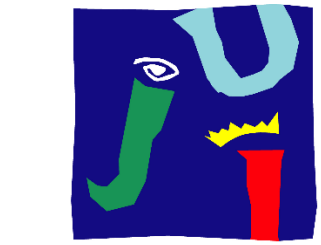

UNIVERSITAT JAUME·I

Trabajo Fin de Grado

REDES P2P Y CIBERDELINCUENCIA

Presentado por:

Eduardo López Pérez

Tutor/a:

Filiberto Pla Bañón

Grado en Criminología y Seguridad

Curso académico 2021/22

ÍNDICE

Extended summary

Technology has advanced over the years to make life easier for human beings. From the invention of the wheel to the invention of smartphones, each time mankind has received new conveniences to improve their quality of life.

In this way, throughout the last decades, technology has continuously advanced in a multitude of fields and areas that impact our daily lives, being part of the diversity of contexts in which our lives are developed. In particular, computers, information technology and information and communication technologies have undoubtedly brought about a worldwide revolution. In addition, the advent of the Internet has allowed us to be in contact with people located on the other side of the world and to establish relationships that would have been unimaginable a few years ago. In addition, the network has made it easier for us to be informed about what is happening in the world and to acquire new knowledge.

However, not everything brought about by computers and the Internet has been of benefit to humane society, but it has also brought with it new threats that can cause serious problems for the people concerned.

Also since the beginning of humanity, there have been people who performed acts in order to harm or benefit from the pain caused to other people. Killing, stealing, swindling, injuring... These are what we know as crimes.

Some criminals, with the arrival of computers and the Internet to the vast majority of homes, saw a new opportunity to commit crimes easily from home through these new devices. These crimes committed through the network or computers are called cybercrimes and their perpetrators are called cybercriminals.

With this in mind, cybercrime can be defined as illegal acts that, taking advantage of technological advances, manage to overcome the defenses of computer systems, causing the violation of these and initiating a variety of crimes of different nature or that may have a different criminal essence, such as events that affect privacy and intimacy, events that affect users' businesses or even practices tolerated by a large part of the community such as illegal downloading of movies and files.

Cybercrime stands out for being a poorly typified and unclassified crime. It is also difficult to know or measure the scope of the crime, as well as the difficulty of proving who committed it and the difficulty of proving its existence, due to the complexity of collecting evidence. To this must be added the existence of ignorance on the part of

the jurists and the police, which is why the work investigated by the experts in these cases is very much taken into account. They are simple acts that can be committed in a matter of seconds and without the need for the person responsible to be on the scene, and can be committed from anywhere in the world. In addition, it allows a large number of victims to be reached at the same time, given the network connection of all the computers.

One of the most frequent cybercrimes is computer fraud, in which the cybercriminal tricks the victim into giving the criminal money or something beneficial. Computer fraud is one of the most committed computer crimes in Spain and can be committed by a multitude of behaviors. The scam known as the Nigerian scam stands out, where the perpetrator sends an email to the victim promising a large amount of money in exchange for an advance payment by the victim to an account provided by the perpetrator.

Methods such as carding or phishing are also very common when talking about cybercrime. The first consists of copying credit cards belonging to third parties in order to purchase goods with them. The second consists of fraudulently obtaining bank passwords in order to transfer money to another bank account. The jurisprudence in these cases has admitted that the liability would be of the bank or payment service provider, unless there is gross negligence or fraud on the part of the victim.

However, the most frequent and common cybercrime of all is computer viruses. It consists of deleting, deteriorating, hiding, damaging, altering or suppressing computer data without the computer user's authorization and with a serious result. What is remarkable about this type of crime is that no minimum amount is required for the crime to be understood as having been committed and for a conviction to be handed down. In addition, malware programs can access personal information on another computer without the owner's consent.

One of the safest places for cybercriminals is the dark web. With the evolution of technology has come a lot of progress in the ability to investigate and methods to prosecute crimes, so cybercriminals had to hide in the network to continue committing these. When we talk about hiding in the network to commit a crime, two concepts always arise, the dark web and deep web. However, it should be specified that deep web is not always synonymous with illegality, as it is usually thought. It is called the deep web because of how inaccessible or exposed the data is over the Internet, not because of its origin or its legitimate or illegitimate purpose. It is currently estimated that the Deep Web accounts for 96% of the total network, and only 4% is the surface

network, the one that is visible to the naked eye and used by the vast majority of the population.

This is why when we talk about cybercrime, we talk about the dark web. This network concept emerges from the injection of files or objects according to the first statement, and the distribution of these according to the second and third statements. One of the main pillars of the dark web is that the whole system can provide it with content because there is a certain group of users who are able to overcome all security mechanisms.

Special mention should be made of the fact that not all stolen information always ends up in this network because some files or secrets have more value if they are not disseminated, such as military or industrial information. Finally, although these types of networks seem to be designed to commit crimes, they are also used to maintain the privacy of communications, such as the TOR network.

In addition, one of the advantages of the Internet has been the emergence of peer to peer networks. A peer to peer network is a network in which the nodes act as servers and clients at the same time, without any kind of hierarchy. Thus, in such a network, each computer or device would be on an equal footing with the others, resulting in the existence of a horizontal type of communication. This allows the direct exchange of information in any format between the interconnected terminals. This network model contrasts with the classic client-server model, which is governed by a structure where there is no distribution of tasks between them, only a communication between terminal and user, so they cannot exchange roles.

The characteristics that make peer to peer networks stand out are that they provide a direct connection without any type of intermediary, as well as being able to adapt to the instability and diversity of connections, automatically adjusting to failures and the high variability in the number of nodes. Also noteworthy is the robustness and replication of content, which, due to its nature, increases robustness in the event of various data replication errors to multiple destinations. Cost sharing among users is another outstanding feature. Security is the most desirable feature of peer to peer networks, although there is still work to be done. The objectives of a secure peer to peer network would be to identify and circumvent malicious nodes and malware infected content dangerous to users, prevent eavesdropping on inter-node communications, the creation of secure node groups within the network, and secure storage of all information. Finally, scalability is one of the most important features. Peer to peer networks have a global reach with a huge number of potential users. Ideally, the more

nodes connected to a network, the better its performance. To this end, when nodes come together and share their own resources, the total resources of the system increase. This is a great advantage over the classic server-client architecture with a server system, since the entry of more clients can mean that data transfer would be slower for all users.

There are different types of peer to peer networks that differ according to their own characteristics. The best known are eMule and BitTorrent. The first is a classic in peer to peer networks, as it was the one that made this system for downloading movies and songs for free known in Spain. It also gave rise to numerous other networks. Users connect to the network client and the latter to the eMule server to connect to another user and download the file.

Besides, BitTorrent works in a different way, connecting to different users and downloading different fragments from them, and then joining them together to obtain the requested file. It is necessary to connect to a user who has the complete file to ensure that no fragment is missing.

The most widely used peer to peer darknet is called Freenet. It is totally anonymous and distributed, designed as a distributed data store, so a large number of programs and applications have been built on it, allowing the publication of a web page from anonymity, for example. It is practically impossible and unfeasible to remove content, since the information as specified above is distributed, which is a real problem when dealing with criminal files, such as child pornography, which will never cease to be accessible on this network. However, it is a great tool when you want to avoid censorship.

According to the Spanish legal system and the legislation currently in force, downloading movies through peer to peer networks is not illegal, as long as it is not for profit, it is not punishable under criminal law, since it overrides the right to have a copy of the file. However, it may constitute a civil offense, in which the author of the file can sue for copyright infringement. But these cases are very rare, given the difficulty of identifying the users who own the IP that downloaded the file.

The most common crime committed through the use of peer to peer is child pornography. Given the nature of the peer to peer system, it is very easy to find these illicit files and at the same time, they are duplicated and spread very easily, because it is not only the people who knowingly share these files and their consumers who share and download them, but there are also many cases where people mistakenly download

them and in turn mistakenly share them. The police enter some identified child pornography files into the peer to peer network in order to trace the hash fingerprint and be able to locate the consumers of this material, but unfortunately this is not the majority of the content on the network. By not having the material localized, they cannot trace them and it makes it difficult to arrest the consumers in most cases.

A year ago, several people were arrested in Galicia for a crime of possession and distribution of child pornography in which investigations were initiated by tracing the footprints of different files, which led to the identification of seven IP addresses from where child pornography files were being shared on peer to peer networks. When these users were arrested and their computer systems were searched, thousands of files, both video and photographs of child pornography were found.

The Spanish legal system punishes everything related to child pornography in peer to peer networks with the same harshness as it punishes traditional child pornography. In addition, in cases where it has been downloaded or shared by mistake, despite how difficult it may be for the detainees to prove their innocence and that it was all a mistake, they are usually acquitted and not convicted of innocence.

