esquema que se muestra en la "*Figura 5*", denominado esquema del iceberg *(A., 2019)*. Lo poco que sobresale en la superficie, la punta, se conoce como *Surface Web*.

Lo que hay debajo del agua es la *Deep Web*, y la parte más profunda es la *Dark Web* y *DarkNet*. No obstante, este esquema es muy sencillo, ya que la *Deep Web* es mucho más de lo no indexable en buscadores, y al lado del de *Dark Web* hay que introducir otro término, como se ha comentado en la introducción, el de *DarkNet*, que no suele aparecer. Así, existe una pequeña diferencia entre estos dos términos, ya que *Dark Web* y *DarkNet* no es exactamente lo mismo, existen unas pequeñas puntualidades a comentar.

Por ello, a continuación se procede a describir cada uno de estos cuatro términos (*Surface Web*, *Deep Web*, *Dark Web* y *DarkNet*):

- *Surface Web*: Es conocida como "*Surface Net*" o, dicho de otra manera, "*Red Limpia*". Se trata del Internet que conocemos toda la sociedad de manera sencilla, ya que se puede acceder fácilmente desde cualquier navegador, y, además, los usuarios son rastreados sin ninguna complicación a través de su IP. Se compone no sólo por páginas indexadas por los buscadores tradicionales como Yahoo o Google, sino también por las webs a las que se puede acceder de manera pública aún sin estar indexadas, como pueden ser las redes sociales (Twitter, Facebook, etc.).

Por otro lado, mencionar que el tamaño exacto de la *Surface Web* no es posible descifrarlo de manera cierta. Según Internet Live Stats, se compone por más de 1.139 millones de webs. Si nos basamos en los datos de WorldWideWebSize.com, la *Surface Web* se compone por 4.700 millones de páginas indexadas. De la manera que sea, la *Surface Web* sólo es una pequeña porción de todos los datos que se encuentran en el ciberespacio.

- *Deep Web*: Se puede decir que la *Deep Web* es el término contrario a la *Surface Web*. Además, si se tiene en cuenta que, en el 90 % del contenido de la red, no es posible acceder mediante buscadores básicos, se está hablando de que existen muchos datos contenidos en la *Deep Web*. También es conocida como "*Web Invisible*", y se trata de toda la información que se encuentra online, pero que no se puede acceder de manera pública. Así, podemos hablar de páginas estándar que son protegidas por un paywall, pero también se habla de archivos de DropBox o de correos electrónicos (emails) almacenados en servidores.

Además, también se compone, por ejemplo, por páginas dinámicas generadas al consultar una base de datos. A modo de ilustración, si se busca un hotel en una ciudad determinada para un día en específico, la página creada con los resultados se indexa en ningún buscador, es temporal y, por tanto, forma parte de la *Deep Web*, como las consultas bancarias y análogas.

- *Dark Web*: Forma parte de la *Deep Web* y, en muchas ocasiones, es confundida con ésta. Se trata de esa porción de Internet a la que sólo es posible acceder a través de aplicaciones concretas. Si la *Deep Web* compone el 90 % del contenido de Internet, la *Dark Web* compone solamente el 0.1 % de ella *(Fernández, 2021b)*.

Algunas páginas, como Diccionary.com, la definen como: "*La porción de Internet que está intencionalmente oculta a los motores de búsqueda, usa direcciones IP enmascaradas y es accesible sólo con un navegador web especial: Parte de la Deep Web*" *(www.dictionary.com, 2000)*. De esta manera, aunque las dos están ocultas de los buscadores tradicionales, la *Deep Web* es una recopilación de todo lo que hay fuera de ellos, lo cual incluye la *Dark Web*.

Además, existe el mito de que, como la *Deep Web* es la parte de Internet que no está indexada por los buscadores tradicionales, la *Dark Web* no puede ser indexada por ninguno. Esta afirmación no es del todo cierta, ya que aunque en Google no vas a encontrar el acceso a ella, en otros buscadores específicos sí lo puedes encontrar.

