Trabajo Fin de Grado

Criminología y Las Nuevas Tecnologías

Presentado por:

Noelia Ramírez Perea

Tutora:

Marta Guinot Martínez

Grado en Criminología y Seguridad

Curso académico 2019/20

Índice

Extended summary

Evolution is part of the life of human society, without innovation, our means of transport par excellence, would still be horses. Nevertheless, any change has consequences, which will normally be both negative and positive, ideally the benefits outweigh the disadvantages. This paper discusses the progress that new technologies have made in our daily lives, but focuses on the point of view of criminals, now known as cybercriminals.

In order to study the problem of cybercrime, it is essential to have knowledge of Criminology, which focuses on analyzing everything that involves a crime, such as the offender, the victim, social control and the crime itself. With this information it manages to prevent the commission of crimes, while explaining it, without forgetting the intervention of the criminal. Although it seems that Internet crime is something totally new, we have to remember that the basis of many of the offences are exactly the same, already known by Criminology. The difference lies in the profile of the cybercriminal, but above all in the method by which it is carried out, which is none other than the network and the computer devices that contain it.

Despite the fact that some of the new technologies could already be classified as old because they have been living in our homes for more than two decades, Spanish legislation only began to contemplate them in 2010 to add the rest in the reform of 2015. The trigger was the Convention on Cybercrime on 23 November 2001 in Budapest, which was ratified by Spain ten years ago. At present, there are many articles that condemn illegal cyber actions based on the protected legal good, ie, in each crime that has a computer figure, has been included a new article or paragraph. This crime is really broad and therefore includes several titles of the Criminal Code, from crimes against freedom to crimes against heritage and socio-economic order. Some examples are cyberstalking (freedom); cyberbullying (moral integrity); childgrooming, distributing pornography for profit and producing pornography with or without economic benefit (sexual freedom and indemnity), sexting and hacking (privacy, right to one's own image and inviolability of the home), computer fraud and computer sabotage (heritage and socio-economic order).

All the above-mentioned cybercrimes can be classified into two groups. The first group includes those crimes that are typical of new technologies and that could not be committed before the existence of these tools, considered as new forms of criminality.

This group includes hacking, which is the action of entering a computer system without the owner's authorization, and always with an illicit purpose such as obtaining bank passwords, although there are also white hat hackers who use cyber security to prevent these actions, protecting the web pages. Very similar to this is sabotage, which differs from hacking because the aim is not to enter the device, but to prevent the information it possesses from being used again, either by deleting, changing or destroying the data. To close this group, there is sexting, a very common behavior in recent years, which is based on sending photographs or videos of a sexual nature to someone and that person decides to spread them without victim`s permission.

On the other hand, there are the crimes that have passed from the physical world to the virtual world, and now, apart from existing as crimes, they are also like cyber crimes, they would be the classic forms of criminality that have been computerized. At this point is the cyberstalking, which is the harassment but led to the network with behaviors such as excessive sending of unnecessary emails or create false profiles on social networks. There is also pornography, which nowadays through the Internet has managed to be sent to millions of people in a few minutes, while creating it without the need of a minor, just with a computer program. Finally, fraud has also joined the cybercrimes and although trickery remains its main feature, it has developed new techniques such as phishing, pharming, or extortion.

However, cybercrime does not only affect the elderly, but also attacks the younger population, because they are the generations that have more knowledge about new technologies, since most have grown up with mobiles, computers, tablets and internet at home, and some even have them at school or high school. This has made them able to learn in a more interactive and fun way, but on the other hand has led many of them to become cyber-aggressors and others to become cyber-victims, but not only among minors, but there are adults who use the innocence of youth to take advantage of them. This can be seen in cyberbullying, which is known as bullying between equals, but it also takes place on the Internet, and on many occasions in both worlds, in the virtual and physical worlds, with the bullying continuing practically 24 hours a day. Victims of

bullying suffer much more nowadays, because before social networks, they knew that when they left school they were free, and until the next day no one was going to insult them, but today they have no such comfort, because when school is over, bullying becomes cyberbullying. Their main tools are flaming, harassment, denigration, impersonation, outing and trickery, exclusion and cyberstalking. Although it may seem that turning off the mobile phone is the end of it, this continuous harassment damages the cybervictims excessively, producing from feelings of fear and sadness, to low self-esteem and school performance.

In contrast, there is childgrooming, a cybercrime in which minors only play an unpleasant victim role. It consists of an adult contacting a teenager pretending to be a minor who shares similar tastes, has a good physique or a similar age, in order to get their attention, and thus gain their trust. Trust is the basis of this cybercrime, since the aggressor needs it so that he does not suspect him and achieve his goal. The purpose will always be a physical encounter that the adult will use to sexually assault or abuse the child, but to get to this point, it is required that the child falls into his trap and turn on the webcam or send some picture of a sexual nature (sexting), so the cybergroomer has something very valuable of the teenager with blackmail, and that to avoid being published will do everything he asks, even if it is to stay in the real world.

Cybercrime, despite being within habitual crime, has some characteristics that make it much more problematic than what we are used to, as much for the police as for the justice system, without forgetting the damage it causes to the cyber victims.

The problems begin with the possibility of committing a crime in one country while being physically in another, that is, they have been transformed and are now international crimes. Thanks to the internet we can talk to relatives living on other continents, as criminals can also use this tool to do illegal things at a distance, because, unlike a robbery, they do not need to leave home to hack into a person. Along with transnationality, there is the issue of legislation, which adds a further inconvenience, since there is no joint law for all the countries of the world, so when it happens that a person commits a cybercrime from Spain that affects Canada, it is very likely that he or she will not be convicted, due to the existing problem of jurisdiction, which makes it complicated to extradite, as well as to prosecute in the country itself.

In addition, there is the question of anonymity. This is an important detail, since through fingerprints or facial recognition it is possible to identify a person if their information is in the database, but with an IP it is not the same, because its location requires a much longer process and there are the barriers of nicknames that facilitate hiding the identity of the subject, especially in social networks and public chats.

It is also a much cheaper option that requires less preparation to carry out. This is because of the few materials needed, only a device such as a computer and an Internet connection, which can be obtained free of charge at a public library or an Internet café. That is why it is more cost-effective, since you do not have to make an investment in weapons or hire professional criminals or even be physically well. Furthermore, the only thing required are the cybercriminal's computer skills, which are very easy to acquire through courses, books or even the university, in the case of more complex cybercrime such as hacking or sabotage.

As the Internet is present in almost every area of the world, with a few exceptions, it increases the number of users who can continue a cybercrime that was started by someone else, creating a chain that expands from one city to a country, and from there to another continent. The consequence is that people totally unknown to the cyber victim can cyberstalk her and publish their opinions about her, while in a bullying crime, at most it would spread in that institute. Besides reaching more people, they also have a very fast diffusion, making that in a few hours, a whole country could have been swindled or could have visualized the intimate and private photos of a girl who is suffering from sexting. The consequence of this last example is that these images, even if they manage to be removed from a social network, will always be present on the Internet, because cybercrime is characterized by being permanent, since any user has been able to make a capture of that picture or download it, and that allows you to publish it again later.