Although there is no specific law to punish the use of peer to peer networks or the crimes that can be committed through them, the Spanish legal system has found an effective way to deal with these crimes, at least in the medium term, equating them with those committed in the traditional way. But at some point it will be necessary to legislate peer to peer network crimes and cybercrimes in general.

In addition, in my opinion, it would be a top priority to find a way for the police to cut off the flow of child pornography and track the hush fingerprint of all files and not only those previously identified, because in my view, the greatest danger of P2P networks is this sensitive material of minors, that every day thousands of new files of this kind appear on the network.

Resumen

La tecnología ha avanzado de forma considerable durante los últimos tiempos aportando gran cantidad de beneficios a la sociedad. Sin embargo, con la llegada de internet y la facilidad de difusión de archivos han surgido y han aumentado con el paso de los años los llamados ciberdelitos.

Algunas herramientas como las redes P2P se han convertido en uno de los métodos más empleados para compartir archivos ilícitos entre usuarios de diversas partes del mundo. Debido a sus características y su modo de proceder estas redes vulneran los derechos de autor. Además, su naturaleza de igual a igual, sin un servidor central, dificulta a la policía el poder localizar a los ciberdelincuentes que actúan empleando este tipo de redes.

Se ha visto que el principal delito compartido a través de redes P2P es la pornografía infantil a través de servidores no muy conocidos como Freenet en manos de ciberdelincuentes y a través de otros altamente empleados como BitTorrent y eMule, lo cual ocasiona su descarga errónea en muchos usuarios de estas plataformas, contribuyendo a la distribución de material sensible y convirtiéndose en sujetos activos del delito.

Actualmente, el ordenamiento jurídico español castiga los delitos cometidos a través de las redes P2P como si se tratasen de delitos tradicionales, pues el uso de estas herramientas no se considera necesariamente un ilícito penal, castigando solamente las acciones tipificadas cometidas a través de éstas.

Palabras clave: informática, redes P2P, ciberdelito, pornografía infantil, copyright, ordenamiento jurídico.

Abstract

Technology has advanced considerably in recent times, bringing many benefits to society. However, with the arrival of the Internet and the ease of file sharing, cybercrime has emerged and increased over the years.

Some tools such as peer-to-peer networks have become one of the most widely used methods for sharing illicit files between users from different parts of the world. Due to their characteristics and the way they operate, these networks infringe copyright. In addition, their peer-to-peer nature, without a central server, makes it difficult for the police to track down cybercriminals using such networks.

It has been seen that the main crime shared through peer-to-peer networks is child pornography through not very well known servers such as Freenet in the hands of cybercriminals and through other highly used ones such as BitTorrent and eMule, which causes many users of these platforms to mistakenly download, contributing to the distribution of sensitive material and becoming active subjects of the crime.

Currently, the Spanish legal system punishes crimes committed through P2P networks as if they were traditional crimes, since the use of these tools is not necessarily considered a criminal offense, punishing only the criminalized actions committed through them.

Keywords: computing, peer-to-peer networks, cybercrime, child pornography, copyright, legal system.

1. Introducción

Históricamente la tecnología se ha empleado con objeto de satisfacer nuestras necesidades. Así, el desarrollo tecnológico ha proporcionado en las distintas sociedades desde recursos considerados primarios (por ejemplo: alimentación, vivienda, protección…) hasta otros más específicos y complejos (por ejemplo: estética o redes sociales) (Cruz, 2009).

De esta manera, a lo largo de las últimas décadas la tecnología ha avanzado de forma continua en multitud de ámbitos y áreas que impactan en nuestro día a día, siendo partícipes de la diversidad de contextos en los que se desarrolla nuestra vida. En concreto, las tecnologías de la información y comunicación (TIC) han supuesto, sin duda, una revolución a nivel mundial (Pozas et al., 2018). Así, la creación de internet ha generado un fenómeno conocido como globalización que nos ha permitido estar en contacto con personas ubicadas a miles de kilómetros y establecer relaciones, en el pasado, inimaginables. Además, la red nos ha dado acceso a crear vínculos en entornos más cercanos como el escolar y el familiar, lo cual ha generado grandes beneficios para las personas.

No obstante, la informática no solo ha abierto la puerta a nuevos beneficios y ventajas para la vida de los usuarios, sino que ha facilitado la creación de nuevos métodos para delinquir. Estos crímenes cometidos a través de la red son conocidos como ciberdelitos, actos de aquellos conocidos comúnmente como ciberdelincuentes, y son un problema cada vez más extendido y más difíciles de frenar. En este contexto, las redes P2P, con un uso malicioso, pueden ayudar a la difusión de material ilícito que afecten a las víctimas de un ciberdelito. Este trabajo, por tanto, tiene los siguientes objetivos:

- Estudiar las redes P2P, sus características principales, los distintos tipos de estructura que pueden tener y cuáles son las más conocidas.
- Definir lo que es la ciberdelincuencia, sus características y cuáles son los tipos de ciberdelitos más cometidos.
- Relacionar ambos conceptos, reflejando como los ciberdelincuentes actúan a través de las redes P2P.
- Tratar el impacto jurídico de estos comportamientos y como la legislación española persigue y castiga estos delitos.

2. Redes P2P

2.1 Definición

Una red P2P, cuyas siglas significa red de pares o red entre iguales en inglés, es una red en la que los nodos cumplen la función de servidores y de clientes al mismo tiempo, sin que exista ningún tipo de jerarquía al respecto. Así, en una red de estas características cada ordenador o dispositivo estaría en un plano de igualdad con los demás, provocando la existencia de una comunicación de tipo horizontal (Duarte, 2015). Esto permite el intercambio directo de información, en cualquier formato entre los terminales interconectados.

Este modelo de red contrasta con el clásico modelo cliente-servidor, el cual se rige mediante una estructura donde no hay ningún tipo de distribución de tareas entre sí, solo una comunicación entre terminal y usuario, por lo que estos no pueden intercambiar roles (Pla, 2021).

2.2 Origen e historia

La primera red P2P fue el programa Hotline Connect, creado por el australiano Adam Hinkley en 1996 cuyo objetivo era proporcionar una plataforma donde las universidades y empresas pudieran distribuir archivos de forma rápida, cómoda y eficaz. Pero al poco tiempo, se observó su utilidad para uso entre particulares, en el que los usuarios podían intercambiarse cualquier tipo de archivos, desde música en formato mp3 hasta contenido ilícito o material pornográfico. Hotline Connect usaba un sistema descentralizado, pues no utilizaba ningún servidor central, sino que eran completamente autónomos. Los archivos disponibles para descargar se almacenaban en los ordenadores de los usuarios que querían que funcionasen como servidores. Pero si el dueño de ese ordenador lo apagaba, no se obtenían los datos y no podías seguir descargándolo. Esto provocó que el sistema, aunque bien planteado al comienzo, se quedara obsoleto rápidamente. Además, esta aplicación solo funcionaba en los ordenadores con el sistema operativo MacOs por lo cual no llamó la atención de la prensa a gran escala. Estas dos razones fueron el motivo por el que el programa y su funcionalidad cayeron en el olvido (CurioSfera, s.f).

Poco tiempo después, Shawn Fanning y Sean Parker cofundaron Napster en el verano de 1999. La aplicación de *software* Napster permitía a los usuarios ubicar y compartir archivos de música desde una interfaz conveniente y fácil de usar (Buttle y Correia, 2002). Al contrario que Hotline Connect, este usaba una red centralizada para indexar

los usuarios y archivos compartidos. Durante el año 2000, Napster alcanzó la cifra de 13 millones de usuarios que descargaban sin pagar millones de canciones, lo cual provocó que diversas discográficas y figuras importantes del mundo de la música[1] presentaran una demanda contra Napster por infracción de copyright. Paralelamente, Justin Frankel y Tom Peeper desarrollan Gnutella, red donde ningún servidor hace de puente.

En 2001, el juez encargado del caso Napster decretó el cierre de la plataforma. Tras esto se convirtieron en un servicio de pago. Pero conforme avanzaba la tecnología, se creaban más redes descentralizadas[2] por lo que a Gnutella se les unió otros servicios del estilo como Kazaa, Grokster o Ares, que ya no solo podía intercambiar archivos MP3, si no que archivos MP4, videojuegos y archivos de todo tipo. Desde entonces hasta la actualidad, han ido apareciendo y desapareciendo sistemas de redes P2P, siendo la más conocida actualmente BitTorrent (García, 2019).

2.3 Características

Entre las características de las redes P2P, Los Santos (2009) las numera y define, destacando en concreto **dos** que hacen que este tipo de red sea tan único:

- El intercambio de recursos informáticos se realiza a través de una conexión directa sin necesidad de que exista un intermediario que ejecute la función que realizaría un servidor central. Los servidores centralizados, característico de un tipo concreto de red P2P que se mostrará más adelante, pueden ser utilizados a veces para insertar nuevos nodos en la red, obtener claves globales para la encriptación o para arrancar el sistema.
- Las redes P2P son capaces de adaptarse a la inestabilidad y diversidad de las conexiones, ajustando automáticamente ante fallos y la alta variabilidad en el número de nodos.

