TRABAJO DE FIN DE GRADO:

LA RED TOR: UN ANÁLISIS DESDE EL PUNTO DE VISTA TÉCNICO, DE SUS CONSECUENCIAS PRÁCTICAS Y ASPECTOS LEGALES.

GRADO EN CRIMINOLOGÍA Y SEGURIDAD

CURSO ACADÉMICO 2016/2017

ALUMNA: **Clara Esteller Vidal**

TUTOR: **Manuel Mollar Villanueva**

Extended summary

The evolution of new technologies (ICTs) has brought numerous and important advances. For this reason, society considers them as a fundamental tool because these allow it to be constantly connected to Internet. However, this imperative need also pose important problems which affect both social and virtual people security.

No matter whether posted data has been sensitive or not because all information is equally indexed by traditional search engines, subjecting them to traffic analysis. This allows having under control and tracking what was being introduced and searched to the network. In order to avoid this, users look for alternative methods which enable an anonymous connection, highlighting among them the Deep Web. Although, the access to this part of the web requires services specifically designed for the purpose, an area where Tor predominates. This is considered as the main tool against censorship for being the most widely used and the most well-known. This reputation emerges thanks to support from international organizations, such as Electronic Frontier Foundation (EFF).

In this study, the principal objectives to be achieved are:

1) Learning the technical functioning of Tor and the purposes sought with its use, particularly focusing on the anonymity.

2) Analysing the consequences at a practical level that the existence and its increasing use of users worldwide has caused.

3) A legal study on the legislation aspects that may affect its use, mainly the problem associated with it due to be of the technology field and, especially, different implementing legislation on this matter.

Hence, the first section of this study is emphasizing the importance to know what Tor network is and how it functions. This requires clarifying all key concepts associated with Tor. First of all, its definition is presented in order to get started with the most important concept which includes both its origin and its further development from the Tor Project. This section also describes the components that form this network, which are the nodes (onion routers (OR) and onion proxy (OP)) that must be connected to other nodes through the Secure Socket Layer (SSL) encrypting technology. This is

because the different information properties provided by this protocol, which are the privacy, authenticity, integrity and availability as a basis for cyber security.

From a technical point of view, a distinction must be made between users and servers. On the one hand, there is the process designed to ensure users anonymity in their connections. This is possible through the creation of private circuits which are formed by encrypted connections that link the main nodes OR (at least three of these: entry, middle/bridge and exit nodes). But this would not be possible without the application of asymmetric cryptography (or public key), which prevents that each relay can know the other relays with which it communicates. This encryption method used encrypts each circuit layer through the use of symmetric cryptography (or secret key) by creating a separated encryption layer for each relay. Each of these three channels is connected to the following relay until the last node, so that as the message is sent to the next node the encryption layers are progressively eliminated. This complex structure is the main cause of the network access slowdown and that is why a slower connection can exist. On the other hand, there is the process followed by the hidden services. Hidden services are the services that are used to send and receive data packages in Tor network. These servers, which need TCP protocol to run, have an architecture that allows the users and services anonymity. In this case, the mechanism is the location-hidden services that consist of the virtual distribution of rendezvous points in order to users and servers can communicate not directly, but through these constructed points.

In this first section, the subsections below include other relevant concepts. Firstly, the aims pursued with the use of Tor are mainly anonymity and privacy, but also others, such as implementability, usability, flexibility and facility of design. Secondly, there are the risks in relation to the Tor usage because of the fact that these also exist in this type of networks. The threats are classified in three categories, which are errors committed by the users, problems within the network itself and indirect problems affecting the system. Thirdly, the usage recommendations include the considerations to be borne in mind whether an extreme security conditions are sought or medium-level security is considered as sufficient. Fourthly, the users profile is an important section because not only are Tor now used by citizens subject to oppressive regimes, but also for different sectors of society, such as journalists, IT professionals, cybercriminals and even law enforcement agencies, among other. Subsequently, having explained this, Tor Browser is to be introduced since it is the project developed for ensuring the network access, which has been previously configured to use Tor. There are various

versions of it depending on the operating system of the device used and its download can be made through the official website of Tor Project. In the final subsection, there are ".onion" domains, that is, the characteristic URLs addresses of Tor network. Therefore, although they are server's addresses, these are not considered domains as such, but rather pseudo-domains or high level domains. These present a particular format and so not belonging to DNS (domain name system) controlled by ICANN (Internet Corporation for Assigned Names and Numbers). The main advantage of this system is the greatest difficulty to track the packages of data navigating through the network.

As it appeared to in this study, the second section is to go further into the intrinsic relationship between Tor and the Deep Web. The first thing to know is the meaning of Deep Web. This is the Invisible Web, that is, the part of web whose content is not indexed, nor is it crawled, so it cannot be recovered by traditional search engines. Inside, it can be found the Darknet at which can only be accessed with systems specifically designed for it. Moreover, it allows the users to have direct access to the content that is hosted only in Tor, constituting the deep web of Tor. The Deep Web is represented as an iceberg because the Invisible Web has access to only a minor part of the total web, in comparison of the cyberspace immensity. For this reason, it can be divided into different levels of depth, approximately five to six levels, where there are greater differences as users deepen in the web. An exact count is not available because, after a certain point, the depth and its content is yet uncertain of which only the absence of rules and the security is known. In addition, on the one hand, as it cannot run with the traditional search engines, specific browsers have been designed to search in Tor. Although, in this respect, the importance is in the wikis, which are not browsers as such, but rather lists of hidden services classifications (for example, the most relevant wiki is the Hidden Wiki). On the other hand, there is also a mention of virtual coins, this is, coins used to virtual transactions, especially bitcoins for its popularity in the Deep Web.

The third section add another key point to take in account, and that is the legal aspect by making a distinction between legislation and legal problems related to the usage of Tor. First, it raises the question of whether or not a legal framework exists to regulate this situation. So, what should be highlighted is that the national legislation establishes what the position of each country is in relation to the Internet use and its application to protect users' privacy. Second, this part point out the fundamental role that plays the international standard on technological field, particularly in computer

field. The problems mainly arise by the simultaneity of law enforcement and Tor use. In this moment is when the jurisdiction issues associated with computer data take place for the reason that physical boundaries have disappeared with the emergence and use of new technologies. But where security concerns are growing, is about the protection of personal rights and freedoms, which want to be protected with the Tor use and may be affected with the investigations. Further laws are needed to provide a strong legal and regulatory framework both national and international applicable to cyberspace in order to provide legal cover to Tor use. Therefore, there is a legal vacuum.

To finish this study, a practical approximation work has been conducted in order to put into practice the knowledge acquired, as well as widening and deepening in the research. As mentioned above, Tor is used as a tool to protect users but it is also exploited by criminals who use this network for cybercrime. But, this practical part has focused only on analysing it as a secure platform for cybercrime, given the importance of it for investigation and prevention.

This way, the main conclusions that have emerged from the study are:

1) The main objective of Tor network is to ensure the users and servers anonymity. To achieve it, Tor creates a technically complex circuit that is made up of three nodes among which data is passed from the user to the server. In spite of this technical complexity, the circuit is not safe from all risks. So, its most worrying problem is that the anonymity cannot be granted in absolute terms.

2) The focus is on the use of Tor in the Deep Web and, especially, in the Darknet. The major search engines have indexed the visible Internet content which permits to know the connection and behaviour habits. That is why society thinks that this continuous intrusion constitutes an inadmissible restriction on the rights and freedoms, notably privacy right and virtual freedom. Consequently, users decide to use Tor in order to browse anonymously the network. Thus, they can also access to the content available only in Tor network, that is, the hidden services. Although these services complicate seeking information, it is compensated by the vast amount of existing information.

3) Notwithstanding the importance of Tor use in favour of users' rights, the access to this network to commit cybercrimes cannot go unpunished. Cybercrime is even further expanded with the usage of such anonymizing tools which allow

reaching all kinds of content. All of this has made possible to find out a monumental virtual market which operates according to its own rules and its own virtual currency. This way, an analysis of the Tor use is necessary to evaluate the impact resulting from its participation in cybercrime by making the criminals' investigations much more difficult.

4) The difficulties that previously existed increase with the important legal problem. The use of Tor hinders finding the origin and destination of perpetrators for the cybercrimes, as well as the consequences of these worrying criminal activities. All this complicates the criminal investigation and prosecution. For these reasons, the aim at national, European and international level is to achieve legal coverage, which provides a real basis for fighting this problem. In this way, all authorities responsible for the investigation and prosecution must acquire a minimum training and knowledge in the field. In the cyberspace, the application of the means used by cybercriminals is needed to combat them. But the refusal by the most governments to participate in this network complicates to further the investigation. Thus, it will be necessary a profound conceptual change in order to act and to respond adequately to grave threats encountered in the cyberspace.

In summary, it seeks to acquire comprehensive knowledge of the Tor network through on a detailed analysis of the most important aspects that make up it in order to get a study on the reality of the Tor, its users and the adjacent problems. In this way, the competent professionals in criminal investigations for technological field know what phenomenon they face in order to that crime prevention can be achieved and ensured.

The final conclusions, at the personal level, raise the need to know the existence and operation of Tor. As a result of ICTs influence, the information has become a strategic factor for criminological investigation in the virtual world. It is important to note that the Deep Web provides the criminal opportunity, that is, cybercriminals can exploit the benefits of the Tor use. Therefore, the better action against cybercrime must be taken from the core of criminal action. So, this intervention should necessarily be from the prevention, which is the main tool used by Criminology to reduce all factors that encourage cybercrimes. Special attention must be paid to primary prevention; hence it requires the training and specialization of competent actors by experts with government spending. Consequently, it indicates an essential multilevel awareness that will ensure with a global and multidisciplinary coordination.

Abstract:

The evolution of new technologies (ICTs) has produced the emergence of a society that is constantly connected to the Internet. This provides many advantages, but it also entails important problems due to continuous exposure of data. All information is indexed by major search engines and is therefore subject to a data traffic analysis. Thus, alternatives measures are sought to ensure users' online privacy and anonymity, highlighting the Deep Web. In order to access to this part of web, new users need to use specific systems such as Tor, which is the most well-known anonymity network. The technical functioning of the Tor network is based on the "onion routing" because it is structured in encryption layers. Furthermore, it is considered a fundamental tool to defend users' rights, making both clients and servers anonymous. Despite these advances, this network has led to the emergence of new types of cybercrime. Consequently, the problem transcends physical boundaries, so an effective international cooperation is needed to find responses and to prevent future cases.

Keywords: Tor network; anonymity; users' rights; Deep Web; cybercrime; prevention.

Resumen:

La evolución de las nuevas tecnologías (TIC) ha generado el surgimiento de una sociedad constantemente conectada a Internet. Esto supone importantes ventajas, pero también una continua exposición de datos que plantea problemas significativos. Ello es debido a que toda la información está indexada por los principales buscadores y está, por tanto, sometida a análisis de tráfico de datos. Por ello, se buscan medidas alternativas que garanticen privacidad y anonimato en la red, destacando la Deep Web. Para acceder a esta parte de la web se necesitan programas específicos, siendo Tor la red anónima más conocida. El funcionamiento técnico de la red Tor se basa en el llamado enrutamiento de cebolla al estructurarse en capas de cifrado. Además, se considera una herramienta fundamental para la defensa de los derechos de los usuarios, anonimizando tanto a clientes como a servidores. Aunque estos avances también han favorecido al surgimiento de nuevos tipos de cibercriminalidad. Por tanto, es una problemática que trasciende las fronteras físicas requiriendo una cooperación eficaz a nivel internacional para intentar dar respuesta y prevenir supuesto futuros.

Palabras clave: Red Tor; anonimato; derechos de los usuarios; Deep Web; cibercriminalidad; prevención.

ÍNDICE

1. Introducción

En la actualidad las nuevas tecnologías o TIC (Tecnologías de la Información y la Comunicación), se han convertido en una herramienta esencial, siendo utilizadas diariamente y en todo momento por la mayoría de la sociedad (Cervantes & Tauste, 2015). Esta continua necesidad de estar conectados a la red genera, además de los tantos beneficios conocidos, importantes problemas ya que la constante exposición de datos, sensibles o no, de forma pública genera inseguridad tanto a nivel social como virtual (Vitoria Real, 2015). La información a la cual se accede está indexada por los motores de búsqueda, de manera que los datos son sometidos a análisis del tráfico seguido, permitiendo el seguimiento y conocimiento de lo buscado e introducido por los usuarios en la red. Por esta razón, muchos miembros de la sociedad deciden acudir a la Deep Web, conocida, entre otras denominaciones, como la Internet Invisible, y para ello requieren de medios que les garanticen una conexión anónima. Entre esos medios destaca sustancialmente el uso de Tor (Echeverri Montoya, 2016).

Por tanto, la red Tor es conocida como la principal y más grande red anónima utilizada para acceder a la Deep Web, yendo en aumento su popularidad y el contenido de la misma. Ello es debido, en especial, al reconocimiento de Tor como la primordial herramienta contra la censura, por parte de organizaciones destacadas internacionalmente, como es la Fundación Frontera Electrónica, concediéndole cierto prestigio (The Tor Project, n.d.). Por ello, los principales objetivos de este trabajo son:

1) Conocer su funcionamiento desde el punto de vista técnico y los propósitos buscados, esencialmente el del anonimato.

2) Analizar las consecuencias, a nivel práctico, que produce su existencia y creciente empleo por usuarios desde todas las partes del mundo.

3) El estudio legal sobre los aspectos de la legislación que pueden afectar a su uso, destacando la problemática acarreada por tratarse del ámbito tecnológico y en especial, la distinta legislación en la materia.

En definitiva, se pretende tener un conocimiento global de la red Tor mediante un análisis pormenorizado de todos los elementos más destacables que lo conforman para obtener un estudio sobre la realidad de Tor, sus usuarios y la problemática adyacente. Y así saber a qué fenómeno se enfrentan las investigaciones criminales en el ámbito tecnológico para poder hacer efectiva y garantizar la prevención del delito (MG, 2011).

2. Conceptos

Este apartado incluye la terminología necesaria para el entendimiento del dicho trabajo mediante la explicación de los conceptos claves más relacionados con la red Tor.

2.1. Red Tor

2.1.1. ¿Qué es?