En algunos de ellos se puede acceder desde la *Surface Web*, como Onion City, que trata de un proyecto que no ha sido creado para combatir el crimen, sino simplemente como una herramienta para poder acceder a mas de 650.000 páginas escondidas bajo los dominios .onion, sin que sea necesario utilizar un navegador concreto, como puede ser TOR. También existen buscadores dentro de la propia *Dark Web*, como Torch, el cual ha indexado más de un millón de sitios web. No obstante, citar que Torch no puede ayudarte sobre el estado de los enlaces.

- *DarkNet*: Dicho término fue instaurado por cuatro investigadores de Microsoft en 2002, los cuales lo definieron como una "*colección de redes y tecnologías que podría suponer una revolución a la hora de compartir contenido digital*".

Para comenzar a explicar dicho concepto, hay que decir que, mientras que la *Dark Web* es todo el contenido oculto que se encuentra en Internet, las *DarkNets* son esas redes específicas, como TOR o I2P, que alojan dichas páginas. Así, aunque Internet sólo hay uno, sí que existen diferentes *DarkNets* en sus profundidades, ocultando el

contenido comprendido en la *Dark Web*. La más popular es TOR, una red de anonimato que contiene su propia *DarkNet*.

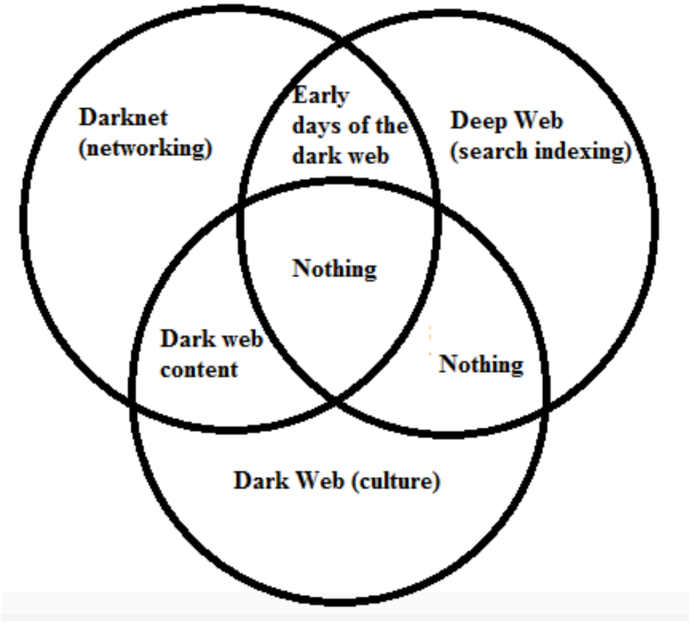


Figura 6. Imagen que diferencia la Dark Web de las DarkNets.

Así, aunque no existe una definición perfecta y preestablecida para las *DarkNets*, se ha de tener en cuenta que aunque de manera técnica es algo diferente, en muchas ocasiones se suele utilizar dicho término para referirse a la *Dark Web*. Por ello se muestra la "*Figura 6*", que sirve para diferenciar de una manera más clara y visual estos dos conceptos. Con todo ello, para poder diferenciarlo, se dice que la *DarkNet* son las redes ocultas en sí, mientras que la *Dark Web* se refiere a dos cosas:

- Para referirse al contenido, a las Webs Oscuras.

- Para hablar de la cultura que implica, un concepto ambiguo para referirse a todo lo comentado, y que se confunde la mayoría de ocasiones con *Deep Web*.