Nevertheless, Criminology has decided to take advantage of new technologies in its favour and use them to improve its investigations. Among the techniques that have been developed thanks to ICTS is geoprevention, the most popular worldwide, as many countries make use of it. It involves analysing when and where crimes occur, inputting them into a computer program, and this will create a series of hot spots that indicate where and when more police should be present. It also looks at how cities are

built from their entertainment venues to drug trafficking sites, to provide the most dangerous areas with security measures. The aim is to anticipate crime, so that it can be prevented.

Another tool with the same objective is the prediction of crimes by means of Artificial Intelligence which, through surveillance cameras and data collected from citizens, allows authorities to be alerted if a person considered dangerous buys a weapon or changes clothes several times to go unnoticed and mislead investigators.

Finally, the last two techniques are related to Criminalistics, an area of criminology that focuses on obtaining evidence from the scene of the crime in order to discover what happened and who was responsible, and then providing all this data to the court so that it can deliver a fair sentence. The first focuses on the reconstruction of the crime scene, with two purposes. On the one hand, the aim is to obtain as many images of the scene as possible to study them later in the laboratories thanks to drones and 3D technology, since in certain areas such as railway tracks or a road, work is being done against the clock to clear the area as soon as possible so that the rest of the public can continue with their routine. On the other hand, cameras and sensors are used to recreate what happened in this scenario based on the evidence obtained, so that it can be shown visually in the trial, and this will help to pass sentence. The second and last tool is virtopsy, a technique used in forensic medicine instead of the traditional autopsy, which avoids opening the body, since the procedure is done by means of magnetic resonance and radiology. Once done, the data is entered into the computer and it creates a virtual image of the interior of the body, allowing the desired areas to be enlarged for better analysis, which leads to a better determination of the cause of death.

Resumen

Nuestra vida ha cambiado, se ha desplazado al llamado mundo virtual creado gracias a las nuevas tecnologías, y si actualmente nos comunicamos con nuestras amistades mediante redes sociales o adquirimos productos a través de Internet, es lógico pensar que los delincuentes también hayan sustituidos los delitos físicos por los cibernéticos. De acuerdo con las estadísticas, es un hecho que cada año aumentan los casos de ciberdelincuencia, pero estos datos no se limitan únicamente a España, sino que se extrapolan al resto de naciones del mundo, por lo que nos encontramos

ante una problemática global que, en la actualidad, resulta imposible de frenar. Es por ello que los cibercriminales están abarcando, cada vez más, las distintas tipologías delictivas reguladas en el Código Penal, desde el patrimonio hasta la libertad e indemnidad sexual. No obstante, aunque este fenómeno se presente como un reto para la justicia por sus beneficios como el anonimato o su rápida expansión, la Criminología también está haciendo uso de éstas tecnologías optimizando así sus recursos, lo cual se traduce en un perfeccionamiento de la ciberprevención. Por lo tanto, el objetivo del presente trabajo de final de grado es realizar un análisis de los distintos ciberdelitos, consistente en el estudio de su tipificación legal, explicación de sus características y problemática, junto con una investigación de cómo la Criminología está aplicando las nuevas tecnologías a su campo, para así poder formular una serie de posibles mejora.

Palabras clave: Criminología, nuevas tecnologías, ciberdelincuencia, España, prevención, cibervíctimas.

Abstract

Our life has changed, it has moved to the so-called virtual world created by new technologies, and if we currently communicate with our friends through social networks or purchase products through the Internet, it is logical to think that criminals have also replaced physical crimes with cybercrimes. According to the statistics, it is a fact that every year the cases of cybercrime increase, but these data are not limited only to Spain, but are extrapolated to the rest of the nations of the world, so we are facing a global problem that, at present, is impossible to stop. That is why cyber-criminals are increasingly covering the various types of crime regulated by the Criminal Code, from property to sexual freedom and compensation. However, although this phenomenon is presented as a challenge for justice because of its benefits such as anonymity or its rapid expansion, Criminology is also making use of these technologies, thus optimizing its resources, which translates into an improvement in cyber prevention. Therefore, the objective of this final degree work is to carry out an analysis of the different cybercrimes, consisting of the study of their legal classification, explanation of their characteristics and problems, together with an investigation of how Criminology is applying new technologies to its field, in order to formulate a series of possible improvements.

Keywords: Criminology, new technologies, cybercrime, Spain, prevention, cybervictims.

1. Introducción

El término Criminología ha sido definido por varios autores a lo largo de su evolución. Fue mencionado por primera vez por Topinnard, seguido de Garófalo, Von List, Mezger o Redondo entre otros, pero la mejor definición la desarrolló García Pablos de Molina quién estipuló que la criminología es "una ciencia empírica e interdisciplinar, que se ocupa del delito, el delincuente, la víctima y del control social del comportamiento delictivo; y que trata de suministrar una información válida, asegurada, sobre la génesis y dinámica del problema criminal y sus variables; sobre los programas y estrategias de prevención eficaz del delito; y sobre las técnicas de intervención positiva en el hombre delincuente[1]". En resumen, la Criminología se caracteriza por su uso de un método empírico e interdisciplinario, el cual le permite estudiar su objeto de estudio, que es la víctima, delincuente, delito y control social, logrando así explicar y prevenir el delito, a la vez que intervenir con el delincuente.

Por otra parte, el concepto nuevas tecnologías y las TICS[2] es mucho más reciente y se relaciona con la multimedia, redes sociales, internet, comunicación etc. En otras palabras, son los avances, novedades y aplicaciones en el ámbito tecnológico.

La creación y el desarrollo de Internet ha dado lugar a la aparición de un mundo virtual, con ciertas similitudes con el real, pero a la vez con un gran potencial en relación con los comportamientos delictivos. Desde hace años, se ha ido observando cómo la delincuencia se ha ido extendiendo por el espacio cibernético y han empezado a cometer delitos mediante internet y redes sociales. Sin embargo, al inicio, la criminalidad más básica se reducía a dañar los sistemas informáticos, de ahí que su primera denominación fuese "delitos informáticos". En cambio, cuando la finalidad era acceder sin autorización a un dispositivo electrónico (móvil, ordenador, tablet…) o evitar el acceso de una persona legitimada, recibe el nombre de "ciberdelincuencia pura"[3]. Prueba del aumento de los delitos cibernéticos y de la preocupación de las distintas naciones por este tema fue el Convenio sobre Ciberdelincuencia hecho en Budapest el 23 de noviembre de 2001.