Tor es el acrónimo de *The Onion Router*, es decir, el Enrutamiento/Encaminamiento de Cebolla (Panda Security Mediacenter, 2017). Este es un *software* libre específico[1], que sirve como herramienta para evitar la censura de determinados contenidos que de otra forma se encontrarían bloqueados. La red Tor es la red distribuida más famosa y utilizada como herramienta para dar solución a la privacidad y anonimato en Internet, que se basa en un servicio de comunicación anónima de baja latencia y superpuesta a Internet (Çalışkan, Minárik, & Osula, 2015). Su propio nombre indica la estructura de capas que lo conforma, la cual permite el acceso a ese contenido saltando de una a otra capa bajo la protección del cifrado, impidiendo que las páginas por las que se navega identifiquen la IP desde la cual se accede. De este entramado técnico surge el símil a la *onion*/cebolla.

Este fue creciendo de forma cuando se creó el proyecto Tor en el año 2003, considerándose como la tercera generación de proyectos de enrutamiento de cebolla ya que fue la evolución del proyecto *Onion Routing* del Laboratorio de Investigación Naval. En sus inicios se desarrolló como una red mundial de servidores con la Marina de los Estados Unidos para proteger las comunicaciones gubernamentales, permitiendo la navegación anónima a través de Internet. Pero, en la actualidad, además de los objetivos militares, tiene una gran variedad de usos distintos como periodísticos, policíacos, activistas, etc. (David, Mamani, Es, & Su, 2014).

Garantiza la protección frente a la vigilancia a la que se someten los usuarios cuando acceden a Internet, es decir, al llamado tráfico de datos. Este se caracteriza porque los paquetes de datos están conformados por dos partes: la carga útil de los datos, que es lo que se envía, y el encabezado que se usa para el enrutamiento, el

[1] *Software* libre: de licencia libre, *software* de código abierto. Es aquel que respeta la libertad de los usuarios que adquieran el producto para redistribuir el *software* Tor, no tiene por qué ser gratuito, pudiéndose hacer cualquier actividad con el mismo (como usarlo, copiarlo, estudiarlo, modificarlo o bien redistribuirlo libremente). Por tanto, se hace referencia a la libertad y a la falta de restricciones y no a su gratuidad. https://www.debian.org/intro/free

cual aporta mucha información (fuente, destino, tamaño, tiempo, etc.). Así, la persona que recibe las comunicaciones, en base a la cabecera, puede conocer quién lo envió, pudiendo ser intermediarios autorizados como son los proveedores de servicios de Internet o incluso algunos no autorizados para ello. Por ello, como solución a dicha problemática de plantea el uso de una red anónima distribuida.

2.1.2. Componentes

Esta red se compone de un conjunto de nodos, los cuales se comunican a través del protocolo *SSL/TLS* (cada nodo mantiene una conexión *TLS* con el resto de nodos) (FdIwiki ELP, 2016)[2]. Dicho protocolo garantiza las siguientes propiedades de la información. Por una lado, la privacidad puesto que los datos son cifrados antes de enviarse a través de algoritmos criptográficos (uso de la criptografía simétrica). Por otra parte, la autenticación en cuanto a que una de las partes de la comunicación ha de autenticarse para el envío de los datos. También mantiene la integridad ya que los mensajes incluyen un *MAC* (The Gnome Project, n.d.)[3], lo que posibilita verificar su no modificación antes de su llegado al destino final. Por tanto, también se mantiene la disponibilidad de los datos ya que la integridad es una condición de la disponibilidad, por lo que si se rompe la información no estará disponible.

Existen dos tipos de nodos. Los nodos *OR* o *onion routers* (*tor-relays*), que actúan a modo de encaminadores así como servidores de directorio (FdIwiki ELP, 2016)[4]. Estos mantienen una conexión con cada uno de los otros *OR*, la cual nunca se cierra conscientemente si no es por inactividad. Y, por otra parte, los nodos *OP* o *onion proxy*

---

[2] Protocolo *SSL* (*Secure Sockets Layer*)/*TLS*: protocolo cifrado sobre *TCP/IP*, protocolo con el que funciona Internet. Y puede ser usado por cualquier aplicación que soporte *SOCKS*. Es un protocolo de seguridad en las comunicaciones, permitiendo que sean confidenciales y autenticadas, a través de algoritmos criptográficos. Su uso en la web se distingue porque la *URL* empieza en *https*://. Para las operaciones de cifrado y *hash* utiliza esos algoritmos: el cifrador de llave pública *RSA* 1024, el cifrador de clave privada *AES* 128 bits y el algoritmo de *hash SHA1*. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0885_ChaparroZunigaHD.pdf

[3] *MAC* es el identificador único de una pieza de *hardware* de red, es decir, una tarjeta de red inalámbrica o *Ethernet*. Su significado es *Media Access Control*, la cual puede ser exigida por algunos proveedores de servicios para acceder a su servicio, y viene dada por el fabricante por ello es único para cada dispositivo.

[4] Un servicio de directorio (o SD) es una o un conjunto de aplicaciones que se encargan de almacenar y organizar la información sobre los usuarios de la red. En Tor se publica una base de datos que realiza relaciones entre cierta información y cada *OR,* información conocida por todos los *OR* y usuarios finales que les permite tener conocimiento de la red. Se les conoce como un grupo de *ORs*.

(Tactical Technology Collective Front Line Defenders, 2016)[5] que se basan en la obtención de información del servicio directorio, crear circuitos aleatoriamente mediante la red así como de control de las conexiones de las aplicaciones de los usuarios. Cuando se entabla comunicación con los *OR* no se hace de forma permanente sino que los *OP* deberían de cerrarse cuando no hay circuitos ejecutándose sobre la conexión y habiendo transcurrido cierto tiempo (FdIwiki ELP, 2016).

2.1.3. Propiedades

El uso de dicho protocolo garantiza las siguientes propiedades de la información (Zuñiga, 2015).

Por un lado, se garantiza la privacidad puesto que los datos son cifrados antes de enviarse a través de algoritmos criptográficos. Ello es gracias a la criptografía simétrica usada para cifrar los datos enviados. Las claves son generadas para cada sesión, partiendo de la negociación de un secreto compartido al iniciar la sesión. Servidor y cliente detallan el algoritmo de cifrado y las llaves que utilizarán, lo cual asegura su seguridad y su fiabilidad. Además, garantiza incluso el anonimato de los servidores, es decir, protegiendo un destino en Internet y/o un servicio web, aparte de proteger la identidad de los usuarios, ya que permiten ofrecer un servicio *TCP* que oculta su dirección *IP*. Estos servicios ocultos son servicios comunes que se encuentran alojados al interior de la red, conformando la web profunda de Tor, y utilizan dicha red para enviar y recibir los paquetes de datos. Se desconoce el número de servicios ocultos, existiendo de todo tipo. Pero todos tienen en común que han de basarse necesariamente en el protocolo *TCP*, ya que en caso contrario no puede actuar en dicha red (Echeverri Montoya, 2016).

Por otra parte, la autenticación es garantizada a través de la criptografía de llave pública, en cuanto a que una de las partes de la comunicación ha de autenticarse para el envío de los datos. El servidor se autentica enviando un certificado *SSL* firmado por una autoridad certificadora asegurándose que solo el servidor tiene la clave privada. Si no se produce esta la confidencialidad tampoco ya que la comunicación no será segura.

[5] El *proxy* es un programa o máquina intermedia, la cual funciona en el ordenador, una red local u otro sitio de internet, que oculta la *IP* original permitiendo la comunicación hasta el destino final.

También se mantiene la integridad ya que los mensajes incluyen un algoritmo *MAC* (Código de Autenticación de Mensajes), posibilitando la verificación de su no modificación antes de su llegado al destino final. Por tanto, también se mantiene la disponibilidad de los datos ya que la integridad es una condición de la disponibilidad por lo que si se rompe la información no estará disponible.

2.1.4. Principios de funcionamiento técnico (The Tor Project, n.d.)

Respecto al funcionamiento, es necesario diferenciar entre cómo funciona para el cliente y cómo para el servidor.

En primer lugar, es destacable que la red Tor es un modelo totalmente distinto del sistema llamado *I2P*[6], una red *P2P*[7], y, a pesar de las similitudes que puedan presentar por ser ambas redes *proxy* de anonimato[8], hay que diferenciarlos. *I2P* es un sistema anónimo *P2P* distribuido que pretende ser una infraestructura para dichos protocolos *P2P*, garantizando un mejor anonimato en la comunicación (Zantout & Haraty, 2011). En cambio, Tor es una herramienta para navegar, es decir, una red montada dentro de Internet, cuyo funcionamiento se compone de los elementos explicados a continuación (Electronic Frontier Foundation, n.d.).

Por una parte, se encuentra el proceso seguido por Tor para garantizar el anonimato del cliente cuando se conecta. Su propio nombre indica la estructura de capas que lo conforma, la cual permite el acceso a ese contenido saltando de una a otra capa bajo la protección del cifrado, impidiendo que las páginas por las que se navega identifiquen la IP desde la cual se accede. De manera que esta red está

---

[6] *I2P* es definido como un sistema *Garlic routing* (enrutamiento de ajo), inspirado en el *Onion routing*, siendo la unidad de datos la misma en ambos. Pero este está más desarrollado y centrado en compartir archivos. Está programado en Java por lo que necesita que esté instalado este. Por su diseño la arquitectura es menos vulnerable a los ataques ya que enruta de forma distinta cada paquete de datos (a diferencia de Tor que lo hace en cada conexión) y el camino seguido ida-vuelta es diferente, no existe bidireccionalidad. http://wiki.hacktivistas.net/index.php?title=Tools#TOR

[7] *P2P* es una red entre iguales (*peer-to-peer*) frente a las redes cliente-servidor, en las que el servidor es el único que puede proporcionar el servicio al cliente que se conecta a este. Cada nodo es considerado igual dentro de la red, es un *peer*, y estos son los que aportan los recursos mediante conexiones entre ellos. Al estar interconectados todos los equipos las transferencias pueden ser muy rápidas. http://www.elotrolado.net/wiki/Todo_sobre_P2P

[8] https://geti2p.net/en/comparison/tor

conectándose mediante un conjunto de túneles virtuales, en lugar de realizar una ruta[9] directa. Ello supone que los paquetes de datos viajan de origen a destino a través de una ruta siguiendo caminos aleatoriamente mediante saltos entre relés[10] que permite crear un circuito de conexiones, las cuales se encuentran encriptadas mediante diferentes repetidores distribuidos por la red (Electronic Frontier Foundation, n.d.).

Esto es lo que permite crear esa ruta de red privada, pasando el tráfico por, al menos, tres de esos relés (nodos *OR*) hasta llegar a su destino. Los dos primeros se conocen como relés intermedios (*middle-OR*) puesto que son los que reciben y pasan el tráfico al siguiente relé. Estos, a pesar de que son anunciados en al resto de la red y cualquiera puede conectarse con ellos, no pueden ser identificados como la fuente u origen del tráfico por lo que otorgan mayor seguridad. También pueden denominarse como puentes (*Bridge*-Tor), los cuales no se anuncian públicamente en la red, siendo su función ser la entrada a la red Tor en aquello países donde las *IP* de los *OR* están bloqueadas. Y el tercero es el relé de salida (*Exit-OR*), siendo el último por el que pasa el tráfico de datos antes de llegar a su destino final. Este también puede ser usado por otros usuarios por anunciar su presencia en la red. Al ser por donde sale el tráfico la dirección de esta *IP* es interpretada como la fuente del tráfico por lo que los usos que se hagan pueden ser identificados como la causante. Lo característico de los nodos es que estos son voluntarios, es decir, cualquier persona puede participar en la red Tor como un nodo más configurando su ordenador (The Tor Project, n.d.)[11]. Las organizaciones e individuos que actúan como voluntarios, donando su ancho de banda y poder de procesamiento, son los que posibilitan el funcionamiento de la red (FdIwiki ELP, 2016).

El uso de la criptografía de clave asimétrica es la que impide que cada relé pueda conocer los otros del circuito con los que no se comunica directamente, siendo el único conocedor el *software* Tor del equipo desde el que se accede (Hsu & Marinucci, 2013). Una representación gráfica de ello se aprecia en las figuras 1 y 2 (Tyler, 2007). Los diagramas muestran el mecanismo de cifrado utilizado, el cual va por niveles del

[9] Una ruta es el camino de comunicación en Internet entre su ordenador y el servidor de destino

[10] Los relés (*relays*) de Tor también se conocen como routers o nodos. Estos se encargan tanto de recibir el tráfico como de transmitirlo. Existen tres tipos de relés que pueden ser ejecutados para ayudar al funcionamiento de la red Tor. Estos son los intermedios, los de salida y los puentes.

[11] La propia página oficial de la red explica cómo se apoyan en las donaciones de ancha de banda realizadas por los voluntarios y explica cómo configurar un servidor Tor. https://www.torproject.org/docs/tor-doc-relay.html.en

circuito. La comunicación a nivel nodo se cifra con una conexión *TLS*, dentro de la cual el Directorio Tor lista o registra las claves públicas utilizadas por el cliente para la creación de las tres claves de sesión secretas *AES* (Nechvatal et al., 2001)[12] (las claves simétricas son las utilizadas para el cifrado de una sesión), que son secretas entre sí y en cada salto sucesivo en el circuito. Por tanto, hay una capa separada de cifrado para cada uno de los tres relés, es decir, el cliente Tor al elegir los nodos crea un canal cifrado al nodo de entrada, a través de este se crea el canal cifrado al nodo central y por último, a través del canal anterior se acaba conectando al nodo de salida. Así, los mensajes son enviados al servidor cifrados varias veces en cada uno de los nodos con las claves de sesión negociadas y, a medida que se transfiere al siguiente, se elimina una capa de cifrado ya que las respuestas que da el servidor son cifradas por cada nodo y se descifran por el cliente. Por dicha razón, los mensajes originales únicamente se conocen por el último nodo (de salida), que encamina la información en plano, y no se puede asociar los mensajes por su contenido que entra en un nodo al que sale del nodo (Loesing, Murdoch, & Dingledine, 2010).

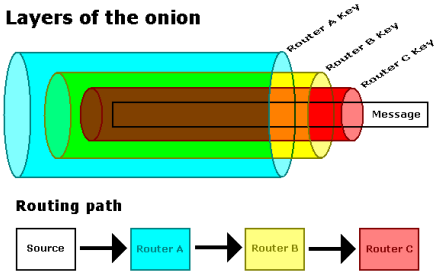

Figura 1. Gráfico del principio de "enrutamiento de cebolla".