Además, el autor también menciona que las redes P2P requieren de ciertas características más para que puedan funcionar de manera correcta y sin ningún tipo de problema. Una de ellas es la **robustez y replicación de contenidos**, por la que debido a su naturaleza incrementa la solidez y robustez en caso de que se produzcan diversos errores de replicación de datos a múltiples destinos. En los sistemas P2P

1 Entre los más destacados, se encuentran Lars Ulrich (batería del grupo Metallica), el rapero Dr. Dre o la discográfica A&M Records.

2 Al no depender de un servidor central, no hay constancia de los archivos intercambiados, por lo que es más difícil perseguirlos a nivel judicial.

puros, permite a los *peers* encontrar información sin realizar ninguna solicitud a ningún servidor de indexación centralizado.

- El **reparto de costes** entre usuarios e incentivos también es una característica importante. Dependiendo de la aplicación de la red, los recursos pueden ser archivos, ciclos de proceso, ancho de banda o almacenamiento en disco. Además, se espera que el autor de un contenido, lector, editor, el servidor que lo aloja y la solicitud para encontrarlo sean anónimos siempre que así lo necesiten los usuarios. Hay que recordar que en estos sistemas la información puede pasar a través de ciertos nodos, que no son ni la fuente de origen ni el destino de la comunicación, los cuales almacenan estos datos de forma transparente y sin participar el usuario de forma activa en estas acciones.
- La **seguridad** es una de las características más deseables de las redes P2P, pero menos implementada y bajo mayor investigación. Los objetivos de una red P2P segura sería identificar y esquivar los nodos maliciosos y el contenido infectado de *malware* peligroso para los usuarios, evitar el espionaje en las comunicaciones entre los nodos, la creación de grupo de nodos seguros dentro de la red y un almacenamiento seguro de toda la información.

Por último, Los Santos (2009) señala que una de las características más importantes es la **escalabilidad**. Las redes P2P tienen un alcance mundial con un enorme número de posibles usuarios. Idealmente, cuantos más nodos estén conectados a una red, mejor será su rendimiento. Para ello, cuando llegan los nodos y comparten sus propios recursos, los recursos totales del sistema aumentan. Esto es una gran ventaja respecto a la clásica arquitectura servidor-cliente con un sistema de servidores, puesto que la entrada de más clientes puede significar que la transferencia de datos fuera más lenta para todos los usuarios.

2.4 Tipos de redes

Según Nicolini (2017) se pueden clasificar los tipos de redes P2P en los siguientes tres grupos y con las siguientes características:

2.4.1 Red centralizada

Este tipo de arquitectura se basa en el hecho de que todas las transacciones de los usuarios se hacen a través de un único servidor al cual todos los nodos se conectan entre si (Cantos, 2020), lo que permite que estos puedan almacenar y distribuir los nodos donde se encuentras los contenidos. Tiene por tanto una estructura monolítica,

pueden realizar un seguimiento de donde se almacena el contenido y presentan una gestión muy dinámica con una disposición de contenidos más permanente.

Sin embargo, es muy limitado en términos de privacidad del usuario además de otras dificultades como problemas legales, puntos únicos de fallo, mayor consumo de ancho de banda y enormes costes de mantenimiento. Un ejemplo bien conocido es la anteriormente mencionada Napster.

2.4.2 Red híbrida, semidescentralizada o mixta

En este tipo de red se pueden ver las interacciones entre un servidor central que actúa como un HUB o multiconector para administrar los recursos de banda ancha, enrutamiento y comunicación entre nodos, pero sin conocer la identidad de cada nodo y sin almacenar ninguna información, por lo que el servidor no comparte archivos de ningún tipo con otros nodos. Tienen la propiedad de funcionar (por ejemplo, un *torrent*) de ambas formas, es decir, puede incorporar varios servidores que gestionen los recursos compartidos, pero también, en caso de que estos se caigan, la agrupación de nodos puede permanecer en contacto a través de una conexión directa entre ellos, por lo que se puede seguir compartiendo y descargando más información sin ningún servidor.

2.4.3 Red descentralizada

Las redes descentralizadas son las redes P2P más comunes y las más versátiles, ya que no requieren ni de gestión ni servidores centrales (Rodríguez, 2012). En este tipo de red no hay directorios o cualquier otro punto de control con respecto a la topología o ubicación física en el que se encuentra el contenido. Son los propios usuarios los que se erigen como nodos de las conexiones y los encargados de almacenar esa información. La anteriormente mencionada Gnutella es un ejemplo de este tipo de red P2P (una red formada por nodos que entran y salen de la red de forma casi constante). Hay muchos factores que impulsaron el uso de redes descentralizadas, como el control de la privacidad, la disponibilidad del contenido, la escalabilidad, la seguridad y la confianza que trasmite esta arquitectura.

Pero, por otro lado, un aspecto controvertido de este tipo de red es la forma en la que se localizan los contenidos, en la que cada nodo envía la consulta a todos los vecinos. Este método se denomina *Flooding* (Inundación) y es extremadamente ineficiente y genera una gran carga en los nodos de la red.

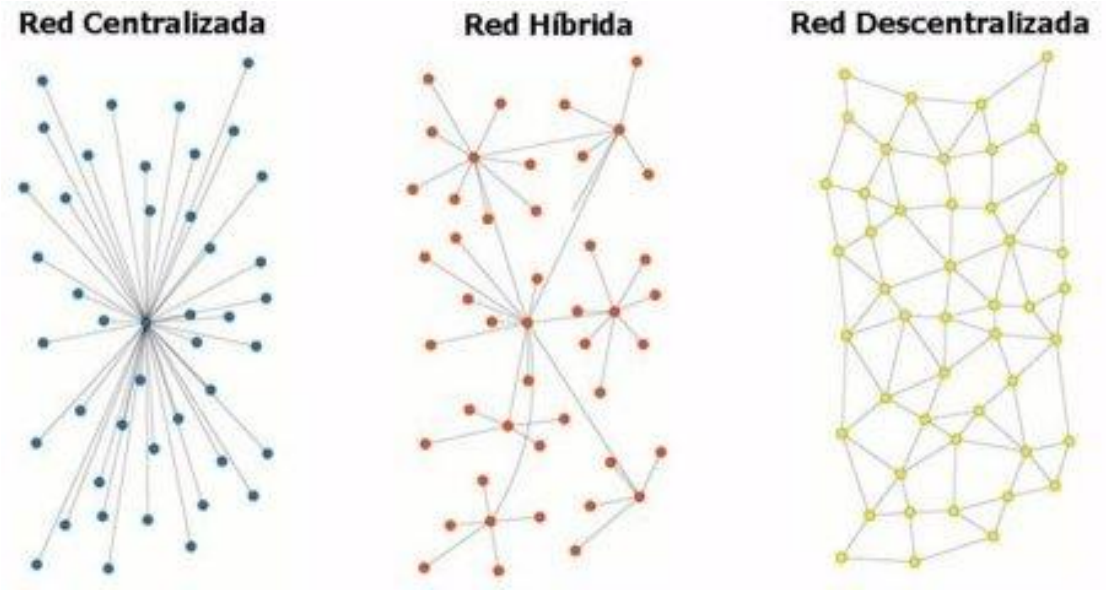

Figura 1. Tipos de Redes P2P (Rodríguez, 2012).

3. Ciberdelincuencia

3.1 Definición

El término **ciberdelito** proviene de la denominación anglosajona "*computer crime*", término que fue acuñado por diversos autores de la materia a finales de la década de los 80. De Urbano Castrillo (2011) define el delito informático de la siguiente manera:

> *se trata de un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta. El Convenio de Budapest ofrece un concepto basado tanto en la utilización de determinadas técnicas y modos de proceder informáticos …, como en ciertos contenidos cuya vulneración se ve facilitado por el medio Internet. (p.18)*

Una vez ha delimitado el autor este concepto, distingue entre los delitos informáticos clásicos, que se cometen a través de internet (ciberterrorismo, amenazas, chantajes, delitos contra la libertad sexual…) y los delitos "*strictu sensu*" que son los que necesitan la intrusión en equipos o la captación de información, fraudes, etc. Por otra parte, Carlos Sarzana en su obra escrita en 1979 "*Criminalitá e Tecnología"* define el concepto de ciberdelito como "*cualquier comportamiento criminógeno en el cual el ordenador o computadora ha estado involucrado como material, como objeto de la acción criminógena o como mero símbolo"* (Alvarado, 2017).