[1]García-Pablos de Molina, A. (1989). La aportación de la Criminología. *Eguzkilore, Cuaderno del Instituto Vasco de Criminología*. Número 3,P.79-94.
[2] Tecnologías de la Información y la Comunicación.
[3] Extraído de Interpol. Enlace https://www.interpol.int/es/Delitos/Ciberdelincuencia

A lo largo de la historia de la criminalidad en internet, se ha ido vislumbrando como la ciberdelincuencia se podría agrupar en dos grandes clasificaciones, en función si este hecho delictivo existía antes o no. En otras palabras, la estafa ya se tipificaba en el Código Penal antes de la llegada de internet, por lo que la ciberestafa es el mismo delito, pero usando las nuevas tecnologías. En oposición, el hacking sin un ordenador no sería posible, ya que es necesario para introducirse en otro aparato electrónico. No obstante, este tema se desarrollará en los próximos capítulos.

También se debe mencionar hasta qué punto las víctimas de las nuevas tecnologías facilitan o motivan la comisión del delito, ya que a través del contenido que publican a diario en las redes sociales, comparten datos personales que, en ocasiones, derivan en una tragedia. Un claro ejemplo de ello ocurrió en Australia, donde una adolescente subió a su perfil de Facebook una foto contando una gran cantidad de dinero, y eso hizo que dos ladrones entraran en su casa por la noche a robar. Afortunadamente, la chica no se encontraba en casa y el dinero le pertenecía a su abuela, por lo que la cantidad robada fue mínima. No obstante, gracias a esa publicación y otras en las que constaba su dirección, los ladrones supieron la casa en la que tenían que entrar[4]. Al igual que le ocurrió a una pareja londinense que subieron a su perfil que se mudaban de su casa actual y un grupo de ladrones se hicieron pasar por los transportistas, consiguiendo así todo el mobiliario[5]. Un último caso, más trágico, fue el de Matthew Pyke[6], quien, con su novia Joanna Wilton, creó una página web sobre videojuegos, y a través de ella conoció al que en un futuro se convertiría en su asesino, David Heiss. Todo comenzó como un hobbie, sin embargo, Heiss se enamoró de Wilton, haciendo que ésta se distanciara y que Pyke tomase medidas como eliminarle de algunos chats. No obstante, Heiss no se rindió y mediante la información de la propia página web y los comentarios de otros aficionados a los juegos de rol, consiguió la dirección de la pareja, empezando así un largo camino por las sendas del acoso y del ciberacoso. Incluso se llegó a presentar en su vivienda en

[4] Veáse Antena 3 Noticias
https://www.antena3.com/noticias/tecnologia/sube-foto-dinero-facebook-roban-casa_201205295754e5454beb2837bbff7363.html
[5] Veáse ABC
https://www.abc.es/recreo/abci-roban-todas-pertenencias-publicar-foto-facebook-201608081854_noticia.html
[6] Veáse El Economista
https://www.eleconomista.es/empresas-finanzas/noticias/1236890/05/09/Un-aleman-obsesionado-por-Internet-mato-un-britanico.html

un par de ocasiones antes del asesinato, lo que resultó realmente alarmante, ya que la pareja era de Nottingham y él de Alemania.

Destacar, por otra parte, que la delincuencia informática ha dificultado la detención y encarcelación de muchos delincuentes, dado que la ventaja de realizar un delito mediante la red es que se puede llevar a cabo desde la comodidad del hogar o el trabajo. Actualmente no es necesario comprar una pistola, pasamontañas y un saco para robar un banco, en estos momentos sólo se necesita un ordenador, una conexión wifi y habilidades informáticas. Es más, se puede estar incluso enfermo o tener alguna incapacidad física.

No obstante, no se debe olvidar que, en contraposición, las empresas y hasta el propio Instituto Nacional de Estadística[7] recopilan los datos de nuestras búsquedas por internet para posteriores usos comerciales y estadísticos. Es más, muchas empresas se dedican a vender dicha información a otras organizaciones que los utilizan para ofrecer sus servicios a través de publicidad en emails (spam[8]), llamadas, anuncios en las páginas webs que visitamos etc. Así pues, hasta las redes sociales se han sumado a este "hurto" de información, como ocurrió con Facebook hace unos años[9].

2. Marco Legal

La legislación debería ir acorde con los nuevos delitos, no obstante, aunque esta realidad sería la ideal, no siempre es así, puesto que en el Código Penal[10] no se incorporó este fenómeno criminológico, es decir, los delitos cometidos a través de internet no se consideraban tipología delictiva penal hasta el 2010. Durante este período, se produjeron numerosos casos que quedaron impunes, debido a que no se contemplaban en nuestras leyes, dejando así, desamparadas y desprotegidas a las víctimas, ya que quien les podía defender (ley) no las incluía.

[7] Veáse RTVE https://www.rtve.es/noticias/20191029/ine-seguira-movimientos-moviles-espanoles-durante-ocho-dias-para-estudio/1986520.shtml

[8] "Spam o correo basura: correo electrónico de distribución masiva y contenido normalmente publicitario o malicioso, que se recibe sin haberlo solicitado." Véase RAE https://dle.rae.es/correo#Sc9DCpf

[9] Véase El Mundo https://www.elmundo.es/tecnologia/2018/06/30/5b35f2f4468aeb22438b457d.html

[10] De ahora en adelante CP

El año 2010 fue clave para esta temática, porque fue el año en el cual España modificaría y ampliaría los tipos delictivos relativos a la ciberdelincuencia, especialmente de carácter sexual y relacionados con las redes sociales, consecuencia del Convenio sobre Ciberdelincuencia hecho en Budapest el 23 de noviembre de 2001 y ratificado por España mediante instrumento de 20 de mayo de 2010[11].

No obstante, como bien se mencionaba anteriormente, hubo muchos casos de difusión de vídeos o fotografías con alto contenido sexual, que no se castigaron porque el antiguo CP recogía que para que fuere reconocido como delito dicho material debía haber sido obtenido de manera ilícita. Por lo que no se contemplaba la posibilidad de que la víctima hubiese enviado voluntariamente las fotografías, pero no hubiese prestado su consentimiento para que el receptor las compartiese con terceros. Un ejemplo de este tipo de situaciones, que, además de convertirse en una muestra clara de esta deficiencia,sirvió de motivación para reformar este aspecto en el CP fue el "Caso Olvido Hormigos[12]". Tuvo lugar en 2012 en un pueblo de Toledo, cuando la exconcejala en cuestión, facilitó a su amante un vídeo en el que se mostraba a ella masturbándose, y éste acabó al alcance de media población española, además de colgada en distintas plataformas pornográficas y de contenido, como Youtube. Es más, tuvo tanta repercusión, que nivel interno, se llega a hablar del "artículo Olvido Hormigos[13]", para hacer referencia al art.197 CP.