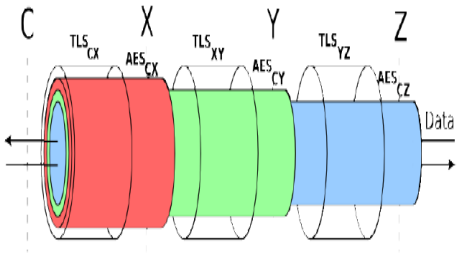

Figura 2. Encriptación Tor

De manera que los usuarios que quieren acceder se descargan e instalan este *software* cliente, el cual utiliza el protocolo de *proxy SOCKS* (Armentano, 2016; Çalışkan et al., 2015)[13] para recibir las transacciones de la red, es decir, que se

[12] *AES* (*Advanced Encryption Standard*) es un método de cifrado estándar. Es un algoritmo simétrico de cifrado por bloques que se utiliza en modo contador para generar una transmisión cifrada. Se obtiene una clave simétrica para cada dirección (dos claves simétricas) a partir de generar una clave compartida *D-H* (protocolo de establecimiento de claves entre partes que no han tenido contacto de forma previa, siendo el medio para acordar y negociar las llaves de cifrado) negociada al inicio de la sesión y no conocida por un tercero.

[13] El *proxy SOCKS* (*Socket Secure*), es inicializado y configurado mediante Tor, trabajando a un nivel más bajo que el *proxy HTTP*. Este es un *proxy TCP*, que intercepta y filtra las conexiones *TCP*, es decir, es un protocolo de Internet encargado del encaminamiento de los paquetes de red mediante un servidor *proxy* entre cliente-servidor. Esto permite que no sea

encarga de interconectar este *software* con la red Tor (Loesing et al., 2010). Al ocuparse de las peticiones *HTTP*[14] y de otros flujos de datos permite el soporte de las sesiones cifradas de extremo a extremo utilizando *HTTPS*[15] o *sockets* seguros.

Una representación práctica de su proceso de funcionamiento se escenifica en las Figuras 3, 4 y 5 (The Tor Project, n.d.).

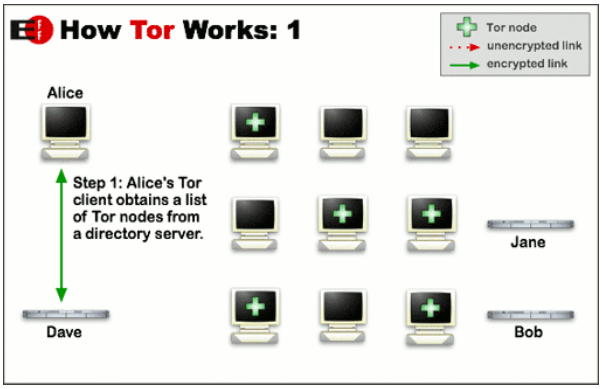

Figura 3. El *software* del usuario construye un circuito de conexiones cifradas a través de relés disponibles en la red, seleccionando tres. Cada uno solo conoce el relé que le dio los datos y al que le entrega los datos, no teniendo conocimiento de la ruta completa de los datos transferidos.

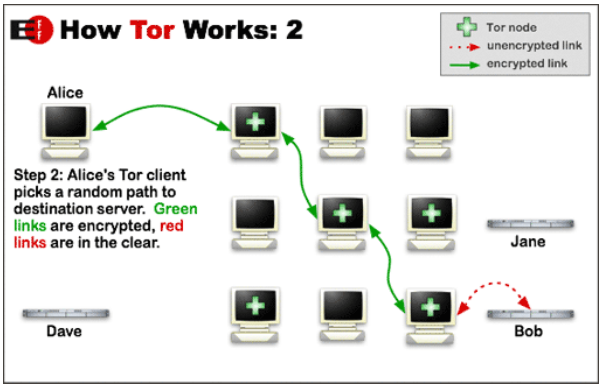

Figura 4. Una vez el *software* de Tor selecciona la ruta aleatoria y cifrada se procede a la transferencia de cualquier tipo de dato hasta llegar al servidor de la web que se quiere visitar. Como cada relé o nodo no conoce más que el salto realizado en el circuito no puede vincular el predecesor y sucesor de la conexión.

---

específico para cada aplicación, sino que es suficiente con que pueda enviar paquetes de datos mediante el *proxy SOCKS*.

[14] *HTTP (Hyper Text Trnasfer Protocol*) es el protocolo usado en las comunicaciones mantenidas entre los navegadores y los servidores web. Estos se caracterizan por requerir que el propio usuario o *software* sea el encargado de modificar la configuración del navegador. Además, solo puede ser utilizado para contenido web.

[15] *HTTPS* es *HTTP* sobre *SSL* o *TLS*, lo cual permite transacciones web seguras.

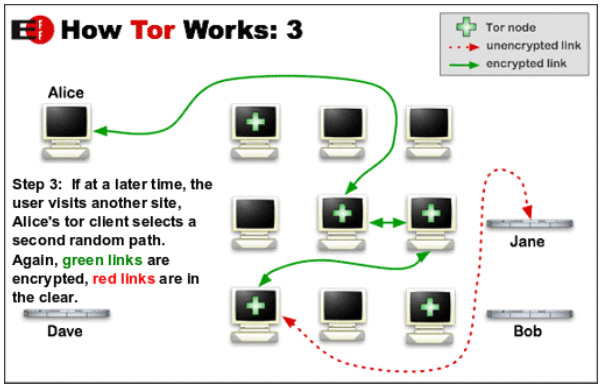

Figura 5. El *software* Tor utiliza el mismo circuito en las conexiones realizadas durante unos diez minutos. Una vez transcurridos estos se concede un nuevo circuito, evitando así que se puedan vincular sus acciones realizadas con las que realizará.

Todo este entramado técnico, es decir, el haber de conformar cada vez el circuito con nodos al azar y seguir todos estos pasos, produce la ralentización de la carga de los accesos. Por esta razón, puede considerarse que la conexión es más lenta que cuando se accede a los navegadores tradicionales pero en los que no se garantiza el anonimato proporcionado por Tor. No soportan este tipo de webs, por lo que no pueden acceder a ellas (Cervantes & Tauste, 2015).

Por otra parte, destacan los servicios ocultos. Son servicios comunes que utilizan la red Tor para enviar y recibir paquetes de datos. Estos servicios pueden ser de cualquier tipo como por ejemplo servidores web, pero todos indispensablemente han de utilizar el protocolo *TCP* para poder funcionar. La arquitectura de estos servicios ocultos garantiza que clientes y servicios sean ambos desconocedores de la ubicación e identidad del otro, asegurando así su anonimato. El mecanismo se conoce como los servicios ocultos de ubicación (Echeverri Montoya, 2016)[16], cuya técnica consiste en la distribución de puntos de encuentro en la red para que cliente y servidor se puedan comunicar.

El proceso que se sigue para la instalación, configuración y acceso a un servicio oculto se compone de los siguientes pasos. En primer lugar, se requiere de la disponibilidad del servicio en la red Tor para que sea conocido por los usuarios que quieran utilizarlo. Por ello, selecciona tres nodos aleatoriamente y construye un circuito

[16] Cualquier usuario puede crear un servicio oculto en la web profunda de Tor mediante la configuración de su propio servidor web. La página propia del proyecto Tor detalla los pasos a seguir para configurar los servicios ocultos de Tor (https://www.torproject.org/docs/tor-hidden-service.html.en).

hacia ellos, no conectándose directamente con estos por lo que conserva su anonimato. Estos son los llamados puntos introductorios ya que son los que reciben las peticiones solicitadas por los clientes, encaminándolas hacia el servicio oculto. Este les enviará su clave pública a cada uno de estos puntos, permitiendo asociar clave pública-servidor. Como anteriormente se ha dicho, se necesita publicitar el servicio oculto y para ello, este crea un fichero en el que consta su dirección *onion,* su clave pública y los puntos introductorios seleccionados. Este fichero se envía a la base de datos distribuida de Tor (*DHT*)[17], la cual registra el servicio y procesa las solicitudes de los clientes. Con esto se ha garantizado la disponibilidad del servicio, debiendo el cliente crear un circuito hacia la *DHT* para mantenerse anónimo. A partir de ello, el cliente recibe el fichero perteneciente a dicho servicio oculto (dirección *onion*, clave pública y lista de puntos introductorios) teniendo ya todos los elementos necesarios para conectarse al servidor. Antes de iniciar dicha conexión, el cliente habrá tenido que elegir un nodo en la red que actuará como punto de encuentro, es decir, será el lugar de encuentro donde finalmente el cliente y servidor puedan comunicarse. Hacia este se creará otro circuito, el cual generará una llave que identificará unívocamente dicho circuito establecido entre punto de encuentro y cliente.

A partir de este paso, el cliente envía un paquete, llamado mensaje introductorio, que incluye la dirección del punto de encuentro y dicha llave generada, a través del circuito creado al elegir aleatoriamente un punto introductorio. Este paquete es cifrado con la clave pública del servicio oculto para que nadie conozca el contenido del mismo. El paso final consiste en el conocimiento del contenido del paquete por el servicio, por lo que puede crear un circuito hacia el punto de encuentro. Este podrá relacionarlo con el circuito previamente creado por el cliente, informándole de que el servicio oculto ha respondido al mensaje introductorio enviado por el cliente. A partir de esto, cliente y servicio oculto ya pueden usar el punto de encuentro para el intercambio de la información.

En definitiva, la conexión entre ambos no será directa ya que harán uso de dichos circuitos creados hacia el punto de encuentro, siendo la manera con la que se asegura el anonimato buscado. Esto es debido a que dicho punto de encuentro desconoce la ubicación de ambos. De manera que para garantizar la comunicación se han de crear, como mínimo, dos circuitos cada uno de los cuales estará conformado por tres relés, uno que conecta al cliente con el punto de encuentro y el otro que conecta servicio con

[17] *Distributed Hash Table:* registra el servicio y procesa las peticiones de los clientes.

el punto de encuentro. Así, la información, que se envía, se distribuye por los nodos principales.

2.1.5. Objetivos

Tor permite la ocultación de la identidad digital de los sitios visitados a los que accede el usuario, la evitación de la censura existente en Internet y las reglas de los filtros así como la ocultación de destinos en línea desde los Proveedores de Internet (*ISPs*) y otros mecanismos de vigilancia(Collective & Front Line Defenders, 2016).

Por tanto, el propósito principal del uso de dicho navegador radica en el anonimato y privacidad que concede. Al igual que el resto de diseños de anonimato de baja latencia, pretende evitar que los nodos o las comunicaciones sean asociados con el usuario por parte de los atacantes o restos de usuarios (The Tor Project, n.d.). Por ello se dice que protege del análisis de tráfico, una forma de vigilancia realizada a través de Internet, ya que analizando dicho tráfico de datos se posibilita llevar a cabo un seguimiento de las acciones realizadas por el usuario al conocer el origen y destino de este tráfico (Çalışkan et al., 2015). Pero hay que tener en cuenta que dicho tráfico no lo cifra (Starke, 2016). Esto supone que dicho anonimato permite, no solo evitar represalias a la hora de ejercer el derecho a la libertad de expresión aportando opiniones e información, sino que también permite la elusión de los cortafuegos de Internet utilizados por parte de los países con regímenes opresores, pudiendo acceder a sitios restringidos en sus respectivos países de origen (Watson, 2012).

Pero hay que considerar otros aspectos que han garantizado su evolución. Por una parte, se destaca la implementabilidad, es decir, que se pueda poner en funcionamiento y utilizar a la práctica, no costando su ejecución por ser una carga de responsabilidad excesiva para los operadores. Por otra parte, la usabilidad, es decir, que pueda ser utilizado ya que un sistema de uso dificultoso supone el acceso de menos usuarios. Ello se concibe como un requisito fundamental para la seguridad y por eso, Tor no ha de solicitar excesivos requerimientos para con estos. Esta es la razón por la cual se garantiza que se pueda ejecutar en el sistema operativo del usuario y no obligar a cambiarlo. También se requiere su flexibilidad, en cuanto a que ha de ser flexible para así poder usarse como medio de pruebas e investigaciones futuras para solventar problemas que surjan. También se busca un diseño sencillo, es decir, que se entiendan bien los protocolos y los factores relativos a la seguridad. En definitiva, persigue la implementación de un sistema que esté integrado por los

enfoques aceptados que garanticen el anonimato (Dingledine, Mathewson, & Syverson, 2004).

2.1.6. Riesgos

Existen amenazas en Tor que pueden ser clasificadas en tres grupos distinguidos: los errores del usuario, los problemas de la propia red Tor y los problemas indirectos que afectan al sistema (Çalışkan et al., 2015).

Por una parte, respecto a los errores de usuario se destaca un buen uso del sistema, no accediendo a contenidos, direcciones u objetos con ejecutables incrustados que desvíen la comunicación de los relés del circuito. Esto provocaría una fuga en el mecanismo del sistema y se darían a conocer las direcciones IP reales de los usuarios. Esta razón es por la cual no se aconseja el uso de Torrent ya que el ser una aplicación basada en la compartición de archivos puede no seguir la configuración de *proxy* del navegador de Tor conectando directamente con otros usuarios (Çalışkan et al., 2015). También se da el mismo caso respecto al acceso a sitios web *HTTP* (no *HTTPS*) ya que, como los nodos de salida pueden ver los paquetes que circulan por ellos, podrían ser sometidos a seguimientos y control. El *HTTPS* es seguro, evitando que los nodos de salida accedan al contenido transportado, siempre y cuando los servidores a los que accede el cliente sean confiables y se corrobore siempre la veracidad de sus certificados(Abbott, Lai, Lieberman, & Price, 2007).

Por otro lado, los problemas propios de Tor se centran en su propio diseño, pudiendo afectar a la privacidad de los usuarios. Por una parte, que los usuarios sean redireccionados a servidores especiales mediante operadores de telecomunicaciones puede facilitar ataques *MitM* (*Man-in-the-Middle*)[18]. Estos son conocidos como ataques de correlación de extremo a extremo (*end-to-end*) ya que el atacante al controlar los dos extremos puede correlacionar las *IP* con las peticiones enviadas al servidor. Se pueden distinguir entre los de tiempo, estudiando los patrones de temporización, y los de tamaño, mediante el recuento de paquetes.