Partiendo pues de ambos conceptos, se puede definir el ciberdelito como los actos ilegales que, valiéndose de la ventaja surgida de los avances tecnológicos, consiguen superar las defensas de los sistemas informáticos, provocando la vulneración de estos e iniciar una variedad de delitos de distinta naturaleza o que pueden tener una esencia delictiva distinta, como por ejemplo los hechos que afectan la privacidad e intimidad, hechos que afectan a los negocios de los usuarios o incluso prácticas toleradas por gran parte de la comunidad como es la descargas ilegales de películas y archivos.

3.2 Características

Los ciberdelitos cuentan con un gran número de características propias y particulares (Cordero, 2021).

- En primer lugar, se trata de un **delito poco tipificado y no clasificado** debido a que cada día aparecen nuevas técnicas y herramientas a un ritmo más veloz de lo que el Derecho puede alcanzar. También es difícil saber o medir el alcance del delito, así como la dificultad probatoria para demostrar quien lo cometió y la dificultad de demostrar su existencia, debido a la complejidad que tiene la recolección de pruebas. A esto hay que sumar la existencia del desconocimiento por parte de los juristas y de la policía, razón por la que se tiene muy en cuenta el trabajo investigado por los peritos en estos casos.

- Son **actos simples** y que pueden llevarse de forma rauda, en algunas ocasiones cometiéndose en cuestión de segundos y que sin que la persona responsable esté en el lugar de los hechos. También la ciberdelincuencia se beneficia de la inexistencia de barreras geográficas, pues todo el mundo está conectado por la red y existen países donde hay poca o nula regulación de la materia, por lo que, al igual que existen paraísos fiscales para evadir impuestos, también existen paraísos cibernéticos para los ciberdelincuentes.

- Por último, una de las características más importante es **la masividad**, dado que la red permite la difusión masiva de contenidos, lo cual facilita la comisión de estos delitos desde cualquier parte del mundo.

3.3 Actualidad y herramientas

Como ya se ha mencionado antes, los ciberdelitos son cada vez más comunes y peligrosos debido a la evolución casi diaria que tiene la tecnología. Están a la orden del día. Entre los ciberdelitos más frecuentes encontramos las estafas informáticas, los delitos informáticos de daños, las defraudaciones de telecomunicaciones y los ciberdelitos contra la intimidad (Esparís, 2020).

La conducta realizada en las **estafas informáticas** consiste en producir un desplazamiento patrimonial, con ánimo de lucro, en perjuicio de la víctima por medio de una actividad engañosa. Estos actos de engaño se han de dirigir a sistemas informáticos que a su vez producen el engaño de la víctima. Si no se cumpliera este requisito, se trataría de un delito de estafa normal.

La estafa informática es uno de los delitos informáticos más cometidos en España y se puede cometer por una multitud de conductas. Destaca la estafa conocida como estafa nigeriana, donde el autor envía un correo electrónico a la víctima donde le promete una gran cantidad de dinero a cambio de un pago por adelantado de parte de la víctima a una cuenta proporcionada por el autor.

Dentro de los tipos de este ciberdelito también se encuentran los fraudes informáticos conocidos como ***carding*** **y** ***phishing***. El primero consiste en el copiado de tarjetas de créditos ajenas al autor para realizar adquisiciones de bienes con ellas. El segundo consiste en la obtención de contraseñas bancarias de forma fraudulenta con el fin de transferir el dinero a otra cuenta bancaria a través del correo electrónico como soporte material para reconducir a la víctima a un sitio “web” falso (Oxman, 2013). La jurisprudencia en estos casos ha admitido que la responsabilidad sería del banco o proveedor de servicios de pago, salvo que se aprecie negligencia grave o fraude en la víctima.

Los delitos informáticos de daño son los comunes **virus informáticos**. Consiste en borrar, deteriorar, ocultar, dañar, alterar o suprimir datos informáticos sin que el usuario del ordenador dé su autorización y con un resultado grave. Lo destacable de este tipo de delitos es que no se exige una cantidad mínima para que el delito se entienda como cometido y recaiga condena en él. Las defraudaciones de telecomunicaciones por otro lado, consiste en aprovecharse ilícitamente de alguna telecomunicación de otra persona, por ejemplo, el *Wifi*. Es necesario que le cause un perjuicio económico.

Por último**, los delitos contra la intimidad** son aquellos en los que una persona instala un programa que contiene *malware*[3] en su dispositivo y el creador de ese *malware* accede a la información personal del ordenador sin el consentimiento del propietario.

4. Utilización de redes P2P para la ciberdelincuencia

4.1 Tipos de delitos en redes P2P

4.1.1 Redes oscuras P2P. Freenet

Antes de hablar de redes oscuras P2P, vamos a definir lo que es la red oscura (*darknet)*. Con la evolución de la tecnología se ha avanzado mucho en la capacidad de investigación y en los métodos para perseguir delitos, por lo que los ciberdelincuentes tuvieron que esconderse en la red para seguir cometiendo estos. Cuando hablamos de ocultarse en la red para cometer un delito siempre surgen dos conceptos, la **red oscura** y **red profunda** (*Deep Web).* Sin embargo, hay que especificar que red profunda no siempre es sinónimo de ilegalidad, como se piensa normalmente. Se le llama red profunda debido a lo poco accesibles o expuestos que se encuentren los datos a través de internet, no por el origen o su finalidad legítima o ilegítima. Actualmente se estima que la *Deep Web* supone un 96% del total de la red, y solo el 4% se asocia al internet convencional (Álvarez et al., 2018), es decir, la que se ve a simple vista y que utilizamos la gran mayoría de la población.

Es por esto por lo que cuando se habla de cibercrimen, se habla de la red oscura. El término fue acuñado por un grupo de investigadores de Microsoft en un documento denominado "*The Darknet and the Future of Content Distribution"* (Biddle, 2002) donde afirman que esta se basa en tres supuestos:

- Cada objeto distribuido estará disponible para una fracción de usuarios de forma que puedan copiarlos.
- Los usuarios copian objetos si es posible y les interesa.
- Los usuarios están conectados a redes de banda ancha.

Este concepto de red emerge de la inyección de archivos u objetos de acuerdo con la primera afirmación, y la distribución de estos cumpliendo la segunda y tercera afirmación. Uno de los principales pilares de la red oscura es que todo el sistema

[3] Traducido como "programa maligno" en castellano.

puede proveerla de contenido porque existe un determinado grupo de usuarios que son capaces de sobrepasar todos los mecanismos de seguridad.

Mención especial a que no siempre toda la información robada termina en esta red debido a que algunos archivos o secretos tienen más valor si no son difundidos, como puede ser la información militar o industrial. Para finalizar, aunque este tipo de redes parezcan concebidas para cometer delitos, también se utilizan con el objetivo de mantener la privacidad de las comunicaciones, como por ejemplo la red TOR. Se considera que existen dos tipos de red oscura, **las *peer to peer*** y las no *peer to peer* (ver Figura 2). La red TOR forma parte de la segunda, aunque nosotros solo vamos a hablar de las primeras.

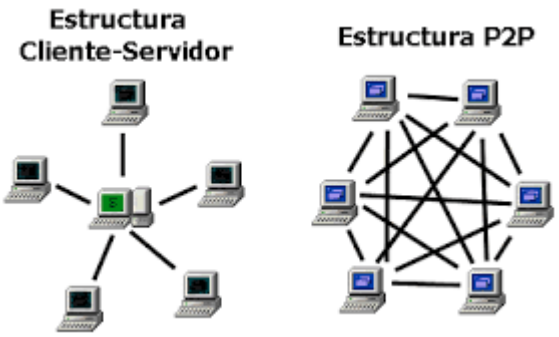

Figura 2. Estructura de los dos tipos de redes (Javier, s.f).

En las redes oscuras P2P podemos encontrarnos dos tipos diferentes, las conocidas como **redes P2P anónimas** y las conocidas como **amigo a amigo** (*friend to friend*) (Catá del Palacio, 2014)**.** Las primeras reciben ese nombre porque tanto sus usuarios como los nodos que emplean son pseudónimos, es decir, es necesario que los nodos tengan un pseudónimo para poder llegar a ellos, aunque en principio esto no influye en el anonimato de los *hosts*. Las segundas, por otro lado, son totalmente anónimas. Los usuarios sólo se conectan con equipos que previamente han sido conocidos. Este tipo de red permite la trasmisión libre de la información. Debido a cómo funciona Internet, ciertos grupos de personas están desarrollando redes en la red oscura fuera del control de este, generalmente en zonas limitadas y a través de Wifi consiguen montar una red paralela a Internet con una enorme capacidad para compartir información.