7. TIPOS DE DELITOS QUE PUEDEN TENER RELACIÓN CON AMBAS REDES.

Para comenzar, citar que la navegación por la *Deep Web* o *Dark Web* por parte de los usuarios no es considerado un delito en sí, es decir, en la actualidad no existe ningún tipo penal que sancione como delito el navegar en la *Deep Web*. No obstante, que no esté regulado expresamente en el Código Penal Español, no quiere decir que

todas las acciones y navegaciones que se realicen tengan validez y queden impunes dentro de la *Deep Web (Díaz, 2020).*

Los delitos más populares de cometer dentro de la *Deep Web* son el delito de pornografía infantil y el delito de tráfico de drogas. A continuación se explica con detalle el método que utiliza la Policía para el seguimiento de dichos delitos *(R., 2021)*:

- **Delito de pornografía infantil.**

La manera que utiliza la Policía para este tipo de delitos es mediante el uso de "anzuelos", es decir, adentrarse en las profundidades de la *Deep Web*. Así, una vez adentrados en la *Deep Web*, dejan esos desapercibidos "anzuelos" con contenido de pornografía infantil, pero que en realidad llevan indexado un archivo de localización, por lo cual en el momento que el usuario descarga dicho "anzuelo", lo que se está produciendo es ese seguimiento del archivo o "anzuelo", que lleva hasta la dirección IP de su ordenador mediante su cuenta de Internet.

Una vez se ha localizado al usuario, la Brigada de Delitos Tecnológicos pide la autorización judicial correspondiente, la cual se pide al Juez de Guardia en el Juzgado de Instrucción correspondiente. Una vez obtenida la autorización, se procede a efectuar la entrada y registro en la vivienda del usuario con el fin de localizar el ordenador, o, en todo caso, todos los dispositivos de almacenamiento que puedan contener archivos con pornografía infantil.

Una vez obtenidos dichos archivos, se detiene al usuario y se le lleva en presencia judicial, con la acusación formal por un delito de posesión de pornografía infantil, regulado en el artículo 189.5 del Código Penal, que dice: "*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. 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].

A modo de ejemplo, citar la operación internacional que se realizó para frenar la pornografía infantil en la Deep Web, en la cual se utilizó el rastreo de los BitCoins para frenar dicha delincuencia, que acabó con la detención de 338 usuarios que se

[6] *Texto extraído de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en concreto de su citado artículo 189.5.*

adentraban en la página web “Welcome To Video”, en la que existía todo contenido relacionado con pornografía infantil *(Europa Press, 2019)*.

- **Delito de tráfico de drogas.**

El modo utilizado por la Policía para estos delitos es idéntico al comentado anteriormente. Hay que hacer un especial apunte para estos delitos ya que, de manera obvia, el comprar droga para consumo propio no se considera delito de tráfico de drogas. No obstante, ello no quiere decir que no pueda considerarse como una infracción administrativa grave, que requiere su correspondiente sanción, con arreglo al artículo 36.16 de la Ley de Seguridad Ciudadana, que dice: “*El consumo o la tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas, aunque no estuvieran destinadas al tráfico, en lugares, vías, establecimientos públicos o transportes colectivos, así como el abandono de los instrumentos u otros efectos empleados para ello en los citados lugares*”[7]. La multa que se impone es entre 601 € a 10.400 €.

No obstante, estas operaciones no son de especial relevancia para castigarse mediante el Código Penal. En estos casos se hablan de operaciones de gran escala, lo cual sí puede considerarse delito de tráfico de drogas. Por tanto, con los “anzuelos” comentados, la Policía rastrea la IP del usuario, y, una vez obtenida su IP, la Brigada de Delitos Tecnológicos, pide la correspondiente autorización judicial al Juez de Guardia en el Juzgado de Instrucción y, una vez aprobada, se efectúa la entrada y registro para obtener el ordenador del usuario, para así comprobar el rastro de la operación comercial de compra de drogas, y, además, obtener la propia droga en sí.

El siguiente paso es detener al usuario para llevarlo en presencia judicial, con la acusación formal por un delito de tráfico de drogas, regulado en el artículo 368 del Código Penal, que dice: “*Los que ejecuten actos de cultivo, elaboración o tráfico, o de otro modo promuevan, favorezcan o faciliten el consumo ilegal de drogas tóxicas, estupefacientes o sustancias psicotrópicas, o las posean con aquellos fines, serán castigados con las penas de prisión de tres a seis años y multa del tanto al triplo del valor de la droga objeto del delito si se tratare de sustancias o productos que causen grave daño a la salud, y de prisión de uno a tres años y multa del tanto al duplo en los demás casos*”[8].