Los artículos modificados o añadidos en el Código Penal que tienen relación con el ciberdelito son los siguientes:

2.1 Título VI: Delitos contra la libertad

En primer lugar, en cuanto al primer título que nos incumbe, destacamos el art.172.1 ter[14] añadido en el 2015. Éste hace referencia a aquellos actos que consisten

[11] Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. BOE-A-2010-14221.
https://www.boe.es/buscar/doc.php?id=BOE-A-2010-14221

[12] Véase La Sexta
https://www.lasexta.com/noticias/sociedad/olvido-hormigos-caso-que-cambio-codigo-penal-difusion-videos-sexuales-consentimiento-video_201905305cef93a50cf21b72629f1c3f.html

[13] Auto del Juzgado de Primera Instancia e Instrucción nº 1 de 15 de marzo de 2013.Véase sentencia http://www.poderjudicial.es/search/AN/openDocument/01b366bb5bfb10e3/20190624

[14] 1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana.

en acosar a una persona de manera repetitiva, sin ninguna justificación legal y que acaben por perturbar su día a día a la víctima. Pero en especial, nos centramos en el apartado 2[15] y 3[16] que especifican que este contacto se realice mediante algún medio de comunicación o que utilice su información personal para contratar servicios o mercancías, respectivamente. Este delito se conoce como acoso, y a nivel informático ciberacoso o cyberstalking.

2.2 Título VII: De las torturas y otros delitos contra la integridad moral

En este título se trata el art.173, el cual fue modificado en 2010 y en 2015, no obstante nos centraremos únicamente en su apartado primero[17]. En él se define la acción de llevar a cabo una conducta humillante hacia otra persona, y que dicho comportamiento dañe su integridad gravemente. A primera impresión parece no estar muy relacionado con el ámbito que nos incumbe, sin embargo, se hace referencia a él puesto que es al que se acude cuando se está ante el acoso escolar, o también denominado bullying. Además del existente maltrato físico y psicológico que ocurre en el ámbito escolar, también se ha trasladado a las nuevas tecnologías, recibiendo el nombre de cyberbullying.

2.3 Título VIII: Delitos contra la libertad e indemnidad sexuales

En relación con el bien jurídico protegido de la libertad e indemnidad sexual se encuentran numerosos artículos necesarios de mención, en especial, por tratarse de delitos cuyas víctimas son menores de edad o personas discapacitadas necesitadas de especial protección.

---

[15] 2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

[16] 3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

[17] 1. El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.

Con la misma pena serán castigados los que, en el ámbito de cualquier relación laboral o funcionarial y prevaliéndose de su relación de superioridad, realicen contra otro de forma reiterada actos hostiles o humillantes que, sin llegar a constituir trato degradante, supongan grave acoso contra la víctima.

Se impondrá también la misma pena al que de forma reiterada lleve a cabo actos hostiles o humillantes que, sin llegar a constituir trato degradante, tengan por objeto impedir el legítimo disfrute de la vivienda.

En primer lugar, el 183 ter[18], añadido en el 2015. Éste trata el tema del engaño, por parte de un adulto, a un menor con la finalidad de organizar un encuentro en el que se realicen actividades de carácter sexual o para que dicho menor le provea material pornográfico propio. En otras palabras, una persona adulta intenta contactar con un menor de edad y aprovecharse de la inocencia de éste, para conseguir que el menor acepte quedar con el adulto para mantener relaciones sexuales, o por otro lado, que el menor le envíe fotografías o vídeos comprometedores. Estos delitos también son conocidos como childgrooming y sexting, respectivamente.

Por otra parte, el siguiente artículo, también fue modificado con la reforma del 2015, se trata del art.186[19]. Tipifica diversos comportamientos vinculados con la distribución de pornografía de menores o aquellas personas que tengan una discapacidad y eso les haga necesitar una especial protección, ya sea con fines lucrativos o de disfrute.

El último es el art.189, también está relacionado con la pornografia de menores o incapaces, pero contiene un catálogo de distintas acciones a castigar en el ámbito de la pornografía, no obstante nos centramos en su apartado primero[20] el cual hace hincapié en los verbos captar o utilizar a víctimas menores o incapaces, y todos los

[18] 1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.
2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años.

[19] El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.

[20] 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.

vinculados con su producción y distribución, sin importar si mediante estas transacciones se obtiene un beneficio monetario o no.

2.4 Título X: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

El artículo que se va a mencionar ha sido de los más relevantes a nivel social, puesto que, como se citó anteriormente, fue muy polémico debido al "Caso Olvido Hormigos", ya que mostró una realidad que se vivía a diario, pero con una repercusión nacional. Éste ha sufrido diversas modificaciones en 2010, 2011 y 2015. Es el art.197, que en su primer[21] apartado se refiere a conseguir materiales personales, ya se trate de correos electrónicos, comunicaciones, papeles etc; el segundo[22] habla sobre apoderarse o cambiar la información de una tercera persona en formato papel o informático; y el más importante el apartado siete[23], el referente al sexting, es decir, el hecho de que una persona comparta una imagen íntima o de carácter sexual con otra, y ésta última la difunda sin el consentimiento de la víctima y esta distribución afecte a su intimidad. Además, el siguiente párrafo estipula que si la persona que comparte dichas fotografías privadas es su çonyuge o una persona con quien haya tenido o tenga una relación, las penas se impondrán en su mitad superior.

[21] El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

[22] Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

[23] Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.
La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Por otro lado, nos concentramos en los sistemas informáticos. Para empezar, el art.197 bis[24] que es acceder o facilitar el acceso a un sistema informático o se mantenga en él, o que intercepte datos, conocido también como hacking o hackeo. Muy relacionado con el ter[25], ya que es entregar contraseñas o códigos que permitan el acceso o un programa informático que posibilite la comisión de este tipo de delitos.

2.5 Título XIII: Delitos contra el patrimonio y contra el orden socioeconómico

Existen varios artículos que se pueden incluir en este título, como el art.238.4, 239, 256 y 270 y ss. Sin embargo, los primordiales son en el art.248.2[26] referido a las estafas informáticas, esto es, engañar a una persona manipulando o facilitando programas informáticos. En cambio, los art.264, 264 bis y 264 ter que recogen las actividades vinculadas con el sabotaje informático entre las actividades que se encuentran alterar, dañar o impedir el acceso a los datos, incapacitar un sistema informático o crear un programa informático o proporcionar una contraseña a un sistema privado.

---

[24] 1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.
2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

[25] Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:
a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos;
b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

[26] También se consideran reos de estafa:
a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.
c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Es importante recalcar que según el art.201 CP los delitos relacionados con el intrusismo informático será necesaria la interposición de denuncia, ya sea por parte de la víctima o su representante legal, o en caso de ser menor de edad o discapacitada, a instancia del Ministerio Fiscal.