Según Catá del Palacio (2014) la red oscura P2P más utilizada se llama **Freenet.** Es totalmente anónima y distribuida, diseñada como un almacén de datos distribuidos por lo que se han construido sobre ella un gran número de programas y aplicaciones que permiten la publicación de una página web desde el anonimato, por ejemplo. Es prácticamente imposible e inviable eliminar un contenido, ya que la información como

se ha especificado antes está distribuida, lo cual es un verdadero problema cuando se tratan de archivos delictivos, como puede ser la pornografía infantil, que nunca dejará de estar accesible en esta red. Sin embargo, se trata de una gran herramienta cuando se quiere evitar la censura.

Freenet funciona de la siguiente manera. Cada nodo tiene una caché visible con información y la información que más se solicita es la más replicada. Cuando se accede a esta, se replica en todos los nodos que atraviesa hasta llegar al usuario que ha realizado la petición. Cuando un nodo se queda sin espacio para más información, se elimina la información que menos veces ha sido accedida. Su sistema de publicación es muy similar al tan conocido WWW. La información también está asociada a una clave que se requiere para acceder a un fichero, de la misma forma a la que se hace uso de una URL. Al estar todos los datos distribuidos, es imposible que los datos no estén accesibles a un ataque DoS. Freenet emplea un protocolo NGR (*Next Generation Routing)* que se adapta a la topología de la red o toma las decisiones de enrutamiento dependiendo de los tiempos de respuesta de los nodos y no de la cercanía.

El protocolo NGR funciona mediante nodos que contienen una lista de otros nodos conocidos iniciales a los que realiza las primeras consultas. Con cada petición de información, esta lista se amplia y almacena una lista de pares de nodos para mejorar la eficiencia. Entonces el protocolo supone que, si un nodo tiene información sobre un tema, tendrá más información similar. Las tablas de encaminamiento no se trasmiten a otros nodos. Cuando se recibe una petición pueden darse dos escenarios, si tiene la información, se envía a través de los nodos que han hecho llegar la petición. Si no la tiene, la reenvía al nodo con mayor probabilidad de tenerla. La Figura 3 ofrece una representación visual de cómo funciona esta red.

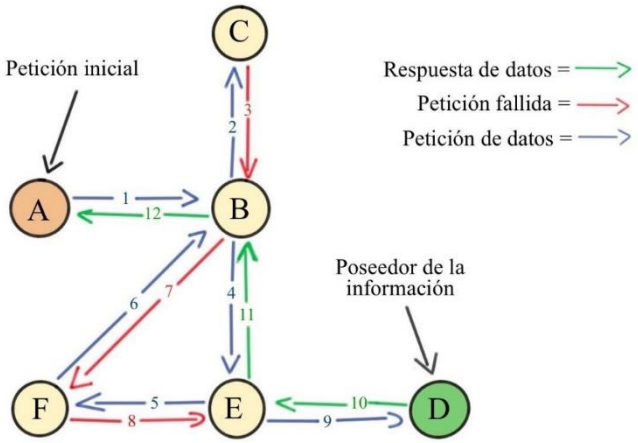

Figura 3. Estructura de Freenet. Elaboración propia.

Cuando se inserta un nuevo fichero, a este se le asigna una clave única GUID (*Global Unique Identifier*). La red utiliza dos tipos de clave:

- **CHK** (*Content-Hash Keys*)**:** está basada en sumas de verificación SHA-1 del contenido del fichero. Así, hay para cada fichero una clave única.
- **SSK** (*Signed-Subspace Keys*): Funciona de forma similar a una URL. En primer lugar, se generan dos claves, una privada y una pública. Luego se elige la descripción del fichero y se hace *hashing*[4] de la clave pública y de la descripción antes de unirlas y volver a hacer *hashing* de la suma.

Además, según Ferrer (2018) existen otros dos tipos de claves adicionales que se pueden emplear: USK (*Updatable Subspace Keys*) y KSK (*Keyworld Signed Keys*).

El problema con Freenet es que al no saber quién tiene los datos, se puede inundar de peticiones la red hasta que llegan al nodo adecuado, controlándolo con el tiempo de vida y la detección de bucles (si un nodo recibe la misma petición desde dos nodos distintos, le indica a uno de los dos que por ahí no va a encontrar los datos). Las actualizaciones de documentos antiguos pueden inundar la red con notificaciones y mensajes de actualización. Hay que recalcar que utilizar Freenet en sí no es ningún tipo de delito, pero como se ha explicado antes, puede ayudar a muchos delincuentes

[4] El *hashing* o función *hash* permite calcular la huella digital para poder identificar de forma inequívoca un archivo determinado (Pla, 2021). En este caso, con la función *hash* se localiza rápidamente el archivo solicitado.

a compartir archivos que sí pueden constituir delito, por lo que era necesario hablar de ella.

4.1.2 Compartición de material con copyright y derechos de autor

Una práctica muy extendida actualmente en nuestra sociedad, aunque quizá algo menos desde la aparición de servicios multimedia vía *streaming* como Netflix o Spotify, es la de descargar archivos multimedia como películas o canciones entre otras cosas. La gran mayoría de personas que viven en España ha descargado algo o conoce a una persona en su entorno familiar o social que lo haya hecho, aunque sea una sola vez, mediante páginas web o a través de programas como eMule y BitTorrent. Antes de entrar en materia sobre si esto es delito o no, se va a explicar que son y cómo funcionan estos dos programas, ambas redes P2P.

El programa **eMule** (Fernández, 2021a), coloquialmente conocido como "la mula" es una red P2P que emplea un sistema descentralizado, explicado en el apartado 2.4 de este trabajo. Es una aplicación de *software* libre y, por tanto, totalmente gratuita. Este programa emplea la red eD2K (eDonkeyNetwork o eDonkey2000) y la red Kad. La red eD2K es un sistema de intercambio P2P diseñado para proporcionar, a largo plazo, de disponibilidad de archivos de datos a largo plazo. Fue la red más utilizada por eMule (Portia, 2021). La red Kad, por otra parte, es una red de funcionamiento similar que se conecta a la red eDonkey, por lo que se podría decir que es una red de apoyo para un mejor funcionamiento de eMule. Se podría decir que eMule fue la aplicación que inició la fiebre por las descargas P2P en España, hace ya muchos años, concretamente en agosto de 2002 que fue cuando salió disponible para su descarga. Fue tan popular que no solo se convirtió en un imprescindible en el mundo P2P, sino que, al tener un código libre, se llegaron a crear otros programas derivados para poder llevarlo a otros sistemas operativos.

Para poder utilizar eMule, se necesita un cliente para la red de eDonkey y a través de ese cliente se conecta a uno de los servidores que existen, que son los que dan el acceso a la red completa, aunque no se comuniquen entre ellos. La conexión entre el servidor de eMule y el cliente se realiza por TCP[5], donde una vez accedida a él se obtendrán la información sobre los archivos que se estén buscando y los demás

[5] TCP son las siglas en inglés de *Transmission Control Protocol,* traducido al castellano como Protocolo de Control de Trasmisión. Permite que dos anfitriones se conecten e intercambien el flujo de datos, a la vez que garantiza la entrega de paquetes y de datos en el mismo orden que se enviaron (TCP, s.f).

clientes que los tienen en sus ordenadores. Entonces una vez pedida la descarga de un archivo, se utilizan conexiones TCP a otros clientes para descargarlo. Si otro cliente pide un archivo que tienes, te conectarás a él y se lo irás enviando. En la Figura 4 se muestra visualmente como se organiza la estructura de eMule.

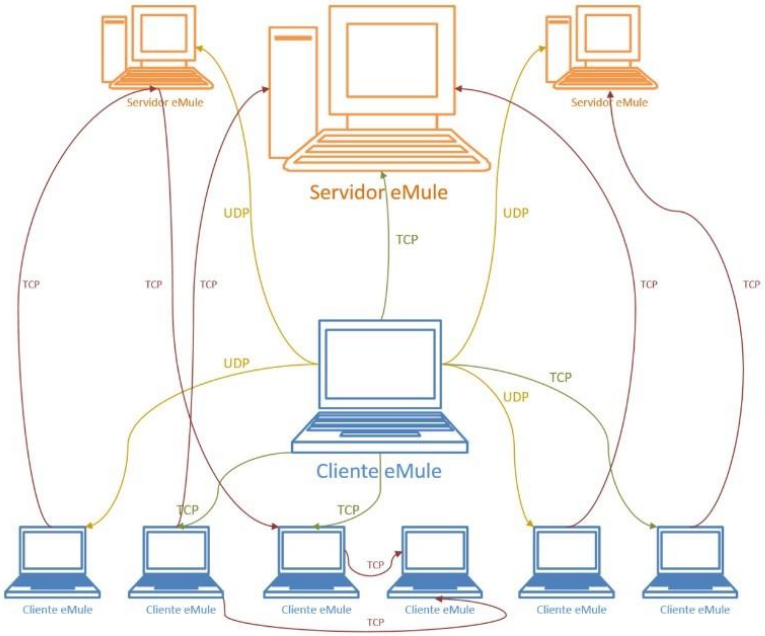

Figura 4. Estructura eMule (Fernández, 2021a).