---

[7] *Texto extraído de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana, en concreto de su citado artículo 36.16.*

[8] *Texto extraído de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en concreto de su citado artículo 368.*

Un gran avance que se realizó en este ámbito fue la detención de Ross Ulbricht, ya que, en 2015, la Corte Federal de Nueva York le condenó a cadena perpetua, por ser el creador de la web mundialmente popular llamada "Ruta de la Seda" ("Silk Road") en la *Dark Web*, en la cual se vendían drogas y otros productos de escasa legalidad. Se le condenó por narcotráfico, violación informática, blanqueo de dinero y otros cuatro cargos criminales. Su sentencia fue confirmada de manera oficial en 2017, ya que se le desestimó el recurso de apelación *(Pozzi, 2015)*.

Por último, otro mérito a citar trata de la operación que se llevó a cabo durante el año 2020, en la cual se consiguió arrestar a 179 personas, además de incautar alrededor de 500 kilogramos de droga, 64 armas de fuego y 6,5 millones de dólares que se confiscaron tanto en efectivo como en criptomonedas. Se consiguió arrestar a personas distribuidas en todo el mundo (Estados Unidos, Alemania, Países Bajos, Reino Unido, Austria y Suecia). Además, los arrestos logrados se llevaron a cabo mediante una investigación con una puntualidad en común, "*Wall Street Market*". Con dicha operación se advirtió por parte de la Policía que ya no sólo pueden cerrar algunos servicios o acabar con tiendas ilegales dentro de la *Deep Web*, sino que también tienen recursos y opciones para encontrar a los que están detrás de dichas actividades (*Rus, 2020*).

Por otro lado, aunque los dos delitos descritos anteriormente son los más comunes de encontrar, existen numerosos delitos cometidos en la *Deep Web* y *Dark Web*. A modo de ejemplo, citar que pueden surgir dudas en torno a la legalidad de comprar armas de fuego o objetos robados en los blackmarkets de la *Dark Web*. En estos casos, ambas acciones son consideradas delitos en nuestro Ordenamiento Jurídico. A continuación vamos a detallar algunos de los delitos que se cometen en la *Dark Web (López, 2021)*:

- **Tenencia ilícita de armas de fuego.**

El artículo 563 del Código Penal cita: "*La tenencia de armas prohibidas y la de aquellas que sean resultado de la modificación sustancial de las características de fabricación de armas reglamentadas, será castigada con la pena de prisión de uno a tres años*"[9].

[9] *Texto extraído de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en concreto de su citado artículo 563.*

- **Compra y venta de objetos robados.**

También se habla de la compra y venta de objetos robados, como productos tecnológicos (tablets, ordenadores, etc.) o vehículos (generalmente robados en la Unión Europea y "legalizados" en otros países). Citar que dicha acción se conoce como receptación, y se encuentra regulada en el artículo 298 del Código Penal, que dice: "*El que, con ánimo de lucro y con conocimiento de la comisión de un delito contra el patrimonio o el orden socioeconómico, en el que no haya intervenido ni como autor ni como cómplice, ayude a los responsables a aprovecharse de los efectos del mismo, o reciba, adquiera u oculte tales efectos, será castigado con la pena de prisión de seis meses a dos años*"[10].

En el caso de dañar obras de arte, la pena que se le impone al sujeto es una pena de prisión de 6 meses a 3 años o multa de 12 a 24 meses, con arreglo al artículo 323 del Código Penal.

En este apartado se puede hablar de la venta de bases de datos robadas, mediante direcciones de correo que se asocian a contraseñas. Algunos ejemplos conocidos a nivel mundial son: El robo de 100 millones de contraseñas asociadas a Linkedin (2012 y 2016); La copia de contraseñas asociadas a Nintendo (abril de 2020), cuando se permanecía en pleno confinamiento a causa del Coronavirus; Entre otras. En estos casos, el robo se regula en los artículos 197 bis y ter del Código Penal, los cuales imponen una pena de prisión de 6 meses a 2 años para el robo, y una pena de prisión de 6 meses a 2 años o multa de 3 a 18 meses para su venta o cesión.