En último término, algunos de los delitos antes nombrados tienen agravantes cuando se realicen por una organización criminal (por ejemplo ciberterrorismo), cuando el infractor sea el responsable de la información o el encargado de los equipos, en caso de que el infractor sea un funcionario público o de que la información sea difundida.

3. Formas de criminalidad

Las formas de criminalidad, son conocidas en el lenguaje jurídico como delitos, definidos por el Código penal español como "las acciones y omisiones dolosas o imprudentes penadas por la ley[27]". Esta definición resulta muy genérica, ya que abarca numerosas conductas de naturaleza demasiado variable. Por eso, en este apartado se va a clasificar aquellos delitos elegidos que tienen en común las nuevas tecnologías, y éstos se han dividido en los siguientes dos grupos.

3.1 Nuevas formas de criminalidad

Para comenzar, este subapartado se caracteriza por tratarse de infracciones legales inimaginables antes de la era del espacio cibernético. Son aquellas que para producirse se requiere un profundo conocimiento de la tecnología y un equipo técnico especializado.

3.1.1 Hackear

Esta actividad es desarrollada por los conocidos como hackers, en español denominados piratas informáticos. Su origen hace referencia a los antiguos piratas de barcos, que se introducían sin permiso en navíos ajenos, para una vez dentro robar las riquezas que éste poseía o el propio buque. En la era informática, la definición es muy similar, según la RAE[28], la acción de hackear es explicada como "introducirse de forma no autorizada en un sistema informático". La finalidad de dicha intrusión es muy

[27] Artículo 10 CP
[28] Real Academia de la Lengua Española

variada, puede ser conseguir contraseñas bancarias, el robo de identidad, revelación de secretos etc. Sin embargo, en la en el mundo informático el término de “hacker” es considerado despectivo, ya que la definición citada se dice que no corresponde a un hacker, sino a un cracker, puesto que consideran que los hackers simplemente son entusiastas de la informática, que utilizan sus habilidades técnicas únicamente para encontrar vulnerabilidades en la seguridad de las páginas webs y así poder mejorarlas, evitando futuras intrusiones. No obstante, dentro de los nombrados hackers, se pueden encontrar subtipos como:

- Hackers activistas: se concentran en atacar con fines políticos, normalmente con la intención de desvelar secretos de los gobiernos y mostrárselos a la ciudadanía, como es el ejemplo de Anonymous[29].

- Black hat: aquellos conocidos como crackers o ciberdelincuentes que de manera consciente y deliberada emplean sus habilidades informáticas en beneficio propio, ya sea a cambio de una cantidad económica o para causar daños.

- White hat o hackers éticos: trabajan para empresas o gobiernos comprobando las vulnerabilidades de sus sistemas y permitiendo así rectificar dichos fallos, para aumentar su protección (Ej.Dr.Chema Alonso[30]).

- Grey hat: aquellos que tienen una moral ambigua, se comportarían en ocasiones como black y en otras como grey. Una conducta común es destruir un servidor mediante la introducción de un virus y contactar con la víctima advirtiéndole que es el único que puede solucionarlo y que para ello tendrá que ser económicamente compensado.

3.1.2 Sabotaje

Este delito está bastante relacionado con el anterior, ya que también se trata de una intrusión, pero la diferencia se encuentra en el objetivo del sabotaje, el cual no es otro que la destrucción de la información contenida en los dispositivos, hacer inaccesible los datos, borrarlos, alterarlos etc. En definitiva, impedir que se puedan utilizar los documentos presentes en los aparatos electrónicos, ya sea mediante programas

[29] Veáse RTVE
https://www.rtve.es/noticias/20120228/anonymous-quienes-son-como-actuan/438765.shtml
[30]Véase El País
https://cincodias.elpais.com/cincodias/2020/01/28/companias/1580232696_339551.html

maliciosos o virus informáticos. En ocasiones se considera una acción del “hacking”, puesto que se están infiltrando en los dispositivos ajenos sin la voluntad del propietario.

3.1.3 Sexting

El sexting es la acción de enviar imágenes o vídeos propios con un contenido sexual, normalmente a la pareja, y que ésta última las comparta con terceros sin su consentimiento. La difusión se suele producir después de una ruptura, una pelea o por ejemplo, una infidelidad, cuya finalidad, por lo común, suele ser la venganza. Esta conducta es propia tanto de menores como de adultos, ya que su uso se ha extendido y se ha convertido en una actividad habitual entre las parejas, aunque los últimos estudios apuntan a que la población con una edad más avanzada suele recurrir a su práctica en mayor medida que la población adolescente (Klettke et al., 2014). Puntualizar que este primer comportamiento se debe realizar de manera voluntaria y consentida por parte de la cibervíctima. Así pues, no cabe la acción de hurtar las fotografías o tomarlas sin su aprobación, dado que en esta situación no se trataría de este delito. A pesar de ello, también sucede, en ocasiones, que previamente a la divulgación del material haya existido un período de chantaje o amenaza, exigiendo a la víctima retomar la relación o más fotografías, entrando en un bucle con un complicado final.

3.2 Clásicas formas de criminalidad informatizadas

La sociedad cambia, pero siempre mantiene sus raíces, y prueba de ello es la evolución que han sufrido las clásicas formas delictivas. A diferencia de las anteriores, éstas llevan produciéndose desde hace siglos, es más, siempre han existido. La innovación acontece en el momento en que los delincuentes transforman su manera de quebrantar la ley, y aprovechan la oportunidad que les brinda la red para ampliar su zona ámbito criminal. Así pues, hace unas décadas, un ladrón que residía en Castellón únicamente podía perpetrar sus hurtos o robos en la misma ciudad o sus alrededores (a no ser que se trasladara o mudara), no obstante, en la actualidad, este sujeto que seguiría viviendo en Castellón, tiene la oportunidad de que sus delitos repercutan en personas de cualquier otro país.

3.2.1 Cyberstalking

En castellano es conocido como ciberacoso, y se define como un tipo de acecho que se produce a través de la tecnología. También es una conducta habitual en el ciberbullying (acoso entre iguales o acoso escolar), la cual suele ir acompañada de otras acciones, no obstante esto se explicará más adelante, en el apartado 3.3 Menores. El acoso se caracteriza por ser una persecución constante de la víctima, cuando ocurre en el medio físico va aparejado a seguimiento del acosado, acudir a los mismo lugares o intentar contactar con ella. No obstante, tanto en el supuesto del cyber como en el tradicional, se exigen dos requisitos. El primero, que se trate de un hostigamiento continuo y repetido, es decir, para considerarse acoso debe ocurrir en más de una ocasión, y éste debe ser seguido, ya que si sucede una vez cada 2 años, no valdría. El segundo, es un elemento subjetivo, puesto que describe cómo el perjudicado concibe este acoso, dado que si no le causa una molestia o alteración en su vida diaria, no se entendería como acoso. Un ejemplo de ello son las celebridades que usualmente son acechadas para tomar fotografías o conocer novedades de su vida, aunque está presente el elemento objetivo, no les supone un problema.