Además, eMule acabó ofreciendo la posibilidad de conectarse también a las redes Kad o Kademlia, otra red totalmente descentralizada con la que también te conectas directamente a otros usuarios en busca de los archivos. Esto se traducía en más posibilidades y más flexibilidad para las descargas. Para finalizar, eMule también incluye una serie de elementos que ayudan a mejorar la experiencia general, como la incorporación de un buscador de archivos, un chat para hablar con otras personas del servidor, la posibilidad de añadir nuevos servidores de forma manual o incluso la de dejar comentarios en las descargas como si de un foro social se tratase.

BitTorrent (Fernández, 2021b) es otra red P2P muy conocida que se conecta a otros ordenadores de la misma forma que eMule para descargar el archivo que se busca. Cuanta más gente tenga ese archivo y lo esté compartiendo, más rápida irá la descarga. En primer lugar, se descarga un archivo *.torrent*, que, de forma coloquial, sirve de mapa para llegar hasta el archivo deseado. A continuación, tu cliente de BitTorrent se conecta a los clientes del resto de personas que posean el archivo y se descargarán varios de los fragmentos mientras que el cliente BitTorrent irá uniendo esos fragmentos y datos para poder utilizar el archivo descargado. Esto es posible

gracias a los ***trackers***, que organizan la distribución de un archivo y los que contienen la información necesaria para que los diferentes usuarios se conecten entre ellos. Los *trackers* son el único punto de encuentro al que los clientes deben conectarse de forma obligatoria. Existen varios tipos de *trackers*, cuantos más activos se tengan, a más redes de usuarios se podrá acceder y con ello se podrá descargar más rápido los archivos o encontrar nuevos.

Al comenzar la descarga, en primer lugar, el cliente de BitTorrent se conecta al *tracker* para pedirle información. Este proporcionara una lista inicial, escogida al azar, de usuarios con ese archivo que se ha buscado y se comenzará la descarga. El cliente irá completando el mapa conforme consiga más usuarios a los que conectarse. La información la reciben de dos tipos de usuarios, los ***seeders*** y los ***leechers***. Los primeros son aquellos que ya completaron la descarga y tienen la posibilidad de permanecer en el sistema tanto tiempo como deseen, facilitando así el proceso de otros usuarios. Los segundos se encuentran en la primera instancia, es decir, todavía están descargando contenido del sistema (Kozynsky et al., 2011). Sin embargo, ya tienen descargados algunos fragmentos de ese archivo, por lo que su programa hace que los compartan con el resto de los usuarios que forman parte de la red para acelerar la descarga. Teniendo en cuenta esto, para poder descargar un archivo completo es necesario que haya al menor un *seeder*. Si todos fueran *leechers*, siempre faltaría un fragmento que nadie tendría. Cuando se elimine el archivo de la carpeta donde se ha descargado o se apague el ordenador, se dejará de aparecer como *seeder* o *leecher* y dejará de participar en la red. En la Figura 5, a continuación, se puede apreciar visualmente cómo funciona la estructura de BitTorrent.

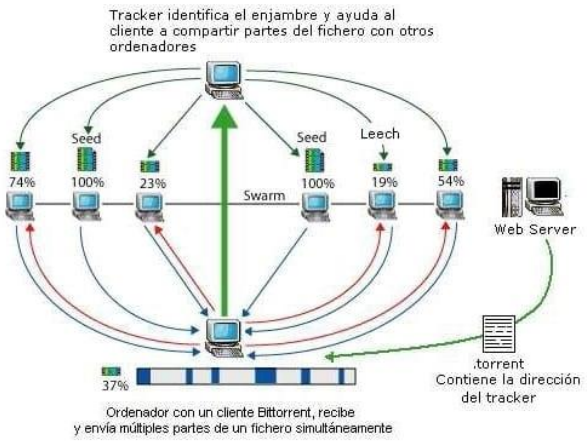

Figura 5. Estructura de BitTorrent (Wikipedia, s.f).

Terminado de explicar el funcionamiento de las dos redes P2P más utilizadas, abordaremos el tema principal de este apartado. ¿Es delito descargar películas, canciones y archivos que tienen copyright de una red P2P? La cuestión de legalidad o no legalidad de las descargas que provienen de redes P2P se redacta dentro del Real Decreto Legislativo 1/1996, de 12 de abril sobre la Propiedad Intelectual. A través de jurisprudencia menor se ha establecido que las redes P2P como concepto son meros medios de intercambio de archivos y que no vulnera este Decreto porque no hay ningún precepto que lo prohíba expresamente. Tampoco hay prohibición expresa alguna a las actividades que se realizan mediante dichas redes, que es el intercambio de archivos. Mientras las obras compartidas en las redes P2P no estén protegidas por el Derecho de Propiedad Intelectual, la protección bajo la que estaban deja de existir porque ha expirado el plazo de protección o bien obras cuya protección no fue confiada a la SGAE (Sociedad General de Autores y Editores). Se puede deducir que existe una necesidad de acotar aquellas obras protegidas y que comportamientos son los que pueden infringir el Real Decreto Legislativo.

El principal problema en esta materia se plantea cuando las obras compartidas por las redes P2P están bajo la protección de dicha norma. Para un sector de la doctrina, esto sigue sin suponer una vulneración de la norma porque quedan apoyados en el derecho de copia privada, siempre que no haya ánimo de lucro, en base al artículo 31.2 del Real Decreto Legislativo 1/1996: "*No necesita autorización del autor la reproducción, en cualquier soporte, de obras ya divulgadas cuando se lleve a cabo por una persona física para su uso privado a partir de obras a las que haya accedido legalmente y la copia obtenida no sea objeto de una utilización colectiva ni lucrativa* […]".

El conflicto viene pues, en delimitar el término copia privada y los intereses del autor de la obra. Según en lo dispuesto en el artículo anteriormente mencionado, no sería necesaria la autorización del autor para la descarga y la reproducción posterior de su obra, ya que las redes P2P no están prohibidas por la Ley y, por tanto, la descarga no es ilícita en los casos de copia privada. Pero de nuevo, en el Real Decreto no se determina el significado de copia privada o lucrativa, por lo que deben definirse esos conceptos. Del artículo 20 del mismo Decreto se puede interpretar que la copia privada es aquella que se utiliza en el ámbito doméstico: "*No se considerará pública la comunicación cuando se celebre dentro de un ámbito estrictamente doméstico que no esté integrado o conectado a una red de difusión de cualquier tipo".* Por tanto, si las copias que se han descargado de redes P2P son utilizadas fuera del ámbito doméstico

serian hechos ilícitos. Del mismo modo, si las copias son utilizadas con un fin lucrativo, también estaríamos ante un supuesto ilícito. Volveremos a tratar este tema en el apartado 5 de este trabajo.

4.1.3 Pornografía infantil

La facilidad de compartir archivos entre los usuarios que proporcionan las redes P2P, como ya hemos explicado en diversas ocasiones a lo largo del trabajo, hace que sea un lugar fructífero para los consumidores de pornografía infantil. La pornografía infantil es definida por distintos organismos de la siguiente manera (Picón, s.f.):

El Consejo de Europa la definió como "*cualquier material auditivo o visual en el que se emplee a un menor en un contexto sexual".*

La Directiva 2011/93/UE la define como "*imágenes de abusos sexuales a menores, y otras formas especialmente graves de abusos y explotación sexuales de la infancia"*.

En el Preámbulo de la LO 1/2015, de 30 de marzo, se cita: *"Se presta especial atención al castigo de la pornografía infantil. En primer lugar, se ofrece una definición legal de pornografía infantil tomada de la Directiva 2011/93/UE, que abarca no sólo el material que representa a un menor o persona con discapacidad participando en una conducta sexual, sino también las imágenes realistas de menores participando en conductas sexualmente explícitas, aunque no reflejen una realidad sucedida"*.

El Tribunal Supremo en sentencias como la de 5 de febrero de 1991, define "pornografía" como "*se trataba en suma de material capaz de perturbar, en los aspectos sexuales, el normal curso de la personalidad en formación de los menores o adolescentes*".

Los peligros que suponen el fácil acceso a estos materiales en las redes P2P son varios y de distinta índole. En primer lugar, aquellos usuarios que tengan curiosidad por este tipo de archivos pueden satisfacer su curiosidad fácilmente, y el hecho de que sea relativamente fácil encontrar estos archivos puede hacer parecer la situación como algo normal y aceptable. Además, aquellos que no pretendían convertirse en traficantes de pornografía infantil, puedan serlo después de encontrar el material en la red (Wolak et al., 2013).