- **Ciberestafas.**

También se puede hablar de las ciberestafas realizadas a través de correos electrónicos (emails) con todo tipo de descripciones y argumentos (servicios profesionales, contactos sentimentales, etc.) para que los destinatarios hagan un servicio económico, o de las ciberestafas realizadas a través de "phishing", es decir, mails que tienen la apariencia de una entidad bancaria reconocida, a través del uso de datos con números de cuentas PayPal y tarjetas bancarias, sus códigos CVV y sus claves.

---

[10] Texto extraído de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en concreto de su citado artículo 298.

En estos casos, se recurre a los artículos 248.2.b) y 249 del Código Penal, que dicen: "*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: b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción. Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses*"[11].

- **Delito de coacciones.**

Por otro lado, se habla de la sextorsión a través de la utilización de bases de datos que han sido robadas, mediante las cuales se lanza spam indiscriminado mediante bots, enviando correos que incluyen la contraseña del destinatario con el fin de darle credibilidad, y se le amenaza con enviar una supuesta grabación sexual suya a todos sus contactos si no paga la cantidad de dinero exigido mediante bitcoins.

Este tipo de delitos se tipifican como un delito de coacciones, regulado en el artículo 172 del Código Penal, que dice: "*El que, sin estar legítimamente autorizado, impidiere a otro con violencia hacer lo que la ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto, será castigado con la pena de prisión de seis meses a tres años o con multa de 12 a 24 meses, según la gravedad de la coacción o de los medios empleados*"[12].

- **Grabaciones "snuff".**

También se dan casos de grabaciones "snuff", es decir, grabaciones de violaciones, torturas, asesinatos, etc. Dichas grabaciones se realizan a través de la descarga de contenidos o mediante la indicación de los nombres de archivos para la posterior descarga con programas de intercambio de archivos P2P, como por ejemplo µTorrent, eMule, etc.

---

[11] Texto extraído de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en concreto de sus citados artículos 248.2.b) y 249.

[12] Texto extraído de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en concreto de su citado artículo 172.

Podemos citar el controvertido vídeo llamado “Daisy’s Destruction”, el cual muestra la violación, abuso sexual, tortura y asesinato de tres chicas menores de edad. A su principal autor, Peter Gerard, se le condenó por 75 cargos criminales *(Moz, 2020)*.

- **Infracción de derechos contra la propiedad intelectual.**

Además, podemos hablar de la infracción de derechos contra la propiedad intelectual, mediante el permiso de descargas de contenidos audiovisuales (música, películas, etc.), libros (ebooks) y contraseñas para el pirateo de videojuegos.

Para este tipo de delitos nos remitimos al artículo 270.2 del Código Penal, que dice: “*Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, 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*”[13].

- **Usurpación de identidad.**

Por último, se habla de la usurpación de identidad, mediante el espionaje o acceso de perfiles de redes sociales (Twitter, Facebook, etc.) de terceros. Si se accede al perfil, se sanciona como delito de violación de secreto de las comunicaciones y la intimidad con pena de prisión de 1 a 4 años y multa de 12 a 24 meses, con arreglo al artículo 197.2 del Código Penal.

[13] Texto extraído de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en concreto de su citado artículo 270.2.

8. CONCLUSIONES.

La gran mayoría de la gente desconoce la existencia o el funcionamiento de la *Deep Web*, por lo que habitualmente surgen dudas como el tipo de actividades que puedes encontrar, los usuarios que navegan por sus profundidades, etc. Además, a día de hoy, mucha gente tampoco sabe de su existencia, y de que muchos de sus datos personales están presentes incluso en la *Surface Web*, siendo fácilmente identificables para otros usuarios. Así, a nivel académico, este proyecto ha servido para obtener muchos conocimientos novedosos acerca de la *Deep Web* y *Dark Web*, resumiéndolos en:

I. Saber identificar las diferencias existentes entre la *Surface Web*, la *Deep Web*, la *Dark Web* y las *DarkNets*, ya que, aunque son conceptos que pueden ser confundidos fácilmente, en realidad, mediante un estudio exhaustivo y comparando la información, se observa de manera clara que tienen bastantes diferencias entre ellas.