Cuando este acoso se traslada a lo virtual se modifica sustancialmente. No significa que las consecuencias no sean las mismas, sino que el método con el que es desarrollado es diferente. El cyberstalking[31] es más complejo de detectar, porque muchos de los comportamientos no son delictivos en sí mismos, en otras palabras, solicitar la amistad por una red social no constituye ninguna infracción, ni tampoco realizar llamadas ni mucho menos escribir comentarios en un perfil virtual ajeno. Así pues, lo condenable es cuando esto se lleva al exceso y las solicitudes de amistad son diarias o incluso, hay una creación de varios perfiles para poder acceder a esta persona. Además, existen usuarios que ciberacosan y no conocen al propio acosado, simplemente se unen a la iniciativa que ha creado otra persona. Algunas de los actos por los que se lleva a cabo el ciberstalking son:

- Envío masivo de emails, mensajes por mensajería instantánea o redes sociales, SMS o llamadas.

[31] Término extranjero, procedente de los países del Common Law, en los Estados Unidos, aunque también es utilizado en Gran Bretaña para definir comportamientos dentro del Harassment.

- Creación de perfiles falsos, aunque difundan datos verdaderos como fotografías reales. También existen aquellos en los que se modifican imágenes apareciendo el rostro de la víctima, pero tratándose de un montaje informático.

- Menciones en numerosas fotografías, chistes, burlas o amenazas o su envío.

- Tomar contacto con personas cercanas al objetivo para intentar interactuar con éste.

- Elaborar clubs de haters[32] en los que se juntan distintos usuarios y se mofan del acosado a horas concretas para dar mayor difusión.

- Publicar anuncios web ofreciendo servicios sexuales o de otra índole, aportando datos personales como el número de teléfono.

- Difusión de rumores o secretos.

3.2.2 Pornografía

En el Código Penal aparece descrito lo que es considerado pornografía (infantil o personas necesitadas de especial protección) en su art.189.1[33], incluyendo material visual de una conducta sexual, órganos sexuales o imágenes realistas[34]. Así pues, desde la invención de la cámara y la fotografía existe la pornografía, por lo que las nuevas tecnologías sólo han amplificado su repercusión y propagación. En la actualidad sigue manteniendo el patrón de producción a través de una cámara, pero ésta puede estar incorporada en un móvil, tablet u ordenador. Lo que ha evolucionado

[32] La traducción literal es personas que odian. Su finalidad en las redes es criticar, insultar y burlarse de distintos perfiles, ya sea por algo físico, psicológico o simplemente por el contenido que sube a internet.

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

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

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

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

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

[34] Esta definición legal fue tomada de la Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011.

ha sido la cantidad de personas receptoras de dicho material, esto se debe a que años atrás la capacidad de reproducción o envío estaba limitada a realizar diversas copias o a remitirlas mediante el correo postal, y por el contrario en el presente se cuentan por millones. Además de un significativo aumento de su difusión, también se han desarrollado nuevas formas para eludir los algoritmos y rastreos de las autoridades, como por ejemplo la criptografía que sirve para ocultar la pornografía dentro de una imagen o archivo, dificultando inmensamente su descubrimiento.

Otra forma de producción de la pornografía virtual es la llamada "pornografía infantil artificial", que sería la correspondiente al art.189.1 d). Consiste en la creación de imágenes, aparentemente de un menor realizando actos sexuales, pero sin que esto haya sucedido nunca, en otras palabras, mediante aplicaciones de ordenador se elabora una fotografía que, sin analizarla por programas informáticos, parece ser real y que se trate de un menor que está llevando a cabo actividades de tipo sexual, es una confección artificial que simula ser realista.

3.2.3 Estafa informática

La estafa, existente desde hace varios siglos se define por tratarse de una conducta en la que priman tres elementos, el ánimo de lucro (búsqueda de una ganancia a nivel individual), el engaño (transmitir que algo es verdadero cuando no lo es) y la inducción al error (la víctima debe creer que es cierto), ésta última irá ligado a una pérdida o desvío en el patrimonio personal de la víctima. Estas tres características son fácilmente trasladables al ámbito de las TICS, sobre todo la inducción al error, ya que es frecuente adquirir productos por páginas webs, utilizar el correo electrónico o pagar mediante tarjeta electrónica. En relación a la estafa informática, se han de nombrar distintas formas de llevar a cabo:

- Phishing[35]: es un ataque basado en la ingeniería social. El delincuente, fingiendo ser una empresa u organización de confianza y mediante la comunicación tecnológica, intenta engañar a la víctima para que le proporcione información privada, la cual, una vez conseguida, éste utilizará a su antojo para poner en funcionamiento todo su plan. Dicho de una manera menos informática, se empieza por el envío de correos electrónicos a diferentes direcciones, en los que se incluye un link, que cuando el atacado clickea le

[35] El término *phishing* proviene del vocablo anglosajón fishing, conocido como la acción de pescar, aunque en ocasiones es traducido como suplantación.

redirecciona a una web falsa, aunque parece un sitio oficial, en el que la víctima introduce sus datos.

- Pharming: su definición es la misma que la anterior, con la excepción de tratarse exclusivamente de entidades bancarias. La finalidad es obtener el usuario y la clave de acceso de las víctimas para poder acceder a su cuenta privada, y operar a través de ella.

- Estafa Nigeriana o fraude 419[36]: se realiza mediante correo electrónico no deseado (spam), en el cual el estafador dícese ser un empresario o príncipe nigeriano que posee una gran fortuna y promete una importante suma de dinero a cambio de una mínima transferencia/datos bancarios o una persona que se encuentra en apuros y necesita ayuda. Las excusas utilizadas son que dicho empresario ser su socio en algún negocio y para empezar necesita un adelanto, va a fallecer pronto y ha observado por internet que la víctima es persona honesta y desea donarle su fortuna pero ahora tiene unos gastos imprevistos mientras se realiza el trámite, la persona está atrapada o secuestrada y quiere salir del país pero no cuenta con dinero con el que viajar y salvar a su familia de ese peligro o que quiere ingresar su capital en el país de la víctima y para ello se requiere una cuenta y si la ésta se la presta le recompensará con un porcentaje[37].