También este fácil acceso contribuye al esparcimiento de la pornografía infantil en Internet (Bissias et al., 2016): cada vez que uno de estos archivos es descargado se crea una nueva copia que permanece en las carpetas compartidas, incrementando la

cantidad de archivos disponible en la red. Al compartirse y descargarse, estos archivos se duplican de forma continua y constante. Los resultados obtenidos por Wolak et al. (2013) indican una generalización del tráfico de pornografía infantil de baja entidad (con menos de 10 archivos) en estas redes, siendo menos del 1% la cantidad de ordenadores que compartieron grandes cantidades de archivos (100 o más). Sin embargo, la detención de los responsables de estas contribuciones grandes y la retirada de sus archivos de la red podría reducir hasta el 30% de los archivos disponibles en la red P2P.

El Código Penal español es muy claro a la hora de castigar los delitos referentes a la pornografía infantil, abarcando toda acción que involucre estos actos lo cual hace que, junto a la dificultad de localizar a estos usuarios, el principal problema con las redes P2P en este ámbito es la distribución del contenido cuando no se sabe que este es material ilícito. Un claro ejemplo sería un padre que descarga lo que él cree que es una película de dibujos animados cuando en realidad es un video de pornografía infantil y deja el ordenador en marcha, descargando el archivo y luego compartiéndolo con otros usuarios. En el apartado 5 de este trabajo, ahondaremos más en estos casos.

4.2 Detección del delito en redes P2P.

Como ya se ha explicado a lo largo del trabajo, la naturaleza de las redes P2P hace que sea más complicado detectar a los usuarios que cometen actos ilícitos. Es más fácil detectar SMS, correos electrónicos e IPs asociadas a estos, o usuarios en foros públicos que a usuarios de redes P2P. En cuanto a la detección de los tres tipos de delito en redes P2P que hemos explicado durante el apartado 4.1 del trabajo, el único que cuenta con un método de rastreo es el de pornografía infantil.

El uso de Freenet u otras redes P2P de la internet oscura no constituye un delito en sí, siendo el delito las acciones que se realicen a través de esta, que en la mayoría de los casos son archivos de pornografía infantil. La compartición de datos y derechos de autor tampoco constituye un ilícito penal como bien se ha explicado anteriormente (en el siguiente apartado se hablará si puede constituir o no un ilícito civil) salvo en los casos donde se comparta con ánimo de lucro o se emplean fuera del uso doméstico donde en ambas situaciones, quedan fuera de las redes P2P y permite un seguimiento más tradicional alejado de estas. Por ejemplo, el que descargue una película para montar un cine clandestino o ilegal y lucrarse, la policía solo tiene que personarse en el local, no es necesario gastar numerosos recursos en rastrear redes P2P, la

procedencia de la película sea red P2P o descarga directa a través de una página web (que no es P2P) es irrelevante, serían el mismo tipo de delito.

Sin embargo, el delito más grave, el de pornografía infantil, sí que cuenta con un método de detección (Soldino y Guardiola, 2017). La policía a la hora de identificar quienes están cometiendo la difusión de archivos ilícitos emplea *softwares* como "*Gnuwatch"* para geolocalizar e identificar las IPs de los consumidores o "*Florencio"* para identificar las redes de intercambio de archivos (Jiménez-Serrano, 2012). En Estados Unidos se emplean otros programas como "*RoundUp, Gridcop o Ephex"* que utilizan el valor *hash* de los archivos identificados como pornografía infantil de investigaciones anteriores para analizar el tráfico de este tipo de archivos y localizar las direcciones IPs, la fecha, el tiempo durante el que se ha compartido… (Wolak et al., 2013). Sin embargo, esto solo rastrea los archivos que ya han sido identificados y no permite localizar archivos nuevos, hasta que se detenga a un consumidor que haya descargado o compartido algún archivo identificado y este posea archivos no identificados, lo cual permitirá a la policía poder rastrear también su huella digital, el identificador único de cada archivo definida proporcionada por la función *hash* (Kaspersky, 2022).

En diciembre de 2021, el Cuerpo Nacional de Policía detuvo a siete personas por tenencia y distribución de pornografía infantil. La investigación se inició en marzo del mismo año, donde se realizó un rastreo en las redes P2P y se identificaron nueve direcciones IP desde donde se distribuían ese contenido. En el registro se incautaron miles de archivos de video y fotografía, algunos de una dureza extrema por la corta edad de los menores (Santiago, 2021).

5. Delitos en redes P2P y legislación española

Como ya se ha visto a lo largo de este trabajo, la normativa española no castiga el uso de las redes P2P. Las redes P2P por si solas no constituyen ningún tipo de delito, el delito es la acción que se puede realizar a través de estas redes. En general, los delitos informáticos son castigados como sus contrapartes tradicionales debido a que el derecho penal no puede avanzar al mismo ritmo que la tecnología informática. Por ejemplo, un delito de estafa informática se castiga como un delito de estafa tradicional. En este apartado vamos a ver como se castiga en España los dos delitos mencionados anteriormente: la compartición de material con copyright y derechos de autor y la pornografía infantil.

El Código Penal español castiga en sus artículos 270.1 lo siguiente:

"Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios"

El legislador pide como requisito indispensable que el autor tenga el ánimo de obtener un beneficio económico directo o indirecto, por lo que en el caso de las redes P2P, tal y como hemos visto en el apartado 4.1.2 de este trabajo, no es delito. El Real Decreto Legislativo 1/1996 anteriormente mencionado especifica que las personas tienen derecho a tener una copia de un archivo, por lo que, al descargarlo y compartirlo, sin ánimo de lucro, no se considera un ilícito penal.

Ahora bien, sí que puede constituir un ilícito civil. Cuando se está descargando una obra se está compartiendo a su vez, vulnerando los derechos de autor de esa obra, por lo que podría pedir responsabilidades por la vía civil. La principal dificultad de esto es que es necesario identificar a esos usuarios y para ello, hay que encontrar la IP de la persona que está descargando o compartiendo el archivo y a su vez quien posee el nombre de la persona a la que está asociada esta dirección IP son las operadoras telefónicas, que no pueden proporcionar esta información (González, 2017).

En definitiva, compartir o descargar películas en redes P2P no es delito penal, pero puede ser un ilícito civil, aunque es muy improbable que el usuario sea demandado. Solo es delito penal si se hace con ánimo de lucro o de obtener un beneficio económico.

En cuanto a la pornografía infantil, como se ha dicho anteriormente, el código penal es muy claro en las acciones que se castiga. El artículo 189.1 del Código Penal dice así:

Será castigado con la pena de prisión de uno a cinco años:

a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

El apartado b abarca una gran cantidad de acciones con la que se comete el delito, incluido el verbo **distribuir**, que es lo que se realiza en las redes P2P al descargar el archivo. Por otro lado, el artículo 189.5 dicta lo siguiente:

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

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

Mención especial al término "**a sabiendas"**, que supone una ventana de salvación para la gente que descargue estos archivos por error. Como podemos observar, la mera posesión de este tipo de material es un delito penal, aunque ha habido casos en los que el autor del hecho lo descargó por error y han de demostrar que la descarga fue accidental, atendiendo al número de archivos descargados o si el nombre del archivo podía inducir a error como pueden ser "recetas de cocina" o "Shrek 2", justificando así la no aplicación del artículo, ya que no sabían lo que estaban descargando (Asuntos Penales, 2022).

Lo mismo sucede con la distribución. Si bien no especifica el término a sabiendas e implica que quien comete la acción de distribuir, comete el delito, en estos casos en los que por error se ha descargado los archivos y el ordenador los comparte de forma automática con otros usuarios, se suele no castigar a los acusados, pues no son conscientes de lo que están compartiendo. Ahora bien, suele ser un proceso largo y tardío demostrar que todo fue por error y puede afectar a la vida personal del sujeto. (Picón, s.f).

6. Conclusiones

PRIMERA: La tecnología evoluciona y avanza a un nivel vertiginoso proporcionándonos numerosas ventajas, pero también en manos de delincuentes, abre la puerta a nuevas y numerosas formas de cometer delitos de distinta índole como las estafas, el robo de datos o el ciberacoso.

SEGUNDA: Las redes P2P son un tipo de red muy interesante debido a que contradice el modelo servidor-usuarios, siendo las redes P2P una conexión entre usuarios y con un modelo de comunicación horizontal y no vertical como había sido antes de la aparición de estas. Tienen un alcance mundial y es difícil de rastrear, por lo que es un sistema empleado por muchos ciberdelincuentes.

TERCERA: Los ciberdelitos pueden ser delitos tradicionales que se realizan a través de los ordenadores y la informática o delitos nuevos que surgieron junto ambos conceptos, como pueden ser los malware. Son delitos más peligrosos que los tradicionales debido a que tienen la posibilidad de abarcar a muchas más personas en cuestión de segundos. Están muy poco tipificados debido a que aparecen nuevas técnicas y delitos a un ritmo más veloz que del que el Derecho puede alcanzar.