Y, respecto a los problemas indirectos que comprometen la privacidad de los usuarios, se destacan las vulnerabilidades explotables del propio navegador Tor al igual que ocurre con el resto de navegadores.

[18] Los ataques del “hombre en el medio” son una forma de interceptación y escucha de las comunicaciones, interrumpiendo la conexión cliente-servidor, los cuales creen estar en una conexión privada, desconociendo que están siendo vigilados. https://tails.boum.org/doc/about/warning/index.en.html

A pesar de que Tor proporcione el anonimato del usuario final a nivel de red, es decir, su dirección *IP*, no garantiza un cifrado de los datos de extremo a extremo. Por ello, el nodo de salida es considerado como el más débil debido a la exposición a la que se somete ya que la información no está cifrada, es decir, es el último que recibe los datos del usuario, retransmitiéndolo directamente a Internet y pudiendo ver lo que está enviando y recibiendo. Por tanto, es fácilmente rastreable. La implicación de los nodos de salida por los atacantes puede dañar la red ya que usan aplicaciones en las que las conexiones realizadas parecen surgir del *OR* de salida. Por tanto, el tráfico que sale en nombre del último nodo es lo que el protocolo y los datos de la aplicación han enviado (Dingledine et al., 2004). Por ello, se utiliza el protocolo *proxy SOCKS* (P2P Foundation Wiki, 2013).

El hecho de conectarse a Internet supone exponerse a ataques dirigidos a producir daño. Por una parte, se encuentran los ataques pasivos, aquellos en los que los atacantes observan o monitorean sin alterar la información. Aquello que se observa es la conexión que realiza mediante los patrones de tráfico y no el destino ni contenido del mismo. Se considera como problema básico para la privacidad que el destinatario del proceso de comunicación acceda a lo enviado mirando las cabeceras de los datos. De manera que pueden acceder tanto aquellos que se encuentran autorizados, como los no autorizados, como intermediarios (por ejemplo, los proveedores de servicios de Internet) como los no autorizados. Una forma simple sería situándose entre el emisor y el receptor del circuito. Y otras más robustas y eficaces serían vigilar a varias partes a la vez o también utilizar técnicas estadísticas creadas con el fin de seguir patrones de comunicación de los usuarios de la red (The Tor Project, n.d.). Dentro de estos, existe la posibilidad de que cuando se esté navegando por Tor un atacante pueda ver parte del tráfico de datos desde o hacia el cliente, bien cuando este entra en el primer nodo del circuito o bien si se ve la respuesta del servidor cuando entra al nodo de salida del circuito. Es decir, lo que se conoce como un ataque de correlación de extremo a extremo, ya explicado anteriormente. Para poder asociar el cliente con el sitio Web visitado el atacante debería de ver ambos extremos del circuito a la vez, al contrario se sigue conservando el anonimato(Dingledine et al., 2004; Hsu & Marinucci, 2013).

Por otra parte, los activos son aquellos en los que el atacante no solo captura el tráfico sino que también altera el flujo de los datos enviados, modificando parte de este o creando uno falso. El hecho de que Tor sea proporcionado como un servicio público favorece a ataques de denegación de servicio contra la red (*DoS*) (Gestal & Pérez,

2011)[19], dirigidos a colapsar el servicio de comunicación para que no se muestre la información. Por tanto, se está atacando contra la disponibilidad. Este es el primer grado de los ataques que se pueden sufrir ya que el servidor no ve alterado el resto de propiedades. Aunque el anonimato que otorgan los servicios ocultos protege frente los ataques *DoS* distribuidos (*DDoS*) ya que los atacantes han de atacar la red debido al desconocimiento de la dirección real del servidor. El uso de los servicios ocultos podría otorgar mayor seguridad resolviendo los problemas en relación a la supervisión del tráfico utilizando nodos de salida (Dingledine et al., 2004).

2.1.7. Recomendaciones de uso

En los casos en los que se busca una seguridad extrema, cabe tener en cuenta los siguientes aspectos.

Se recomienda la utilización de Tails debido a la cantidad de medidas de seguridad disponibles. Y en el caso de que no quisiera utilizarse se recomienda no usar Windows ya que las *cookies* del resto de navegadores podrían rastrearse y existe el peligro de ser identificado el usuario (Portal TIC, 2013).

También se sugiere la realización de pruebas para el aseguramiento del modo de funcionar del navegador y para ello hay sitios web que permiten realizarlo gratuitamente (Collective & Front Line Defenders, 2016).

Otro elemento a tener en cuenta es que el acceso se lleve a cabo desde una red pública y no desde el propio *router* (Alonso, Un informático en el lado del mal, 2013).

Si se parte de que Tor no es totalmente seguro se advierte la necesidad de utilizar otras medidas de seguridad que complementen esa carencia, tales como servidores *proxy*, *VPN* o cambiar la dirección *MAC*.

Otra sería la inactivación de herramientas del ordenador como son la cámara y el micrófono.

Por otra parte, como usuario medio, no buscando máxima seguridad, se recomienda tener en cuenta estos otros aspectos.

[19] Los ataques de Denegación de Servicio son ataques dirigidos a la obstaculización temporal del funcionamiento del servidor al que se accede.

Cuando se accede a lugares que requieran cumplimentar formularios no introducirse información relevante sobre su identidad, es decir, datos personales como el nombre ya que van a ser guardados y se corre el riesgo de la identificación del usuario (The Tor Project, n.d.). Por ello, es importante no utilizar cuentas personales en las aplicaciones (Facebook, Twitter, Instagram, Gmail, etc.). Ello se soluciona accediendo a las propias redes sociales y servidor de correo que dispone Tor[20].

Se recomienda el uso del navegador Tor Browser, explicado en el apartado posterior, ya que está configurado previamente para garantizar la privacidad y el anonimato que se busca con Tor, no protegiendo todas las aplicaciones sino solo aquellas que estén configuradas para el tráfico mediante Tor (The Tor Project, n.d.) .

El usuario debe asegurarse de que se estén utilizando sitios web *HTTPS* ya que es fundamental para garantizar el cifrado privado al sitio web desde el destino final. Ello es debido a que Tor garantiza el anonimato y encriptación hacia y dentro de la red pero no la del último nodo, no cifrando el tráfico. Esto le corresponde al propio sitio web, debiendo utilizarse encriptaciones y autenticaciones que protejan de extremo a extremo, puesto que si no se expone el tráfico a un nodo salida (Starke, 2016).

El propio navegador se encarga de boquear los *plugins*[21] del navegador (Flash, RealPlayer, etc.) ya que las empresas o los propios gobiernos podrían realizar un seguimiento de los usuarios si esos se mantuviesen activados. Pero, además, se recomienda no instalarse de adicionales o complementos puesto que permite conocer la fecha, hora como el lugar donde se ha accedido (López, 2015).

Es importante evitar abrir documentos que hayan sido descargados de Tor, estando en línea. Esta es la razón por la cual el propio navegador advierte acerca de que estos documentos al incluir recursos de Internet se abren mediante aplicaciones externas a Tor, exponiéndose a que la dirección *IP* del cliente sea conocida. Por ello si se ha de trabajar con documentos con formato PDF o Word se aconseja acceder creando una máquina virtual.

---

[20] http://www.linuxadictos.com/tor-browser-5-0-el-navegador-de-la-privacidad.html

[21] Es un programa o un conjunto de programas que se han diseñado para un determinado navegador, el cual permite una mejora de la conexión del usuario a Internet.

También es destacable el uso de puentes ya que ello evitaría que los atacantes pudieran conocer los sitios a los cuales se accede. De manera que se busca configurar Tor, no con un acceso directo al circuito de Tor sino conectándose mediante un nodo de puente[22].

Por otra parte, es importante consultar, a la hora de ejecutar un nodo de salida, la lista de proveedores de servicios de Internet proporcionada por la comunidad de Tor para reducir la probabilidad de sufrir ataques. En esta se encuentran las calificaciones a las respuestas dadas por estos con lo cual, en base a experiencias previas compartidas, se tiene información veraz si se quiere participar en la red Tor (como puente, relé o nodo de salida) (Çalışkan et al., 2015).

2.1.8. Sus usuarios (The Tor Project, n.d.)

El anonimato en el uso de Internet es atrayente para mucha variedad de personas (Watson, 2012).

Por una parte, cualquier ciudadano puede convertirse en usuario de Tor ya que buscan proteger su intimidad frente a los registros de los proveedores de servicios de Internet así como de los propios sitios web, buscan la protección de las comunicaciones realizadas mediante Internet, proteger a los hijos, sobre todo a los menores, cuando se encuentran conectados, el acceso a información sensible para su investigación, buscar evitar la censura a la que están sometidos en sus países y en definitiva, evitar ser correlacionada una identidad física con su identidad virtual.

Por otra parte, los periodistas utilizan dicha red para obtener información polémica que les permita obtener puntos de vistas distintos sobre las problemáticas existentes. Sobre todo, su uso radica en relación a regímenes represivos. Incluso también es utilizado por las fuerzas del orden ya que les posibilita vigilar los sitios web sin dejar constancia de ello, desarrollar operaciones encubiertas para investigar casos en línea así como un servicio de sugerencias de carácter anónimo (Çalışkan et al., 2015). También destacan activistas y denunciantes de los derechos humanos que aprovechan esta herramienta para denunciar internacionalmente hechos ocurridos en zonas de peligro, evitando la censura y protegiendo su navegación y comunicación de la vigilancia. También se utiliza en el ámbito de los negocios ya bien sea para garantizar la seguridad de sus empresas en los intercambios de información, para conocer datos sobre sus competidores o para conservar la confidencialidad de las

[22] https://www.torproject.org/download/download.html.en#warning

estrategias. Los militares también son usuarios sustanciales de la red puesto que esta les proporciona lo necesario para evitar el monitoreo al que se somete el tráfico en Internet, protegiendo las ubicaciones geográficas de los mismos, los servicios ocultos permiten la seguridad del comando y de los controles militares frente a posibles descubrimientos y sobre todo, les permite recabar información sobre y frente a los insurgentes. Y también son usuarios los propios profesionales de las Tecnologías de la Información. Esta les permite acceder a la hora de desempeñar sus funciones a recursos externos para resolver los problemas, es decir, les permite evitar los sistemas de seguridad de las empresas si así se requiere en su actividad profesional, conectarse remotamente a los servicios desplegados como parte de pruebas operativas o acceder a recursos online sin restricción, no alterando las políticas de seguridad.

Sin embargo, también es conocido como un refugio seguro para el ejercicio de la criminalidad. De manera que la actividad criminal allí desarrollada es muy heterogénea puesto que los cibercrímenes pueden ir desde fraudes (*phishing* o *spam*), *malware* (como virus informáticos), terrorismo, falsificación de tarjetas, compra-venta de droga, de armas, de munición,…hasta compraventa de personas, delincuencia relacionada con menores, destacando la pornografía infantil y la pedofilia, contratación de sicarios, de *hackers*, prostitución entre muchos otros. Por tanto, existe una amplia multiplicidad delictiva que permite apreciar como esta red es utilizada para ocultar acciones delictivas realizadas (Ciancaglini, Balduzzi, Goncharov, & Mcardle, 2013; Rudesill, Caverlee, & Sui, 2015).

De esta manera, se aprecia que el perfil del usuario de Tor es muy variado ya que acceden toda clase de ciudadanos, independientemente del perfil social que presenten. Además también se aprecia la amplia distribución geopolítica ya que acceden desde todas las partes del mundo, de unos 126 países distintos, siendo Alemania, China y los Estados Unidos sus principales clientes (Mccoy, Bauer, Grunwald, Kohno, & Sicker, 2008). Pero todos tienen elementos en común ya que con su uso buscan garantizar sus derechos a la privacidad, intimidad y libertad de expresión que de otra manera son menoscabados. El anonimato que les proporciona es la clave para convertirse en usuarios puesto que este es el medio a través del cual pueden llevar a cabo las acciones buscadas. Así, se aprecia como los delincuentes se aprovechan de esta plataforma para o bien realizar conductas que ya se hacían pero aprovechando el funcionamiento de Internet o bien realizar de nuevas.

2.2. Tor Browser

Tor Browser es el proyecto desarrollado para navegar en Tor. Este es una versión de Moxilla Firefox que está configurada previamente para el uso de Tor (Echeverri Montoya, 2016). Aunque está incluido en Tails como el navegador por defecto puede ser descargado para utilizarse independientemente en cualquier sistema operativo sin necesidad de descargar ningún *softwar*e adicional, comenzando a usar Tor rápidamente[23]. El diseño de este navegador para conseguir la privacidad buscada no garantiza la protección de los datos guardados en el disco duro o un *USB*. Por esta razón, el historial de navegación es eliminado en el momento que es desconectado del navegador (Tactical Technology Collective & Front Line Defenders, n.d.).

Es importante que el programa se mantenga actualizado respecto todas las novedades y mejoras realizadas. Por ello, el propio navegador notifica cuando las nuevas actualizaciones están disponibles, redireccionando a la página web del Proyecto Tor para su descarga. También es importante la habilitación del *add-on NoScript*[24](Figura 6), puesto que el navegador no lo activa por defecto requiriendo habilitarlo manualmente. Ello es debido a la protección de sitios web y de la desprotección de la identidad del usuario por ejecutar programas o *scripts* en el navegador (Tactical Technology Collective & Front Line Defenders, n.d.).

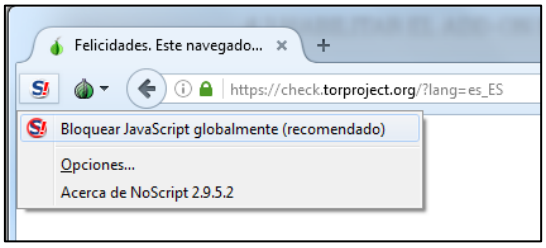

Figura 6. Se produce la activación del *NoScript* seleccionando la opción del menú para bloquear JavaScript globalmente, que es lo que se recomienda.