- Engaños sentimentales[38]: normalmente la víctima suele ser hombre heterosexual, ya que el "cebo" es una mujer joven atractiva. Empieza con un la recepción de un email al futuro engañado, quien descubre que una chica (siempre extranjera, usualmente Europa del Este) quiere contactar con él, al pinchar en el link le deriva a una página web donde aparecen más mujeres que quieren conocer al amor de su vida. Al entablar una conversación más o menos diaria, la chica afirma estar enamorada de dicho hombre y querer conocerlo

[36] Su nombre tiene su origen en que los correos son procedentes de Nigeria o realizados por personas de esta nacionalidad, y además en el art.419 del Código Penal Nigeriano se recoge y pena esta estafa.
[37] Véase La Vanguardia https://www.lavanguardia.com/vida/20200416/48565386077/no-hay-una-rica-heredera-que-done-su-fortuna-a-desconocidos-es-otra-estafa.html
[38] Relacionado con ello está la sextorsión, cuyo procedimiento es muy similar, ya que comienza con una mujer que agrega a la cibervíctima para conocerse, y posteriormente consigue que el hombre le envíe fotos de carácter erótico y le amenaza con hacerlas públicas o enseñárselas a su mujer, si no le transfiere una cantidad de dinero.

personalmente. El problema es que ella no dispone de la cantidad necesaria para comprar el pasaje de avión y la víctima es quien decide regalarle el viaje.

- Extorsión: existen varias versiones de este tipo de estafa, no obstante, se van a mencionar las tres más comunes y recientes. Todas tienen en común que se realizan mediante el correo electrónico y que la información que se proporciona bajo ningún concepto es real, aunque pueda parecerlo.
    a. Amenazas: el destinatario es alertado por un sicario que ha sido contratado para acabar con la vida de éste, su familia, secuestrarles o agredirles y que es conocedor de la dirección de su vivienda . No obstante, el sicario se ofrece a no realizar el encargo a cambio de una suma de dinero, muy inferior a la establecida por su contratante, porque ha visto que la víctima es una buena persona.
    b. Vídeos íntimos: el remitente afirma poseer vídeos de carácter sexual, de la persona receptora del email, más específicamente masturbándose mientras observaba un vídeo pornográfico, y a no ser que se le pague una cantidad de dinero los hará públicos.
    c. Organismos oficiales: la víctima es cazada por la Policía Nacional llevando a cabo actividades ilegales a través de su ordenador, lo que conlleva a un bloqueo del dispositivo para que no cometa más delitos, siempre que no pague la multa correspondiente[39], o que se está investigando a dicha persona por alguna infracción y se le deben facilitar diferentes datos, entre ellos, cuenta bancaria. Recientemente ha ocurrido con la DGT[40] y las supuestas multas de tráfico.

3.3 Menores

Como es lógico, los delitos mediante tecnología también han llegado a los menores de edad. Asimismo, muchos de ellos se han criado con televisión, móviles, tablets, entre otros artefactos. Este hecho ha dado lugar a que gran parte de la población nacida a partir del año 2000 maneje con excesiva facilidad las TICs, y que eso haya hecho que, en la actualidad, el lugar de reunión de este grupo de edad, haya cambiado, pasando del parque a la red.

[39] Véase RTVE https://www.rtve.es/noticias/20120130/virus-informatico-utiliza-como-senuelo-policia-para-cometer-estafas/493944.shtml

[40]Véase Cadena Ser https://cadenaser.com/ser/2020/03/29/sociedad/1585497118_052793.html

Los estudios revelan que casi el 50% de las personas entre 12 y 17 años estarían involucradas como autores y/o víctimas en este tipo de comportamientos (Tamarit Sumalla[41]). La cuestión es el motivo, ¿por qué? De acuerdo con un estudio llevado a cabo por la Universidad Camilo José Cela[42], la razón es por el mal uso o abuso de estas herramientas, ya que "sólo un 32% de los adolescentes harían un uso adecuado de Internet, mientras que el 31,5% mostrarían ya señales de riesgo, un 23,3% mantendrían una conducta de uso abusiva y un 13,2% mostrarían una clara dependencia comportamental en el uso de la red". Del mismo modo que "los datos del INE apuntan que Internet es usado habitualmente por el 98% de los adolescentes a los 15 años y, como apunta este estudio, sólo un tercio lo hace de manera no problemática".

Por ello, esta tipología es sumamente importante, puesto que algunas de estas situaciones son de carácter sexual. A continuación, se enumeran aquellos delitos en los que los menores están involucrados.

3.3.1 Cyberbullying

El término bullying, también denominado acoso escolar, es conocido como la violencia entre iguales, se suele referir a violencia entre menores de edad, normalmente en edad estudiantil, ya sea en colegio o instituto. No obstante, fue definido por Olweus como "una conducta de persecución física y/o psicológica que realiza un/a alumno/a contra otro/a, al que escoge como víctima de repetidos ataques [43]". Además de lo definido, es necesario resaltar que esta conducta debe ser continua durante un período de tiempo más o menos largo, que puede perdurar durante meses o años, y que estas acciones provocan en la víctima una total indefensión, requiriendo, para salir de ese círculo, la ayuda de una tercera persona.

---

[41] Tamarit Sumalla Josep M. (2016). «Presentación». En: «Ciberdelincuencia y victimización» [revista en línia]. IDP. Revista de Internet, Derecho y Política. N.º 22, págs. 30-31. UOC.

[42] Uso y abuso de las tecnologías de la información y la comunicación por adolescentes: un estudio representativo de la ciudad de Madrid.
Véase: https://www.ucjc.edu/wp-content/uploads/Estudio-UCJC-y-MADRID-SALUD-2018.pdf

[43] Collell i Caralt, J. y Escudé Miquel, C. "El acoso escolar: un enfoque psicopatológico" extraído de Olweus, D. (1983). "Low school achievement and aggressive behaviour in adolescent boys". En D. Magnusson y V. Allen (Eds.), *Human Development. An interactional perspective*, New York: Academic Press.
Enlace http://institucional.us.es/apcs/doc/APCS_2_esp_9-14.pdf

En cuanto al ciberacoso tiene muchas características similares con el bullying, básicamente es el mismo comportamiento, lo que sucede es que uno se produce en el mundo físico y el otro en la red. No obstante, es importante destacar que dentro del término se engloban diversas acciones, que se pueden clasificar según Willard[44] en distintas clasificaciones.

- Flaming o incendiario: consiste en el envío de mensajes vulgares que contengan insultos, ofensas o ataques hacia un grupo o persona, normalmente en páginas web públicas como foros o chats (aunque también sucede mediante email o SMS), con la finalidad de irritar o "encender" a ese o esos destinatarios y que contesten de manera maleducada produciendo grandes discusiones. Ejemplo: escribir en un foro que Carla es lesbiana y que quiere mantener relaciones sexuales con compañeras de clase.

- Harassment o acoso: se produce cuando se envía de forma continuada a una persona en particular numerosos mensajes o emails ofensivos. Ejemplo: Una persona anónima le envía a Claudia todos los días a la salida del instituto un mensaje diciéndole que es mala estudiante, está gorda y sólo sirve para comer bollería.

- Denigration o denigración: se define como la divulgación de rumores o información falsa y perjudicial de la víctima, pueden ser desde mensajes falsos o calumnias hasta imágenes manipuladas. Ejemplo: Un grupo de clase crea una página web sobre Pepe en el que publican información sobre él como sus supuestas exparejas o fotos de él robando.