CUARTA: Existen diversas redes P2P, tanto en la internet visible como en la internet profunda u oscura. Los usuarios normalmente emplean redes como eMule y BitTorrent, en la internet visible, para poder descargar películas o música, pero en las redes P2P de la internet oscura, los ciberdelincuentes comparten archivos ilícitos de forma muy sencilla.

QUINTA: Compartir y descargar archivos con derechos de autor y copyright no es un ilícito penal, pero puede constituir un ilícito civil. El principal delito cometido a través de redes P2P es la pornografía infantil debido a la facilidad que supone las redes P2P para la compartición de archivos. Además, no solo los ciberdelincuentes comparten los archivos debido a que puede haber personas que por equivocación descarguen un archivo ilícito de este tipo y lo compartan a su vez, convirtiéndose así en sujetos activos del delito.

SEXTA: La jurisprudencia y el ordenamiento jurídico español castiga los delitos cometidos a través de las redes P2P, que no el uso de las redes P2P pues esto no es delito, como si se tratasen de delitos tradicionales, rastreando la policía los archivos de pornografía infantil por su huella digital para poder identificar y detener a los consumidores de estos archivos. Sin embargo, esto solo es posible hacerlo con los archivos previamente localizados de anteriores detenciones u operaciones, por lo que

un gran contenido de pornografía infantil sigue en la red sin poder identificarse. Se debería de encontrar una forma de poder hacer frente a esta problemática, pues es uno de los métodos de difusión de pornografía infantil más usados del mundo.

7. Bibliografía

Alvarado, M. A. (2017). Aspectos legales al utilizar las principales redes sociales en Colombia. Revista Logos Ciencia & Tecnología, 8(2), 211-220. https://doi.org/10.22335/rlct.v8i2.315

Álvarez, J., Chinea, J. y García, V. (2018). Un paseo por la Deep Web. [Trabajo Fin de Máster, Universitat Oberta de Catalunya]. Repositorio Institucional (O2). http://hdl.handle.net/10609/89549

Asuntos Penales. (8 de marzo de 2022). *Preguntas Frecuentes sobre el delito de pornografía infantil*. Información Legal. Diario de Información Jurídica y tribunales. https://www.informacionlegal.es/delito-de-pornografia-infantil/

Biddle, P., England, P., Peinado, M., & Willman, B. (2002). The darknet and the future of content distribution. *ACM Workshop on digital rights management*, *6*, 54-70.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H. & Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child Abuse & Neglect*, *52*, 185-199

Buttle, F. & Arlette, C. (2002). *Napster*. [MGSM Case Studies in Management]. Macquarie Graduate School of Management.

Cantos, A. (2020). Red P2P centralizada para el streaming de vídeo almacenado. [Trabajo Fin de Grado, Universitat Politècnica de València]. Library. https://1library.co/document/yn4lkm1z-red-p-p-centralizada-streaming-video-almacenado.html

Catá del Palacio, A. (2014). *Ciberdelincuencia. Desarrollo y persecución tecnológica*. [Trabajo Fin de Grado, Universidad Politécnica de Madrid]. Archivo Digital UPM. https://oa.upm.es/34795/

Cordero, N. F. (2021). *La ciberdelincuencia*. [Trabajo Fin de Máster, Universidad de Alcalá]. Biblioteca Digital Universidad de Alcalá. http://hdl.handle.net/10017/49563

Cruz, J.E. (2009). *El avance tecnológico*. http://www.rvcmar.org/otros/mapasc/JCR_EL_AVANCE_TECNOLoGICO.pdf

CurioSfera. (s.f). *Historia del P2P: Origen e inventor*. CurioSfera. https://curiosfera-historia.com/historia-del-p2p-inventor/

De Urbano Castrillo, E. (2011). Los delitos informáticos tras la reforma del CP de 2010. *Revista Aranzadi Doctrinal*, *6*, 163-176.

Duarte, G. (julio de 2015). *P2P (Peer to peer)*. Definición ABC. https://www.definicionabc.com/tecnologia/p2p-peer-to-peer.php

Esparís, M. (24 de abril de 2020). *Ciberdelincuencia: Los 4 delitos informáticos más comunes*. Sistemius. https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos/

Fernández, Y. (8 de febrero de 2021a). *Qué es eMule, cómo funciona, cómo empezar a utilizarlo*. Xataka. https://www.xataka.com/basics/que-emule-como-funciona-como-empezar-a-utilizarlo

Fernández, Y. (8 de febrero de 2021b). *BitTorrent: qué es y cómo funcionan los torrents*. Xataka. https://www.xataka.com/basics/bittorrent-que-como-funcionan-torrents

Ferrer, X. (2018). Un paseo por la Deep Web. [Trabajo Fin de Máster, Universitat Oberta de Catalunya]. Repositorio Institucional (O2). http://hdl.handle.net/10609/89425

García, J. (31 de agosto de 2019). *Napster: inicio, auge y caída del servicio que puso en jaque a la industria musical*. Xataka. https://www.xataka.com/historia-tecnologica/napster-inicio-auge-caida-servicio-que-puso-jaque-a-industria-musical

González, M. (30 de marzo de 2017). *Usuarios que descargan por P2P, uploaders y páginas de descargas: ¿qué es delito y qué no?* Xataka. https://www.xataka.com/legislacion-y-derechos/descargar-archivos-p2p-no-es-delito-y-aunque-pueda-ser-una-infraccion-civil-es-improbable-que-te-demanden

Javier. (s. f.). *Redes P2P y Redes Cliente-Servidor*. Hardware, Software y Redes 4 ESO. https://informatica4esog2.jimdofree.com/redes/redes-p2p-y-redes-cliente-servidor/

Jiménez-Serrano, J. (2012). Tráfico de pornografía infantil: Dinámica, roles y prevención. *Gaceta Internacional De Ciencias Forenses*, *5*, 33-41.

Kaspersky. (20 de abril de 2022). *¿Qué es una huella digital? ¿Cómo podemos protegerla de los hackers?* Kaspersky. https://latam.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

Kozynski, F., Ferragut, A. & Paganini, F. (2011). Reducción de oscilaciones en BitTorrent mediante mecanismos de *unchoking* preferencial. *Porto Alegre*, *14*(1), 29-41.

Los Santos. A. (2009). *Revisión de sistemas P2P*. http://www.albertolsa.com/wp-content/uploads/2009/07/arquitecturaderedes-revision_de_sistemas_p2p-albertolossantos.pdf

Nicolini, A. L. (2017). *Aplicación de mecanismos reactivos y argumentativos para la búsqueda temática en redes P2P*. [Tesis doctoral, Universidad Nacional del Sur]. Repositorio Institucional CONICET Digital. http://hdl.handle.net/11336/95606

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming”. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso XLI, 2, 211-262.

Picón, E. (s. f.). *Claves para la defensa por distribución de pornografía infantil a través de redes peer-to-peer o P2P*. https://peritoinformatico.es/claves-defensa-acusacion-pornografia-infantil/

Pla, F. (2021). Apuntes de la asignatura "Seguridad y Criminalidad Informática", Universitat Jaume I, documento inédito.

Portia. (11 de enero de 2021). *Red edonkey (ed2k)*. Techinfo. https://techinfo.wiki/red-edonkey-ed2k/

Pozas, J., Morales, T. y Martínez-Vilchis, R. (2018). Efectos de un programa de ciberconvivencia en la prevención del cyberbullying. *Psychology, Society, & Education*, *10*(2), 239-250.

Rodríguez, P. (16 de febrero de 2012). *Métodos para compartir archivos y contenidos en Internet (III): P2P, el auténtico espíritu del file.* Xataka móvil. https://www.xatakamovil.com/conectividad/metodos-para-compartir-archivos-y-contenidos-en-internet-iiip2p-el-autentico-espiritu-del-file-sharing

Santiago. (10 de diciembre de 2021). Una operación contra la pornografía infantil en Galicia se salda con siete detenidos. *El Periódico de Aragón*. https://www.elperiodicodearagon.com/sucesos/2021/12/10/operacion-pornografia-infantil-galicia-salda-60528806.html

Soldino, V. y Guardiola, J. (2017). Pornografía infantil: cambios en las formas de obtención y distribución. *Revista Electrónica de Ciencia Penal y Criminología*, *19*, *19-28*.

TCP. (s.f). Mdn web docs. https://developer.mozilla.org/es/docs/Glossary/TCP

Wikipedia. (s.f). *BitTorrent*. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/BitTorrent

Wolak, J., Liberatore, M., & Levine, B. N. (2013). Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect*, *38*(2), 1-10. 10.1016/j.chiabu.2013.10.018

LEYES MENCIONADAS

Directiva 2011/93/UE.

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

LO 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.