[23] http://www.linuxadictos.com/tor-browser-5-0-el-navegador-de-la-privacidad.html

[24] El *NoScript* es un complemento del navegador Moxilla que, mediante la creación de una lista blanca de sitios que considera aceptables, seguros o de confianza, permite la protección del equipo de sitios web inseguros. Para evitar que *NoScript* bloquee de forma automática el contenido que se necesita para que el sitio web funcione es el propio usuario el que ha de establecer las excepciones. Por ello, está la opción de permitir JavaScript de forma temporal para un sitio web en concreto, siendo fundamental no seleccionar que se permita globalmente el uso del JavaScript.

El archivo puede ser descargado y almacenado donde más convenga, pudiendo ser tanto en el escritorio, si se quiere descargar el paquete en el ordenador, como en una unidad flash *USB*, pudiéndolo mover de ordenador o evitar dejar rastro. Este permite que Tor sea utilizado tanto por Windows, habiendo dos versiones (32 y 64 bits), Mac OS X o Linux. Por ello, la propia página del proyecto Tor da las instrucciones a cerca de la instalación en cada caso (The Tor Project, n.d.).

2.2.1. Descarga del navegador Tor

El propio sitio web del Proyecto Tor establece las instrucciones para los diferentes *softwares* (Mac OS X, Linux y Windows). Se destaca Windows por ser el más conocido, y el utilizado para realizar dicho trabajo. En la propia dirección web de descarga directa del Tor Browser se clica y se guarda en el lugar seleccionado, se hace doble clic sobre él para ejecutarlo, se elige el idioma para el instalador y se acepta. Se da a instalar debiendo esperar unos minutos para que se complete la instalación y entonces darle a finalizar. Seguidamente, se accede al asistente y se clica en conectar, abriéndose Tor Browser de forma automática. Hay que tener en cuenta que los sitios web accedidos desde este a Tor no van a afectar a los otros navegadores web. Cuando ya se ha realizado la búsqueda para cerrar el navegador se deben cerrar todas las pestañas abiertas. Una vez ocurre esto se elimina el historial de páginas web y cualquier cookie unida a estas, evitándose así la posibilidad de rastreo (The Tor Project, n.d.).

2.3. Dominios .onion

Hay que tener en cuenta que la Internet Profunda, al ser una red alternativa, las páginas tendrán direcciones (*URL*) con formato distinto al habitual. Se les conoce como identificadores conformados por una combinación de 16 caracteres alfanuméricos incomprensibles derivados de la llave pública del servicio oculto. Este número se conformará con cualquier letra del alfabeto y partir de números decimales que empiecen por 2 y acaben por 7 por lo que se obtiene un número de 80 *bit* en base 32 (Castaño Apaza, 2014).Estas empiezan por *http* ya que siguen siendo una página web pero terminan con *.onion* (David et al., 2014). Es considerado como un dominio de nivel superior virtual (Dingledine et al., 2004) o un pseudo-dominio (Vicente Alarcón & Guillén Guillén, 2015), el cual muestra una dirección anónima a la cual se accede a través de Tor, a diferencia de los otros dominios de nivel superior como *.com* o *.org* a las que se puede acceder sin este (Castaño Apaza, 2014). El formato completo del mismo sería "*x.y.onion*", el cual si es desglosado se identifica la "x" como la cookie de

autorización y “y” se encarga de codificar el *hash* de la clave pública. Un ejemplo de dirección *.onion* podría ser “http://silkroad7rn2puhj.onion/”, que se correspondería con el servidor de la página *The Silk Road 3.0*.

Por tanto, estos sitios web tienen nombres de dominio registrados con una raíz diferente a la del Sistema de Nombres de Dominio (*DNS*) por lo que los nombres de los host se han introducido con un registrador alternativo al de la Corporación de Internet para Nombres y Números Asignados (*ICANN*) (Ciancaglini et al., 2013). Estas raíces de dominio alternativa son las llamadas *TLDs rogue* ya que hace referencia al conjunto de redes que utilizan entidades *DNS* no controladas por la *ICANN*. A pesar de no ser *DNS*, es posible acceder a través de los buscadores web mediante el uso de un proxy web y solicitándolo a través de Tor.

La principal finalidad de este sistema es garantizar la irrastreabilidad, a diferencia de lo ocurre en la Surface Web, ya que en esta se realizan fácilmente seguimientos y se pueden trazar las rutas seguidas por los usuarios.

3. Tor y Deep Web

En dicho apartado se profundizará en la intrínseca relación de la red Tor con la Deep Web.

3.1. ¿Qué es la Deep Web? (Echeverri Montoya, 2016)

3.1.1. Definición

La Deep Web o Invisible Web es la Internet Profunda o Internet Invisible. Por tanto, es la contraposición de la Internet Visible a la que se accede y es conocida por todos. Es aquella parte de la red en la que su contenido no está indexado ni rastreado, no pudiendo recuperarse mediante los motores de búsqueda tradicionales.

Y es destacable dentro de esta, el crecimiento de la llamada Darknet o Internet oscura que hace referencia a la parte de la web que no se tiene acceso con herramientas ordinarias ya que para acceder son necesarios programas específicos. Aunque se suela considerar parte de la Internet profunda estrictamente no es así debido a que existe la posibilidad de que parte del contenido sí pueda estar indexado. Tal como se aprecia con la red Tor, pudiendo acceder a contenido de la Internet visible pero concediendo ese anonimato buscado por el usuario. Pero, además, se enrutan peticiones para acceder a servicios alojados directamente dentro de la propia red, constituyendo la web profunda de Tor. Los ya explicados anteriormente como servicios ocultos.

Pero hay que tener en cuenta que una web no esté indexada no quiere decir esté en la Deep Web (Vicente Alarcón & Guillén Guillén, 2015). Por ejemplo, se conoce que ciertas bases de datos públicas (como la Biblioteca del Congreso de los Estados Unidos, Web of Science, FindLaw, etc.) pero también privadas/de pago que requieren de suscripción (como WestLaw o LexisNexis) pueden llegar a considerarse como parte de esta debido a que contenido de las mismas no está indexado y no se puede rastrear con los buscadores tradicionales. Sin embargo, se accede desde la Internet visible con los motores de búsqueda regulares.

La Deep Web se suele representar de forma gráfica como un iceberg, tal como se puede apreciar en la Figura 7 (Deep Web Proyecto, 2015). Ello es debido a que con la Internet Visible solo tenemos acceso a una pequeña porción de datos respecto de la inmensa totalidad que se encuentran en el ciberespacio. Los estudios concluyen que está conforma el 80-90 % de Internet, es decir, es unas 400-500 veces mayor que la web superficial. Y que, por ejemplo, en comparación con Google, que es el mayor

motor de búsqueda existente, esté solo tiene indexada el 4-16% de la superficie, es decir, solo tienen disponible en la red de un tercio a la mitad de los documentos (Perojo & León, 2006).

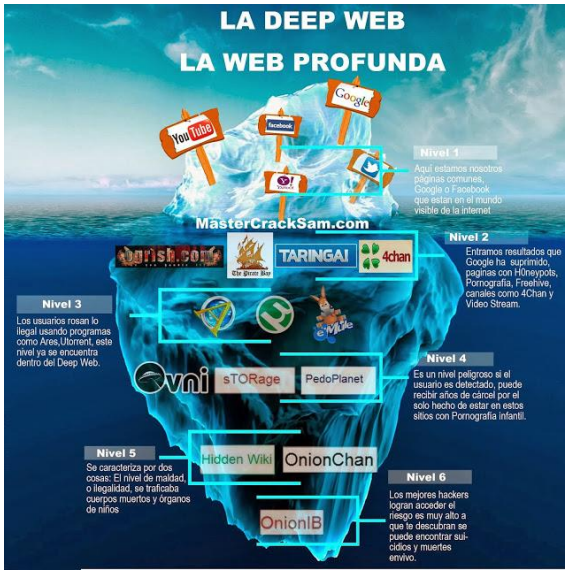

Figura 7. Imagen que representa la Deep Web con sus distintos niveles.

Para acceder a parte de la web se utiliza, mayoritariamente, el navegador Tor Browser de Tor. Ello es debido fundamentalmente al anonimato del usuario, ocultando su dirección *IP* y manteniendo íntegramente el mensaje transmitido. Una vez descargado e instalado, para saber si realmente se está dentro y se ha superado el proceso de acceso con éxito se puede comprobar de varias formas. Por una parte, se puede hacer entrando a una página web que revela cuál es la ubicación e *IP* del ordenador (como puede ser “http://whatismyipaddress.com/”) (Vicente Alarcón & Guillén Guillén, 2015). Así, se observa, a continuación, la comparativa entre ambas informaciones obtenidas en las figuras 8 y 9.

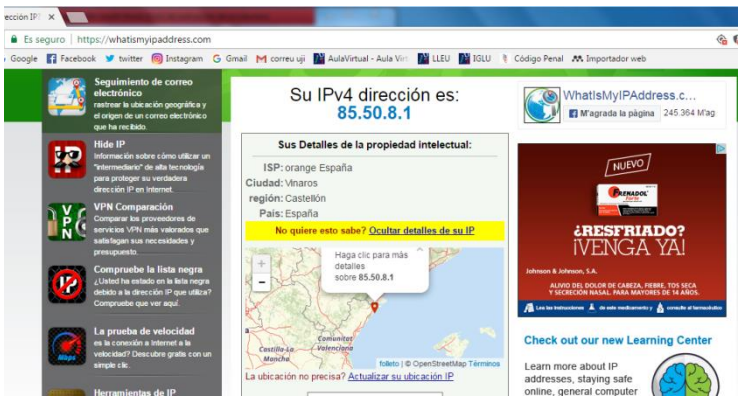

Figura 8. Se muestra la *IP* del ordenador desde el cual se accede.

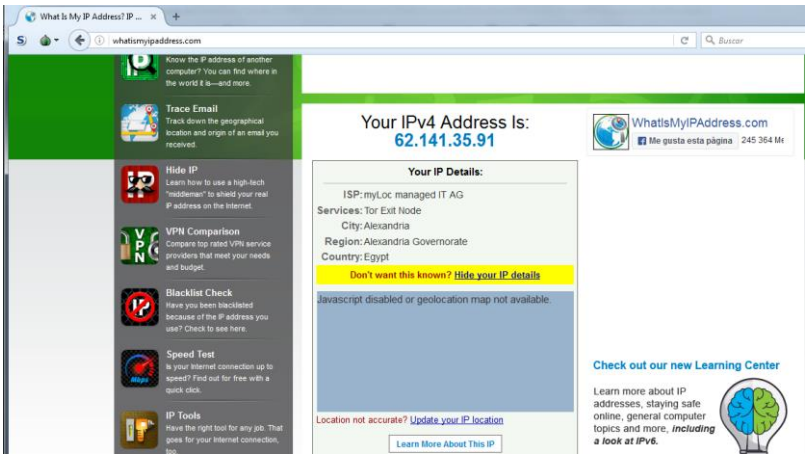

Figura 9. Se representa la *IP* correspondiente con el ordenador que actúa a modo de nodo de salida en el circuito de Tor creado.

Por otra, también se puede comprobar accediendo al enlace directo del Proyecto Tor ("https://check.torproject.org"). Este nos informará, tal y como se muestra a continuación en la Figura 10, si la conexión ha sido exitosa o no.

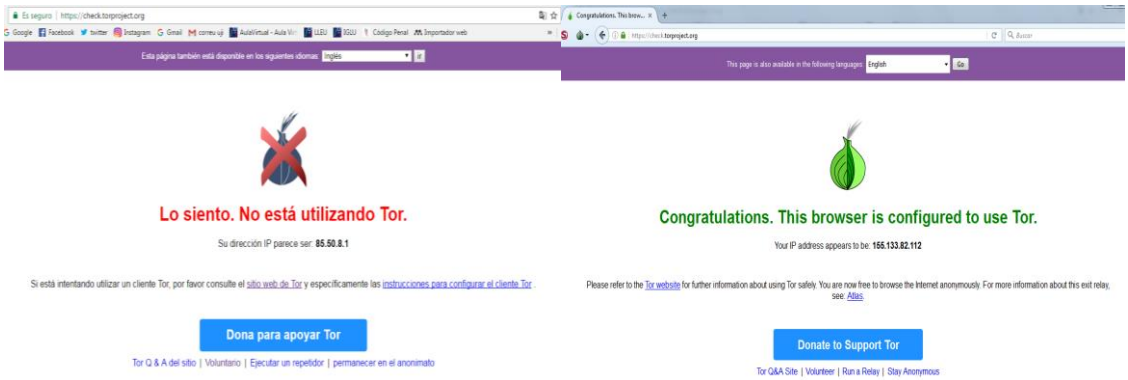

Figura 10. Diferente representación gráfica según si se está conectada o no a Tor.

Cualquier transacción llevada a cabo requerirá del uso de monedas virtuales o electrónicas ya que los métodos de carácter tradicional no tienen cabida para realizar transacciones en la Deep Web (Vicente Alarcón & Guillén Guillén, 2015). Estas serán explicadas posteriormente en el apartado 3.2.

3.1.2. Niveles ("Tor y Deep web: los secretos del lado oscuro de la web," 2016)

La figura 7 es una representación gráfica de los niveles en los que se puede dividir la Deep Web. Esta división es realizada a efectos de entendimiento de la parte oculta y menos conocida de la web, es decir, es una clasificación que tiene la finalidad de mostrar los diferentes aspectos que pueden ser encontrados a medida que se profundiza en la web.

El primer nivel o también llamado Surface Web se corresponde con la parte de la red a la que se accede desde los buscadores tradicionales. Por tanto, es la conformada por la Internet visible, aquella que está indexada y fácilmente rastreable.

El segundo nivel ya supone estar por debajo de la superficie. Se considera que a este acceden quienes tienen la edad determinada para poder entrar al contenido de las páginas incluidas en él. Aquí, la información ya no se encuentra indexada, no siendo, por tanto, ni visible ni rastreada por los motores de búsqueda tradicionales.

El tercer nivel ya se conoce propiamente como la Deep Web. Y en este, ya se empieza a encontrar parte del contenido que roza la ilegalidad. Aquí, ya se requiere de un *proxy* específico poder sumergirse, es decir, navegar por dicha parte de la web.

El cuarto nivel es considerado como el nivel más profundo conocido dentro de la Deep Web al que comúnmente un usuario puede acceder. Esta es la parte más profunda de este nivel, un lugar al cual solo se puede llegar mediante modificaciones del hardware y no ya por medios usualmente conocidos. Aquí, la mayoría de contenido se considera ilegal.