II. Comprender que nuestros datos son fácilmente accesibles no sólo dentro de la *Deep Web*, sino que, si no mantenemos las suficientes precauciones para ello, en la *Surface Web* también pueden estar visibles para todo tipo de personas. Por ello, hay que tener especial cuidado en torno a lo que se comparte en la Internet, ya que, una vez subido a la nube, es prácticamente imposible deshacerse de esos datos, y se suelen quedar de manera permanente en Internet.

III. Conocer diferentes herramientas que existen en Internet, tanto para la obtención de información personal de los usuarios, como para navegar de una forma segura por Internet. Herramientas que no son conocidas por la mayoría de personas, y que sirven para un mayor aprendizaje acerca de cómo manejar nuestros datos personales en Internet.

IV. Conectar de manera clara la criminalidad en las profundidades de la *Deep Web* y *Dark Web*, conociendo los delitos que más se suelen cometer en dichas navegaciones. Además, también se ha podido derrotar un mito que se tiene acerca de estos lugares, ya que, no solo se cometen actos ilegales dentro de la *Deep Web*, también existen buenas acciones en dichas páginas.

En resumen, este proyecto me ha servido para adentrarme en las profundidades de la *Deep Web*, aportándome increíbles conocimientos tanto a nivel personal como laboral.

BIBLIOGRAFÍA.

A. (2019, 11 septiembre). Diferencias entre Surface web, Deep web y Dark web. A2Secure. https://www.a2secure.com/blog/diferencias-entre-surface-web-deep-web-y-dark-web/

Academy, B. (2022, 7 enero). ¿Qué es una red P2P? Bit2Me Academy. https://academy.bit2me.com/que-es-una-red-p2p/

Araújo, S. (2019, 1 octubre). Una semana en la Deep Web, tres años después. Xataka. https://www.xataka.com/analisis/una-semana-en-la-deep-web-tres-anos-despues

Archanco, R. (2014, 20 abril). ¿Internet profunda o Internet oscura? ¿Son lo mismo? ¿si? ¿no? En que quedamos. Lo cierto es que ambos términos son similares pero responden a realidades diferentes. Sin embargo se esta generando Leer Mas. Papeles de Inteligencia Competitiva. https://papelesdeinteligencia.com/internet-profunda-o-internet-oscura/

Archanco, R. (2019, 11 mayo). ¿Qué es eso de la Internet profunda o Internet invisible? ¿Se trata de una especie de triangulo de las bermudas donde solo pueden entrar y salir unos pocos elegidos o Leer Mas. Papeles de Inteligencia Competitiva. https://papelesdeinteligencia.com/internet-profunda/

B. (2020, 30 abril). Qué es la Deep Web, cómo entrar y qué hay allí en pleno 2020. Bloygo. https://bloygo.yoigo.com/visitamos-la-deep-web-para-evitarte-disgusto/

D., & D. (2015, 3 enero). Deep Web: concepto, características y niveles. Derecho de la Red. https://derechodelared.com/deep-web-concepto-caracteristicas-y-niveles/

Deep Web, Dark Web y Dark Net: ¿Qué es cada una? (2018, 17 marzo). [Vídeo]. YouTube. https://www.youtube.com/watch?v=mzXNU5vLNDc

Definition of dark web. (2000). Www.Dictionary.Com. https://www.dictionary.com/browse/dark-web

De Softonic, R. (2021, 14 diciembre). Mucho más allá de la Deep Web: ¿qué es la Marianas Web? Softonic. https://www.softonic.com/articulos/que-es-marianas-web-deep-web-extrema-nzn