Se entiende que una vez superados estos primeros cuatro niveles se procede el acercamiento a la base del iceberg que se correspondería con la, ya explicada, Darknet o Internet oscura. Tal y como se ha matizado, es a partir de aquí donde se encuentra la mayoría del contenido de la web. Se dice que en este es donde están los sitios a los que únicamente se puede acceder a través de un *software* especial como es Tor. Se estaría en el definido como un quinto nivel.

A partir de aquí, se puede hablar del Mariana's Web, como símil al nombre de la fosa más profunda del mundo. Ello es consecuencia del desconocimiento de la verdadera profundidad y contenido de este nivel. Se puede identificar como el mundo de los hackers, en el que solo se conoce la existencia de redes de carácter privado con acceso restringido, en el que no existe ningún tipo de norma ni seguridad.

De esta manera, no existe conocimiento sobre el contenido o material específico que se pudiera encontrar ya que solo los considerados más privilegiados tienen acceso a este. Es el punto de la red que muchos desconocen e incluso no han oído mencionar. Por dicha razón, se presume que toda actividad realizada en este abismo se corresponde con la criminalidad más gravemente repudiada ya que los niveles de seguridad desarrollados sobrepasan los necesarios para garantizar el anonimato buscado.

3.1.3. Buscadores

Tal y como se ha especificado anteriormente, la Deep Web no utiliza los buscadores tradicionales por lo que ha desarrollado sus propios tipos de buscador, específicamente diseñados para la red Tor. Entre estos, destaca especialmente el llamado Torch, TorSearch, Duck Go o Grams (se considera el Google de la Deep Web) (Echeverri Montoya, 2016), entre otros (Rudesill et al., 2015).

Pero más que propiamente buscadores, destacan las conocidas como *wikis* que se utilizan como directorios específicos a partir de los cuales conocemos los servicios que se ocultan en la red Tor. The Hidden Wiki es la principal ya que esta recoge una lista con una amplia clasificación de los servicios ocultos con sus correspondientes direcciones. Pero hay que tener en cuenta que, con el fin de garantizar esa privacidad buscada, los enlaces van variando de pseudo-dominio, teniendo que revisarse continuamente para garantizar su actualización. Aunque también hay que recordar que se puede acceder a esta *wiki* desde el propio Google. Además también se encuentran otras páginas que sin ser consideradas como *wikis* presentan listados de enlaces .*onion* actualizadas (Echeverri Montoya, 2016).

De esta forma, los grupos de esta lista se clasifican en diversos servicios a los que se puede acceder. Incluso también se hace especificación dependiendo del idioma en el que se encuentran. Además, cabe matizar que a algunos de estos es a los que se ha accedido para la realización del posterior apartado 5 de este trabajo (Vicente Alarcón & Guillén Guillén, 2015).

Por otra parte, incluso existe la posibilidad que, ante el desconocimiento de la terminología utilizada en esta red, puedas acceder a una especie de diccionarios en los que se definen y explican los principales términos que uno se va a encontrar navegando en ella (un ejemplo puede ser "https://www.deepdotweb.com/2014/03/02/deepdotwebs-darknet-dictionary/").

3.2. Moneda electrónica (Bitcoin Wiki, 2015)

Existen una gran variedad de criptomonedas o monedas virtuales que se utilizan para hacer transacciones en la red, destacando específicamente los *bitcoins* por su mayor popularidad. Por ejemplo, en la web "http://coinmarketcap.com/" se puede encontrar una lista completa de todas ellas, siendo la primera el *bitcoin*.

Su gran uso la ha convertido en la considerada como moneda de curso legal en la Deep Web. Dentro de esta, se encuentran servicios de intercambio de divisas para poder conseguir *bitcoins* a partir de la moneda propia del país del solicitante.

Pero el hecho de utilizar este tipo de moneda no garantiza que no se pueda rastrear las acciones realizadas. Ello es debido a que, a pesar de la dirección a la que se recibe la transferencia es anónima, las transacciones se mantienen públicamente.

4. Aspectos legales

4.1. Legislación

Debido a que Tor ha sido considerado como refugio de la criminalidad se concibe como una importante amenaza para los gobiernos a nivel internacional. Por ello, la regulación legal en esta materia determinará las posiciones ocupadas por los gobiernos en base a Internet, el uso y derecho a la privacidad así como lo relacionado con el proceso criminal (Watson, 2012).

Desde esta perspectiva, se aprecia la tensa relación entre Tor y algunos gobiernos ya que, el hecho de que del anonimato garantizado se beneficien también para la comisión de delitos, aumentan los problemas existentes en relación al creciente y masivo uso del ciberespacio (Cervantes & Tauste, 2015). A pesar de que, en algunos países, los propios gobiernos apoyan dicha red, aportando incluso sugerencias de aspectos a desarrollar, siendo lo destacable es la contribución financiera realizada (Çalışkan et al., 2015). Además, hay que especificar un elemento esencial que supone un plus de dificultad a una actuación y regulación conjunta en la materia, la falta de formación de todos los agentes y personal en materia tecnológica. El desconocimiento (o escaso) de los elementos básicos de las amenazas contra las que actúan determina la existencia de firmes barreras para la actuación efectiva. La lucha en Ia red requiere del uso de los propios medios usados en Internet al cometer los delitos para investigarlos y perseguirlos (MG, 2011). De ahí, radica la importancia y genialidad de los países que usan la propia red Tor para la investigación de la cibercriminalidad y aplicación de la ley (Starke, 2016), aunque destacando la falta de regulación y habiendo de establecer los límites legales para no acabar vulnerando derechos.

Por ejemplo, destaca que países, como Holanda, Bélgica, Alemania, Noruega y Estados Unidos, hayan posibilitado charlas de formación en Tor a sus policías, destacando, en especial, el FBI (Europol, 2017) e incluso, alguno de estos, haya reconocido la utilización de Tor. De manera que se concibe como un medio a través del cual se aplica la ley a nivel nacional para la realización de las investigaciones criminales. Primordialmente se destacan tres actividades (Çalışkan et al., 2015). Por un lado, se destaca la vigilancia online, es decir, posibilita la navegación de los funcionarios por sitios web y servicios no dejando rastro, evitando así la obstaculización de la investigación. Por otra parte, destacan las llamadas *Sting operations*, es decir, operaciones de picadura, las cuales consiste en, aprovechando el anonimato, los oficiales de la ley desarrollan operaciones encubiertas. Y por último, se

encuentran las líneas de sugerencia anónimas ya que, a pesar de su ya existencia, la ocultación de la identidad favorece a su eficacia, garantizando el acceso y uso de dichos sitios web por usuarios que temen su identificación.

La simultaneidad de aplicación de la ley y uso de Tor supone cuestionarse qué límites se encuentran desde el ámbito legal al utilizarse para recabar información, reunir evidencias así como en considerar los datos subidos a la red Tor como información disponible públicamente (MG, 2011). Esas limitaciones referidas, al estar previstas en cada legislación nacional, presenta variaciones entre los países. En especial, destaca en la recopilación de pruebas ya que al ser de carácter digital suponen importantes retos desde el punto de vista procesal. En relación a ello, algunos sistemas jurídicos pueden cuestionar su fiabilidad y viabilidad ante los tribunales de justicia, en base a la posibilidad de considerarse una fuente para la Inteligencia de Código abierto como cualquier otra. También se estudia el tratamiento que reciben los datos de carácter personal, que se encuentran en las bases de datos que forman parte de sus servicios ocultos.

De manera que se parte de considerar a Tor como una herramienta que garantiza la libertad virtual y permite eludir la censura y restricciones impuestas en el ámbito electrónico. Por tanto, hay que destacar la importancia de la privacidad ya que es reconocido como derecho fundamental tanto en la Declaración Universal de los Derechos Humanos como en los Código Penales y legislaciones nacionales. Por su relevancia, se pretende protegerla y garantizarla en el entorno cibernético a través del desarrollo de herramientas como Tor (Watson, 2012). Esto es debido a que se considera que desde los propios gobiernos se pretende anteponer el orden público y seguridad colectiva a cualquier conducta que consideren amenaza. Por tanto, este conflicto entre libertad virtual y seguridad requiere del desarrollo de medidas y herramientas que, frente a las represiones y restricciones impuestas, garanticen el ejercicio de un derecho fundamental. La sociedad demanda mayor libertad y privacidad ya que el nivel de control ejercido supera los límites de lo que se considera necesario para garantizar la seguridad buscada. Como consecuencia de las continuas regulaciones y leyes dirigidas a la creciente sanción de conductas y limitación de derechos, ciertos sectores y miembros de la sociedad deciden acudir a estas medidas específicamente diseñadas para conseguir el anonimato (Alonso, 2016).

4.2. Problemática legal

El derecho internacional en el ámbito tecnológico-informático juega un papel fundamental en este escenario. En dicho contexto, cuando un Estado interviene los servidores situados en el extranjero necesita de un consentimiento concedido por ese Estado extranjero o de otros motivos de acuerdo a la normativa internacional (Alonso, 2016). Aquí, es donde aparece y destaca la problemática de la jurisdicción, relacionada con todo lo referido a Internet y las nuevas tecnologías. La capacidad de superar cualquier frontera física y llegar a todas partes del mundo tiene esta grave consecuencia ya que su omnipresencia se traduce en importantes problemas de carácter legal dificultando su regulación y penalidad (dificultad probatoria) (Machín & Gazapo, 2016).

También destaca el hecho de que se hayan retenido servidores cuyos usuarios son personas no relacionadas con la investigación en curso (Alonso, 2016). De manera, que habría una clara vulneración del derecho a la libertad que podría ser llamada virtual, en cuanto a acceder libremente a donde el usuario quiera sin que se le restrinjan accesos ni se les intente acusar de poseer servidores unidos con la actividad criminal.

Se dice que el castigo depende de la legislación del Estado en el territorio del cual se encuentran dichos servidores investigados (Alonso, 2016). De manera que se estaría haciendo referencia al principio de la territorialidad, el cual con el mundo virtual parece desvirtuarse ya que la realización de las conductas a distancia trasciende de cualquier territorio físico, pudiendo iniciarse, realizarse y consumirse en lugares totalmente diferentes. Esto plantea disparidad de criterios por parte de la doctrina y soluciones dispares ante este fenómeno complejo (Fernández Teruelo, 2011). Por tanto, se está hablando del desconocimiento de dónde y quién comete los delitos por lo cual supone no poder actuar en su contra. Por ello, se entiende que no se puede conocer el ámbito de actuación en base a la jurisdicción sobre el territorio donde se tiene competencia, mientras no se conozca el lugar donde están los servidores físicos que garantizan el funcionamiento de estas webs. Es aquí donde se aplicaría la legislación estatal correspondiente.

Por otra parte, es interesante destacar si el usuario, a efectos legales, puede ser castigado en España por el uso de mecanismos de cifrado en las comunicaciones mantenidas en la red. La diversa legislación nacional sí permite el uso de del cifrado en la navegación. Partiendo de la propia Constitución Española, una interpretación amplia de su art. 18.3 garantiza el secreto de las comunicaciones puesto que se

entiende, en relación al art. 24.2 de la misma, que la existencia de una ley que limitara el uso del cifrado confrontaría con el derecho a no declarar contra uno mismo ya que supondría una especie de obligación de revelar los medios que utiliza el usuario. Ello se refuerza con el art.36.1 de la Ley 32/2003, de 3 de noviembre, General de telecomunicaciones, conocido comúnmente como LGT, cualquier tipo de información transmitida mediante redes de comunicaciones de carácter electrónico pueden protegerse a través de los procedimientos de cifrado (Maeztu, Del derecho y las normas, 2013).

Pero, supuesto distinto y donde se presentan complicaciones a nivel legal sería en relación a la instalación y administración de un nodo Tor (Cervantes & Tauste, 2015)[25]. Respecto a este supuesto cabe destacar la definición dada desde el punto de vista jurídico (tanto la LGT como el Real Decreto 899/2009) como un operador, cuya definición se prevé en los mismos y se entiende que los nodos caben dentro de esta categoría de operador al tener el ordenador encendido y estar haciendo la función de enrutar el tráfico. De esta manera, las personas que administran públicamente un nodo se les considera como operadores, aplicándoles, en principio, la obligaciones previstas en cuanto a estos (Maeztu, 2013).

En relación a los datos personales, anteriormente mencionados, cabe destacar que al no garantizarse de manera absoluta y completa el anonimato, cuando se llevan a cabo las investigaciones se accedan a datos personales los cuales son innecesarios para las mismas. Por ello, estas investigaciones podrán estar limitadas por las legislaciones en materia de tratamiento de los datos de carácter personal. Se apreció un cambio de tendencia en el ámbito europeo ya que la aplicación de Tor para las investigaciones también requiere de la aplicación de los requisitos y recursos legalmente establecidos por el Reglamento de Protección de Datos. Es decir, las actividades dirigidas a aplicar la ley tampoco se les eximirá de someterse a la normativa de protección de datos que rige en la UE. Se incluyen diversas propuestas en relación a la protección de las personas en cuanto al tratamiento de los datos de carácter personal por parte de las autoridades en el ámbito del procedimiento penal. Con estas se pretendía conseguir armonía entre la diferente normativa que regulaba dicha materia en el ámbito europeo. La propuesta de Directiva sobre protección de las personas en relación al tratamiento de los datos personales se convirtió en el instrumental fundamental para su regulación. Pero, aplicado a la práctica en relación

[25] El acceso a Tor no es ilegal, a pesar de que sí se hayan de tener precauciones previstas anteriormente.

con Tor, muchas veces se encuentra la dificultad de discernir la parte de los datos de dicha red que han de ser considerados como de carácter personal. Unido a ello está la problemática de la variada definición existente acerca de qué datos son de carácter personal frente a los que no en el ámbito europeo (Dir. 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016).