Díaz, M. (2020, 13 octubre). ¿Es legal en España navegar por la deep web? Click Jurídico. https://clickjuridico.es/es-legal-navegar-por-la-deep-web/

Espinosa, O. (2019, 24 noviembre). Qué es la red Tor y qué ventajas me puede aportar. RedesZone. https://www.redeszone.net/tutoriales/seguridad/que-es-tor/

Europa Press. (2019, 17 octubre). Cae la mayor red de pornografía infantil del mundo en la Dark Web por el rastreo de Bitcoins. europapress.es. https://www.europapress.es/portaltic/ciberseguridad/noticia-cae-mayor-red-pornografia-infantil-mundo-dark-web-rastreo-bitcoins-20191017141351.html

Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg. Página 38. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

Fernández, Y. (2021a, abril 16). Deep Web, Dark Web y Darknet: éstas son las diferencias. Xataka. https://www.xataka.com/servicios/deep-web-dark-web-darknet-diferencias

Fernández, Y. (2021b, mayo 14). Qué es la Dark Web, en qué se diferencia de la Deep Web y cómo puedes navegar por ella. Xataka. https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella

Fernández, Y. (2021c, junio 8). Red TOR: qué es, cómo funciona y cómo se usa. Xataka. https://www.xataka.com/basics/red-tor-que-como-funciona-como-se-usa

Jiménez, J. (2021, 30 abril). Problemas principales de privacidad en redes sociales. RedesZone. https://www.redeszone.net/tutoriales/seguridad/problemas-comunes-privacidad-redes-sociales/

Kaspersky. (2021, 9 diciembre). ¿Qué es la Deep Web y la Dark Web? www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/deep-web

Ley Orgánica 4/2015, de 30 de marzo, de Protección de Seguridad Ciudadana (2015). *Boletín Oficial del Estado*, 77, de 31 de marzo de 2015. https://www.boe.es/buscar/act.php?id=BOE-A-2015-3442

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (1995). *Boletín Oficial del Estado*, 281, de 24 de noviembre de 1995. https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

López, J. E. A. (2021, 1 diciembre). Delitos en la Dark Web. Revista Byte TI. https://revistabyte.es/legalidad-tic/delitos-en-la-dark-web/

LOS 7 NIVELES DE LA DEEP WEB EXPLICADOS. (2019, 19 diciembre). [Vídeo]. YouTube. https://www.youtube.com/watch?v=mo0Wkkl4syE

Manuel Fernández (2019, 24 de Octubre). La BBC publica una página de noticias en la 'deep web' para evitar la censura. El Español. https://www.elespanol.com/omicrono/20191024/bbc-publica-pagina-noticias-deep-evitar-censura/439206869_0.html

Moz, I. (2020, 9 noviembre). El creador de Daisy's Destruction. Wattpad. https://www.wattpad.com/978798171-expedientes-criminales-el-creador-de-daisy%27s

Pla Bañón, F. (2021). Delito Informático. Apuntes de la Asignatura Seguridad y Criminalidad Informática. Documento inédito. Castellón: Facultad de Derecho, Universidad Jaume I.

Pla Bañón, F. (2021). Fundamentos Tecnológicos. Apuntes de la Asignatura Seguridad y Criminalidad Informática. Documento inédito. Castellón: Facultad de Derecho, Universidad Jaume I.

Pla Bañón, F. (2021). Seguridad Informática. Apuntes de la Asignatura Seguridad y Criminalidad Informática. Documento inédito. Castellón: Facultad de Derecho, Universidad Jaume I.

Pozzi, S. (2015, 30 mayo). El fundador de Silk Road, condenado a cadena perpetua. El País. https://elpais.com/internacional/2015/05/29/actualidad/1432935074_571369.html

R. (2021, mayo 7). Como te Pilla la Policía en la Deep Web. Información Jurídica y Tribunales. https://informacionlegal.es/policia-en-la-deep-web/

Rochina, P. (2017, 10 marzo). Deep Web o Internet Profunda: La realidad ilegal inimaginable. Canal Informática y TICS. https://revistadigital.inesem.es/informatica-y-tics/deep-web/

Rus, C. (2020, 25 septiembre). Se acabó el anonimato de la Dark Web, avisa Europol tras una operación que ha acabado con el arresto de 179 personas. Xataka. https://www.xataka.com/privacidad/se-acabo-anonimato-dark-web-avisa-europol-operacion-que-ha-acabado-arresto-179-personas —

Security, P. (2019, 9 julio). Consejos para una navegación segura - Panda Security. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/consejos/navegacion-segura/?gclid=CjwKCAiA_omPBhBBEiwAcg7smXoELT18tZUQ83zoJ0lylnofBx021z-Yw68y_csRu_rQFUvG7gP9BhoCs_YQAvD_BwE

Soto, P. (2021, 8 septiembre). Darknet: qué es y cómo se accede a ella. Redseguridad. https://www.redseguridad.com/actualidad/cibercrimen/darknet-que-es-y-como-se-accede-a-ella_20210426.html

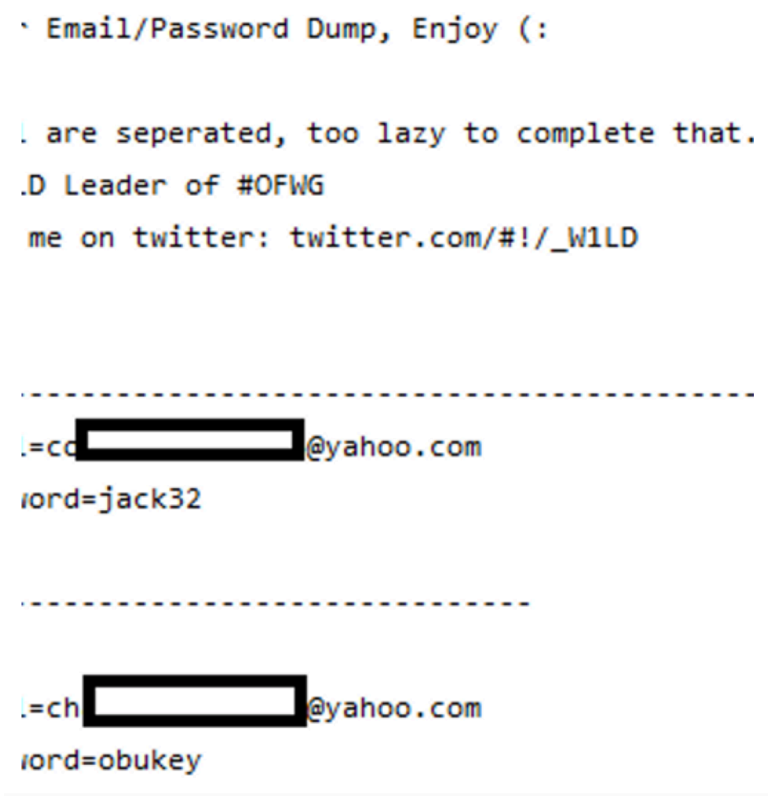
Ugaz, O. (2020, 15 enero). CLASIFICACIÓN DE LOS NIVELES DE LA DEEP. Mapa Mental. Niveles de la Deep Web. https://www.mindomo.com/es/mindmap/clasificacion-de-los-niveles-de-la-deep-web-48f3b0d24f1c44a2b5664bf119b4e2cf

Victoria Coll, M. (2015). Buscador de datos personales en la Deep Web. [Trabajo Final de Grado. Escuela Superior Politécnica UPF]. PDF. https://repositori.upf.edu/handle/10230/25521?show=full

Zavia, M. S. (2019, 29 noviembre). Una semana en la deep web. Esto es lo que me he encontrado. Xataka. https://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado

ANEXOS.

ANEXO I. CUENTAS DE CORREO Y CONTRASEÑAS ROBADAS EN INDEXEUS.



ANEXO II. CLASIFICACIÓN DE LOS NIVELES DE LA DEEP WEB *(Ugaz, 2020)*.