En el ámbito nacional, destaca la Ley Orgánica de Protección de Datos que regula dicha materia en el estado español y el mecanismo utilizado para garantizar su adecuada aplicación y funcionamiento es la Agencia Española de Protección de Datos (Agencia Española de Protección de Datos, n.d.). Tal y como reconoce parte de la doctrina, en base a sentencias dictadas por los tribunales, en el estado español se consideran las direcciones IP como datos de carácter personal. Al ser reconocidas como tales, han de protegerse aplicando las garantías previstas para su tratamiento en el texto legal. Por tanto, se aprecia lo especificado anteriormente en cuanto a las limitaciones que supone la aplicación de Tor para la investigación, puesto que en las actuaciones de las autoridades se puede producir el descubrimiento de datos personales como es la *IP* de personas que no tienen que ver con ninguna pesquisa policial produciendo la vulneración de su privacidad (Noticias Jurídicas, 2014).

Estos son algunos ejemplos a nivel legislativo en el ámbito estatal, europeo y como también a nivel internacional Tor supone un problema que trasciende los retos usuales y requiere de una mayor armonización para conseguir el propósito. La dificultad de su regulación siempre va a existir debido a que todos aquellos delitos informáticos que se producen en la red presentan múltiples dificultades (desconocimiento del impacto y alcance producido, imposibilidad de tipificar conductas que surgen continuamente, dificultad en la obtención de pruebas, falta de formación de las autoridades competentes, problema jurisdiccional) (Rudesill et al., 2015). Por tanto, se plantea como un importante reto a asumir desde las distintas jurisdicciones, requiriendo una verdadera cooperación internacional para la lucha conjunta contra la cibercriminalidad en Tor (Ministerio de Interior, 2013).

5. *Aproximación práctica a la red Tor*

Como bien ya se ha dicho, la red Tor puede ser usada no solo para la protección de las personas sino también para perjudicarlas ya que el anonimato proporcionado supone una plataforma segura para la cibercriminalidad.

Este uso intrusivo incluye un amplio catálogo de conductas. A continuación, se van a mostrar algunas de estas que han sido halladas a partir de una inmersión práctica como usuario/cliente en la red Tor.

Por una parte, destacan conductas consistentes en actividades comerciales, en especial mercados ilegales e intercambio de objetos o elementos entre los cibercriminales. Este comercio anónimo se diferencia en dos categorías, por una parte, aquella en la que las clasificaciones son genéricas pudiendo encontrar cualquier producto, sería como un símil de un supermercado (un ejemplo se aprecia en la Figura 11), o bien aquellos que van específicamente destinados a determinados sectores (drogas, armas, pasaportes, etc.). Un ejemplo de estos últimos se puede apreciar en las Figuras 12, 13 y 14. Un aspecto relevante a destacar es el hecho de poder hacer perfiles de mercado en relación a las transacciones llevadas a cabo ya que se puede recabar toda la información realizando perfiles individuales sobre los vendedores, usuarios así como los bienes que se hayan intercambiado (Watson, 2012). Es decir, se permite hacer una especie de estadísticas de las páginas.

Figura 11. Venta de amplia tipología de documentos falsos.

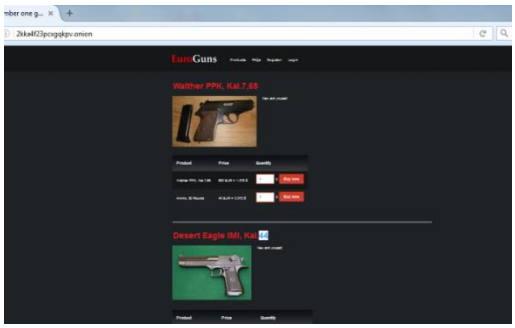

Figura 12. Venta de armas.

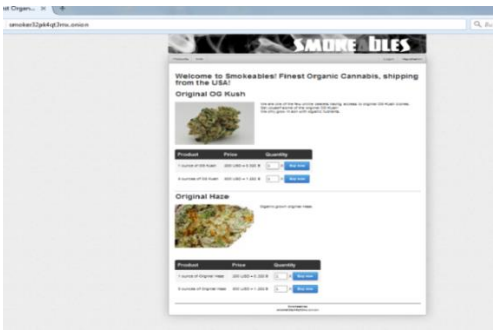

Figura 13. Venta de droga.

de que Navegador Tor tiene permiso para acceder a la web.

Figura 14. Venta de pasaportes falsos.

Por otra parte, se ofrece un amplio catálogo de servicios a contratar. Entre estos se destacan la posibilidad de contratar un *hitman*, es decir, un asesino a sueldo o sicario. Ello se puede apreciar en la Figura 15. Además, cabe resaltar que las páginas que ofrecen este servicio establecen los precios según la forma de matar y según quién sea la víctima existiendo así una catalogación de precios. Otro servicio a destacar también es el de contratar hackers, lo cual también se aprecia en la Figura 15, además de en la Figura 16.

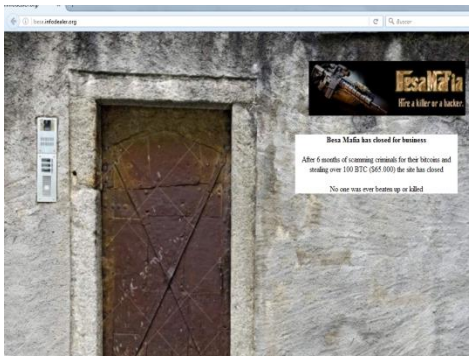

Figura 15. Se ofrece servicio de *hitman*.

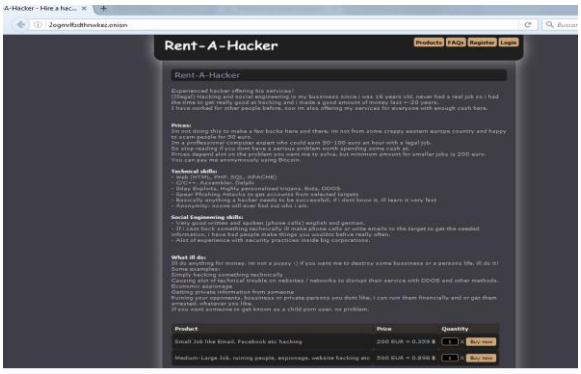

Figura 16. Se ofrece servicio de hacker.

Otras conductas a desarrollar, ampliamente reprochadas por muchos usuarios de la propia red Tor, son aquellas que están relacionadas con menores. En este ámbito, se entra en aspectos particularmente graves e imágenes duras que producen grave afectación no solo a nivel social sino a nivel individual por las víctimas de las mismas. Hay que tener en cuenta que cuando se rastrea en la red la descarga de determinado material ilegal, como la pornografía infantil, supone un delito ya que su mera posesión es ilegal. Ello es debido a que, a diferencia de otros delitos, aquí se tiene en cuenta no solo la descarga sino lo que se descarga, es decir, el contenido. Por esta razón,

también supone un plus de peligrosidad ya que, en su mayoría, las páginas para acceder al contenido requieren su descarga. Un ejemplo de estos servidores que ofrecen dicho material puede ser el que se aprecia en las Figuras 17.

Figura 17. Servidor que ofrece este material.

En relación a este ámbito, es destacable también un servidor que se encarga de establecer listas de direcciones *IP* correspondientes con personas que son clientes de este tipo de material. De manera que ofrecen un servicio totalmente legítimo dirigido a actuar en contra de la pedofilia e, incluso, para ello también se nutren de donaciones para seguir con su lucha.

Aunque se pueda encontrar material de este tipo, hay que especificar que es de los más complicados de acceder puesto que está especialmente protegido por sus propios usuarios. Para ello, se encargan de crear redes pequeñas y privadas montadas en los servidores, estando restringida la entrada y acceso si no perteneces a ese grupo privilegiado. Ello dificulta enormemente poder encontrar material accesible ya que se esfuerzan inmensamente en cubrir sus acciones para que no haya ningún tipo de error o *bug* que permita descubrirles. Sobre todo, teniendo en cuenta la existencia de estos grupos explicados que se encargan de identificarles para acabar con sus reputaciones online. Aun así, una investigación y búsqueda profundizada puede permitir el acceso a alguna pequeña parte del material.

Esta es una visión general a cerca de lo que se puede encontrar en la *Deep Web* a través de Tor. Por ello, hay que matizar que constituye una mínima parte de todo el material disponible, al cual se puede acceder con una menor o mayor facilidad, dependiendo de los medios usados, tiempo invertido e investigación realizada. Además, cabe como posible línea de investigación futura realizar dicha aproximación práctica, en lugar de como usuario, como servidor pudiendo valorarse ambas perspectivas posibles con las que se puede participar en la red Tor.

6. Conclusiones

Finalmente, una vez realizada toda la recopilación de información sobre Tor y realizada una investigación específica sobre esta red, se llega a una serie de conclusiones:

PRIMERA: La red Tor es un servicio específico que fue desarrollado, inicialmente, por el gobierno estadounidense y, posteriormente, por una organización, que se encarga de su supervivencia y funcionamiento (Proyecto Tor). El principal propósito a cumplir es la garantía del anonimato de todos quienes navegan en dicha red, tanto usuarios como servidores. Para ello, crea un circuito técnicamente complejo conformado, básicamente, por tres nodos que permiten saltar la información del usuario al servidor. A pesar de dicho funcionamiento, el circuito no está exento de ataques provocados por otros usuarios. Por esto, se concluye que no concede anonimato al cien por cien.

SEGUNDA: La importancia de la red Tor en la Deep Web, es decir, la Internet profunda y, en específico, en la Darknet. Grandes compañías, como Google, considerado el principal motor de búsqueda utilizado, tienen indexado el contenido de la Internet visible, lo cual provoca la posibilidad de conocer todos los hábitos de conexión y comportamientos realizados en la red. Ante esto, la sociedad demanda una menor intrusión en sus acciones, en defensa de sus derechos, en especial, a la privacidad y a la libertad virtual. Esta es la razón por la cual va en aumento el uso de la red Tor, ya que no solo permite acceder a la parte de la Internet profunda desconocida, sino que permite acceder a la Internet visible pero de forma anónima. Los servidores ocultos, cuyas direcciones no se corresponden con las *URL* usualmente utilizadas sino que finalizan con el formato *.onion*, son la parte a la cual se accede única y exclusivamente a través de Tor. Ello puede suponer un plus de dificultad por no tener buscadores propiamente conocidos, lo que conlleva una mayor implicación de búsqueda del contenido. Pero, esto se considera compensado gracias al elevado nivel de material que se puede encontrar, que no es ilimitado.

TERCERA: Hay que recalcar que, si bien es cierto que garantiza ese anonimato buscado por los usuarios para eludir las intromisiones en sus derechos, restricciones y prohibiciones (en algunos países del mundo), la red Tor tampoco puede quedar impune. Esto plantea la necesidad de hacer una valoración sobre el impacto que produce el uso de Tor porque, más allá de la defensa de los derechos de los usuarios, se cometen conductas delictivas que, a su vez, son de las consideradas más graves y,

por ello, las más duramente penadas. Por tanto, el mundo de la cibercriminalidad se expande todavía más, si cabe, gracias a la existencia de estos sistemas específicos que garantizan el anonimato en el acceso a Internet y, dentro de éste, a contenido de todo tipo. En consecuencia, este mundo virtual se encuentra conformado por un comercio ampliamente extendido, ofreciendo cualquier tipo de producto, elemento o servicio deseado. En efecto, se está haciendo referencia a un amplio comercio virtual que funciona según su propia economía con el uso de las monedas virtuales, en especial, el bitcoin, Además, en este, es fácilmente factible el intercambio de dinero físico por moneda virtual para garantizar las transacciones usuario-servidor. Por consiguiente, se aprecia que en busca de libertad virtual, se favorece, en parte, la impunidad de los cibercriminales al dotarles de herramientas que eluden la posibilidad de investigación y el descubrimiento de sus identidades.

CUARTA: La existencia de una importante problemática legal en la materia. Ello parte de que si ya existen amplias dificultades en conocer y tipificar los delitos informáticos, en especial los que se realizan en Internet, principalmente por el problema de jurisdicción, aún es mayor cuando se habla de la red Tor y la Deep Web. El uso de este tipo de herramientas dificulta conocer el origen y destino de las conductas así como sus consecuencias, por lo cual hace casi imposible poder investigarlas y perseguirlas. Desde los diferentes niveles, internacional, europeo y nacional, se pretende dar solución a todo lo relacionado con Internet para tener, en mayor o menor medida, cierta cobertura legal ante las actuaciones y no garantizar total impunidad de los actos. Hecha la observación anterior, se aprecia un preocupante vacío legal. Así mismo, el desconocimiento y falta de formación, en especial, de los propios miembros de las autoridades competentes en el ámbito de la investigación, persecución y, en su caso, procedimiento penal, no hace más que complicar el asunto. Como consecuencia de esto, se aboga por distintas medidas. Por un lado, se destaca la formación a las autoridades competentes en este ámbito, ya que no se puede luchar contra algo si se desconoce. Y, por otro lado, surge la necesidad de utilizar la propia red Tor para cumplir con sus funciones, puesto que, si algo es destacable en el mundo de Internet es que para responder ante los ataques cibernéticos, se requiere utilizar los propios medios usados por los cibercriminales. En este ámbito, es donde aparece otro problema en relación con la negativa de los gobiernos a participar en una red contra la cual están luchando. Por esta razón, se plantea necesariamente un cambio de concepción y abrir la puerta a los propios medios que proporciona el mundo cibernético.

En definitiva, se aprecia la imprescindible actuación conjunta de la sociedad, gobiernos e Internet para poder afrontar los retos que suponen el uso de la red Tor por los cibercriminales. Pero, eso sí, sin mermar ni limitar los derechos de los usuarios que les son reconocidos por la diversa normativa tanto internacional, europea como nacional. De manera que dicha cooperación ha de garantizar un uso libre de Internet pero no impune ya que la red Tor es una herramienta creada, principalmente, como símbolo de libertad virtual, que no ha de ser desprestigiada.

Como conclusiones finales, a nivel personal, se considera imprescindible tener conocimiento de la existencia y funcionamiento de una herramienta como es Tor. En un mundo totalmente globalizado en el que las nuevas tecnologías (TIC) han irrumpido en todos los ámbitos posibles hasta el momento, hay que incidir en su uso como factor estratégico de la investigación criminológica en el mundo virtual. Por tanto, implica hacer uso y aprovechar el potencial de la red Tor para actuar desde el propio núcleo de acción delictiva. No hay que olvidar que la Deep Web supone una efectiva oportunidad cibercriminal, es decir, facilita la comisión de delitos en el mundo cibernético, con todas las consecuencias problemáticas que ello conlleva. De esta manera, todas ellas se consideran razones para abogar no solo por una actuación reactiva, sino fundamentalmente una actuación proactiva. Esto supone la necesaria intervención de la prevención, siendo esta la herramienta esencial de la que se dota la Criminología para estudiar las causas y factores de riesgo, es decir, adoptar todas las medidas necesarias para reducir los factores criminógenos relacionados con en el uso del espacio virtual para la comisión delictiva. Entre las formas de prevención existentes, se aboga por la prevención primaria, esto es la actuación sobre el origen del problema para poder intervenir de forma pre-delictual. Ello se consigue gracias a la formación y especialización de todos los agentes competentes en los múltiples ámbitos a los que afecta la cibercriminalidad en el uso de redes como Tor, que operan en la Darknet. Esta requiere de una inversión gubernamental en profesionales de la materia para que adquieran los conocimientos y habilidades indispensables para ello.

A pesar de todas estas aportaciones, hay que matizar que esto no se va a conseguir si no existe una sensibilización social, en especial gubernativa, sobre la necesaria intervención preventiva en la parte más profunda y oculta de la *Deep Web*. De ahí, nace la necesidad de conseguir un compromiso multinivel (internacional, europeo, nacional) que favorezca a la coordinación internacional y multidisciplinar. De esta manera, se pretende obtener una cobertura legal a partir de la cual se permita actuar y, así, garantizar una seguridad multidimensional.

7. Bibliografía

Abbott, T. G., Lai, K. J., Lieberman, M. R., & Price, E. C. (2007). Browser-Based Attacks on Tor. *International Worshop on Privacy Enhancing Technologies (PETS)*, 184–199.

Agencia Española de Protección de Datos. (n.d.). Agencia Española de Protección de Datos Glosario. Recuperado el 6 de febrero de 2017, de https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php

Alonso, C. (27 de septiembre de 2013). *Un informático en el lado del mal.* Recuperado el 8 de febrero de 2017, de http://www.elladodelmal.com/2013/09/conectate-tor-con-tu-propio-nodo-y-sin.html

Alonso, C. (13 de febrero de 2016). *Un informático en el lado del mal.* Recuperado el 8 de febrero de 2017, de http://www.elladodelmal.com/2016/02/deep-web-tor-freenet-i2p-privacidad-y.html

Armentano, L. (2016). El Baúl del Programador. Recuperado el 17 de enero de 2017, de https://elbauldelprogramador.com/logrando-el-anonimato-con-tor-parte-2-proxies-y-servidores-de-dns/#configurar-tor-para-resolver-los-hostnames-de-forma-segura

Bitcoin Wiki. (2015). Anonymity. Recuperado el 8 de febrero de 2017, de https://en.bitcoin.it/wiki/Anonymity

Çalışkan, E., Minárik, T., & Osula, A.-M. (2015). Technical and Legal Overview of the Tor Anonymity Network. Recuperado el 17 de enero de 2017, de http://cryptome.org/2015/07/TOR_Anonymity_Network.pdf

Castaño Apaza, G. (2014). Dominios .onion. *Revista de Información, Tecnología Y Sociedad*, *9*, 17–18. Recuperado el 17 de enero de 2017, de http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442014000100008&script=sci_arttext&tlng=es

Cervantes, P., & Tauste, O. (2015). *Internet negro: el lado oscuro de la red.* Barcelona: Editorial Planeta, S.A.

Ciancaglini, V., Balduzzi, M., Goncharov, M., & Mcardle, R. (2013). *Deepweb and Cybercrime It's Not All About TOR*. Recuperado el 16 de enero de 2017, de https://pdfs.semanticscholar.org/bc06/38ec299ef22e4c74f409e61765e7c3f91339.pdf

Collective, T. T., & Front Line Defenders. (2016). Navegador Tor para Windows - Anonimato en línea y evasión de censura. Recuperado el 5 de febrero de 2017, de https://securityinabox.org/es/guide/torbrowser/windows/

David, F., Mamani, F., Es, Q. U. É., & Su, T. O. R. Y. (2014). ¿ Qué es TOR ? *Revista de Información, Tecnología Y Sociedad*, *9*, 1–3.

Deep Web Proyecto. (30 de enero de 2015). *DeepWebPoyecto [Figura].* Recuperado el 6 de febrero de 2017, de https://deepwebproyecto.wordpress.com/page/2/

Dingledine, R., Mathewson, N., & Syverson, P. F. (2004). Tor - The Second-Generation Onion Router. *Naval Research Lab Washington DC*. Recuperado el 24 de

enero de 2017, de http://dblp.org/rec/conf/uss/DingledineMS04%0Apapers3://publication/uuid/9B8E06D9-ACFD-4316-9B8C-12E9D07FF403

Echeverri Montoya, D. (2016). *Deep Web: TOR, Freenet & I2P. Privacidad y Anonimato.* (Zeroxword). Madrid.

Electronic Frontier Foundation. (n.d.). ¿What is a Tor relay? | Tor Challenge. Recuperado el 18 de enero de 2017, de https://www.eff.org/torchallenge/what-is-tor.html

Europol. (28 de Febrero de 2017). *Europol hosts first EMPACT Crypto Currencies Workshop.* Recuperado el 28 de febrero de 2017, de https://www.europol.europa.eu/newsroom/news/europol-hosts-first-empact-crypto-currencies-workshop

FdIwiki ELP. (2016). Red Tor (Funcionamiento). Recuperado el 1 de marzo de 2017, de http://wikis.fdi.ucm.es/ELP/Red_Tor_(Funcionamiento)

Fernández Teruelo, J. G. (2011). *Derecho penal e internet : especial consideración de los delitos que afectan a jóvenes y adolescentes*. (Lex Nova, Ed.) (1ª). España. Recuperado el 18 de enero de 2017, de http://cataleg.ub.edu/record=b2048640~S1*spi

Gestal, M., & Pérez, J. L. (2011). Seguridad electrónica en la gestión de información, 119–143.

Hsu, D. F., & Marinucci, D. (2013). *Advances in Cyber Security : Technology, Operations, and Experiences.* Fordham University Press. Recuperado el 11 de enero de 2017 , de https://books.google.es/books?hl=ca&lr=&id=0wbRCwAAQBAJ&oi=fnd&pg=PA60&dq=tor+network&ots=oASI-sOCYv&sig=D0BVWvSUL2Jn9XaYcmND5_RO3jk#v=onepage&q&f=true

Loesing, K., Murdoch, S. J., & Dingledine, R. (2010). A Case Study on Measuring Statistical Data in the Tor Anonymity Network. *International Conference on Financial Cryptography and Data Security*, 203–215.

López, J. A. A. (2015). El proyecto Tor. *Paakat: Revista de Tecnología Y Sociedad*, *5*(9). Recuperado el 22 de febrero de 2017, de http://www.suv.udg.mx/paakat/index.php/paakat/article/view/246/385

Machín, N., & Gazapo, M. (2016). La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea. *Revista UNISCI*, (42), 47–68. Recuperado el 20 de febrero de 2017, de https://doi.org/10.5209/RUNI.53786

Maeztu, D. (19 de marzo de 2013). *Del derecho y las normas.* Recuperado el 13 de febrero de 2017, de http://www.derechoynormas.com/2013/03/es-legal-cifrar-nuestras-comunicaciones.html

Maeztu, D. (20 de marzo de 2013). *Del derecho y las normas.* Recuperado el 8 de febrero de 2017, de http://www.derechoynormas.com/2013/03/responsabilidad-tor-I.html

Mccoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008). Shining Light in Dark Places : Understanding the Tor Network. *International Symposium on Privacy Enchancing Technologies Symposium (PETS)*, 63–76.

MG, A. (2011). La evolución de la tecnología aplicada a la seguridad. Recuperado el 27 de Febrero de 2017, de http://cj-worldnews.com/spain/index.php/es/criminologia-30/seguridad/tecnologia-y-seguridad/item/1717-la-evolución-de-la-tecnología-aplicada-a-la-seguridad

Ministerio de Interior. (2013). *Ministerio del Interior.* Recuperado el 3 de marzo de 2017, de http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815

Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2001). Report on the Development of the Advanced Encryption Standard (AES). *Journal of Research on the National Institute of Standards and Technology (NIST)*, *106*(3), 511. Recuperado el 11 de enero de 2017, de https://doi.org/10.1.1.32.5335

Noticias Jurídicas. (2014, February 14). Las direcciones IP de los usuarios de Internet deben ser consideradas como datos personales y por tanto, están protegidos por la LOPD. noticias.juridicas.com. Recuperado el 17 de febrero de 2017, de http://noticias.juridicas.com/actualidad/jurisprudencia/5411-las-direcciones-ip-de-los-usuarios-de-internet-deben-ser-consideradas-como-datos-personales-y-por-tanto-estan-protegidos-por-la-lopd/

Panda Security Mediacenter. (2017). Recuperado el 28 de febrero de 2017, de Tor y Deep Web: todos los secretos del lado oscuro de la red: http://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/

P2P Foundation Wiki. (2013). Tor. Recuperado el 22 de enero de 2017, de http://wiki.p2pfoundation.net/Tor

Perojo, K. R., & León, R. R. (2006). El web como sistema de información. *Acimed*, *14*(1), 1–15. Recuperado el 9 de febrero de 2017, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352006000100008

Portal TIC. (7 de agosto de 2013). *La red cifrada TOR recomienda abandonar Windows.* (E. Press, Ed.) Recuperado el 2 de febrero de 2017, de http://www.europapress.es/portaltic/internet/noticia-red-cifrada-tor-recomienda-abandonar-windows-20130807111434.html

Rudesill, D., Caverlee, J., & Sui, D. (2015). *The Deep Web and the Darknet: a Look Inside the Internet's Massive Black Box*. (Woodrow Wilson International Center for Scholars, Ed.). Washington DC. Recuperado el 22 de enero de 2017, de http://dx.doi.org/10.2139/ssrn.2676615

Starke, P. (2016). *Tor and the Dark Net: Avoid NSA Spying and Remain Anonymous Online (Dark Net and Tor)*. Recuperado el 19 de enero de 2017, de https://www.amazon.com/Tor-Dark-Net-Spying-Remain-ebook/dp/B01N0EB43F/ref=sr_1_1?s=digital-text&ie=UTF8&qid=1493306020&sr=1-1&keywords=tor+and+the+dark+net+avoid+nsa+spying+and+remain+anonymous+online

Tactical Technology Collective, & Front Line Defenders. (n.d.). El complemento NoScript | security in-a-box. Recuperado el 10 de enero de 2017, de https://securityinabox.org/es/firefox_noscript

Tactical Technology Collective Front Line Defenders. (2016). Navegador Tor para Windows - Anonimato en línea y evasión de censura. Recuperado el 2 de febrero de 2017, de https://securityinabox.org/es/guide/torbrowser/windows/

The Gnome Project. (n.d.). ¿Qué es una dirección MAC? Recuperado el 1 de febrero de 2017, de https://help.gnome.org/users/gnome-help/stable/net-macaddress.html.es

The Tor Project. (n.d.). *La solución: una red anónima distribuida [Figura].* Recuperado el 18 de enero de 2017, de https://www.torproject.org/

The Tor Project. (n.d.). *Torproject.* Recuperado el 20 de enero de 2017, de https://www.torproject.org/docs/tor-doc-relay.html.en

The Tor Project. (n.d.). *Torproject*. Recuperado el 12 de febrero de 2017, de https://www.torproject.org/index.html.en

The Tor Project. (n.d.). *Torproject.* Recuperado el 21 de enero de 2017, de https://www.torproject.org/about/overview.html.en

The Tor Project. (n.d.). *Torproject*. Recuperado el 1 de febrero de 2017, de https://www.torproject.org/projects/torbrowser.html.en

The Tor Project. (n.d.). *Torproject*. Recuperado el 20 de febrero de 2017, de https://www.torproject.org/about/torusers.html.en

The Tor Project. (n.d.). *Torproject*. Recuperado el 5 de febrero de 2017, de https://www.torproject.org/projects/torbrowser.html.en

Tor y Deep web: los secretos del lado oscuro de la web. (2016). Recuperado el 28 de Febrero de 2017, de http://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/

Tyler, K. D. (27 de septiembre de 2007). Crude diagram of the “onion routing” principle [Figura]. Recuperado el 21 de enero de 2017, de https://commons.wikimedia.org/wiki/File:Onion_diagram.png

Unión Europea. Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. *Boletín Oficial del Estado*, 4 de mayo de 2016, núm. 119, pp. 89-131. Recuperado el 19 de febrero de 2017, de https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80808

Vicente Alarcón, J. A., & Guillén Guillén, V. C. (2015). Guía metodológica de uso seguro de internet para personas y empresas utilizando la Red Tor. *Doctoral Dissertation, PUCE*. Recuperado el 10 de enero de 2017, de http://repositorio.puce.edu.ec/bitstream/handle/22000/11982/Disertacion de grado Guillén Vicente_Final.pdf?sequence=1&isAllowed=y

Vitoria Real, A. (5 de junio de 2015). *Lexnova.* Recuperado el 27 de febrero de 2017, de http://penal.blogs.lexnova.es/2015/06/05/ciberdelitos-regulacion-actual-y-retos-para-el-futuro/

Watson, K. D. (2012). The Tor Network : A Global Inquiry into the Legal Status of Anonymity Networks, *11*(3). Recuperado el 12 de enero de 2017, de http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1417&context=law_global studies

Zantout, B., & Haraty, R. (2011). I2P data communication system. *ICN 2011, The Tenth International Conference …*, (c), 401–409. Recuperado el 12 de enero de 2017, de http://www.thinkmind.org/index.php?view=article&articleid=icn_2011_19_10_10010

Zuñiga, H. D. C. (2015). *TOR, anonimato en internet.* Recuperado el 13 de enero de 2017, de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0885_ChaparroZunigaHD.pdf

Webgrafía

https://www.debian.org/intro/free

http://www.linuxadictos.com/tor-browser-5-0-el-navegador-de-la-privacidad.html

http://wiki.hacktivistas.net/index.php?title=Tools#TOR

http://www.elotrolado.net/wiki/Todo_sobre_P2P

https://geti2p.net/en/comparison/tor

https://tails.boum.org/doc/about/warning/index.en.html