- Impersonation o suplantación: hacerse pasar por otra persona y enviar o publicar mensajes o contenido multimedia, dando lugar a un engaño. Ejemplo: María consigue la contraseña del correo de Luis, porque se ha dejado el ordenador encendido en clase, y decide mandar un mensaje desde la cuenta de Luis al profesor de química insultándole.

- Outing and trickery o revelación de secretos : es un comportamiento en el cual se publica información privada, sensible o embarazosa sobre la víctima. Dichos datos no tienen por qué ser únicamente palabras, pueden ser fotos o vídeos.

[44] Willard, Nancy E. *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research press, 2007. En Río-Pérez, J., Charo Sádaba-Chalezquer, and Xavier Bringué. "Menores y redes¿ sociales?: de la amistad al cyberbullying." (2010).

Ejemplo: a Marta le preguntan por instagram sus “amigas” quien cree que es el chico más sexy del instituto y ella contesta que Pedro. A las horas, su respuesta ha sido transformada en una captura de pantalla que está colgada en todos los perfiles de sus “amigas”.

- Exclusion o exclusión: es la expulsión deliberada de la persona acosada de un grupo virtual (whatsapp, club de deporte, foro, juegos en línea…) o la prohibición de su entrada en dicha comunidad, provocando en la víctima una completa sensación de rechazo y soledad. Ejemplo: Marcos y sus amigos tienen un grupo de videojuegos y siempre que se conectan juegan juntos y hacen videollamadas, pero le echaron y ahora cuando él se conecta para jugar, el resto desaparecen.

- Cyberstalking o ciberacoso: reside en un continuo seguimiento o acecho a una persona en el mundo virtual, llevando a cabo actividades como envíos de emails, llamadas anónimas, amenazar, mandar mensajes...Obviamente este intento de contacto por parte del agresor es totalmente indeseado para la cibervíctima. Ejemplo: Pablo y Paula rompen su relación, pero Paula está muy enfadada porque su exnovio le ha sido infiel y quiere que le pida perdón y le dé más explicaciones, por ello, cada hora le manda mensajes preguntándole e insultándole.

Como se ha observado, ambas tipologías tienen un nexo común que es el maltrato repetido y prolongado hacia una persona. A pesar de ello, difieren en varios aspectos. El primero es que el bullying tiene la posibilidad de ser directo (físico) o indirecto (insulto), en contraposición con el cibernético, ya que su única opción es el indirecto, a través de las redes, ya que un ciberacosador nunca podrá agredir a su víctima. Además, para que se produzca el cyberbullying no es necesario que el agresor conozca a la víctima en cuestión, dado que puede tratarse de un agresor secundario, es decir, que una persona cuelgue en internet una foto menospreciando a la víctima y éste la reenvie, mientras que el bullying es imposible que la víctima no sea una persona de su entorno. Por otra parte, en cuanto a la edad de inicio del ciberacosador suele rondar los 13,6 años[45], una edad dos años superior a la del acosador tradicional, diferencia destacable como que el 70% de las cibervíctimas son chicas, datos muy contradictorios con el bullying, ya que ambos sexos suelen estar igualados. Además,

[45] Véase https://www.anar.org/estudio-ciberbullying/

según el doctor Santiago Resett[46] el alumnado que acosa por internet tiene una apariencia más sociable y amigable, concluyendo así que "las diferencias entre las aptitudes de los autores indicaría que las características psicológicas de quienes hacen cyberbullying y bullying son distintas[47]".

3.3.2 Childgrooming

El childgrooming es una variante del cibergrooming que se identifica por sus sujetos, el activo obedece a un perfil de un adulto[48] y el pasivo, un menor. La dinámica se basa en un intento de contacto con el menor, mediante el engaño para una posterior quedada donde se produce un abuso o agresión sexual. La finalidad siempre es terminar saliendo de lo virtual y pasar al mundo físico, pero no siempre sucede, porque para ello es necesario obtener, primero, la confianza por parte menor y después su miedo a ser descubierto. Se podría sostener que es de los ciberdelitos que requiere más paciencia por parte agresor, dado que este proceso exige que la víctima acabe confiando en él y crea firmemente que con quién está chateando es alguien de su edad. Los lugares favoritos para los cibergroomers[49] suelen ser las salas de chat públicas, en las que cualquier sujeto puede registrarse sin aportar más que un correo electrónico, un nick y una contraseña. A pesar de ello, no es inusual que suceda a través de las redes sociales o correo electrónico. Aunque, la principal desventaja del uso de las redes, es que, pese a que aparente una mayor fiabilidad y ello produzca una aceleración en el proceso de la confianza, da lugar a una complicación de la ejecución del plan, puesto que se exigen datos personales como fotografías, edad o como mínimo una biografía en el perfil. Para ello, será necesario que el adulto invierta cuantioso tiempo en la creación del usuario y sus datos, además de simular una vida de adolescente para no levantar sospechas, subiendo imágenes propias (selfie) o de acciones de jóvenes como estudiar, ver una serie o ir de compras, y aunque todo ello es fácilmente extraíble de los buscadores u otros perfiles, precisa un gasto de tiempo.

---

[46] Véase https://noticiasdelaciencia.com/art/29470/cyberbullying-los-agresores-son-amables-en-persona-pero-ofensivos-en-las-redes-sociales

[47] Véase Agencia Legislativa. Enlace: http://agencialegislativa.com/cyberbullying-perfil-del-agresor/

[48] En España se considera adulta aquella persona mayor a 18 años.

[49] Nombre que reciben quienes cometen cibergrooming.

Al tratarse de un proceso que demanda una organización, autores como Miró Llinares [50] explican que el childgrooming se divide en cuatro fases:

1. Primer contacto: el ciberagresor adulto a través de internet contacta con un menor, usando de cebo un perfil atrayente (tener gustos similares, mismos problemas con los padres, tener un buen físico, edad similar…).

2. Objetivo: en la segunda fase todas esas largas conversaciones han calado en el menor, y éste consiente encender la webcam, enviar alguna fotografía con un posado sexy, ligero de ropa o de carácter sexual.

3. Amenaza: tras la consecución del material sensible, el childgrommer muestra al adolescente su error, y que no es esa adolescente, sino un adulto que tiene en su posesión ese contenido facilitado por él y le amenaza con difundirlo por las redes, subirlo a plataformas pornográficas o ponerse en contacto con su familia y amistades, revelando así sus actividades secretas, sino le proporciona más cantidad de fotografía o vídeos[51].

4. Plano físico: el menor, ahora asustado y temiendo las posibles represalias acepta realizar cualquier cosa con tal de que no se haga pública su situación, incluso aunque para ello tenga que mantener algún tipo de relación sexual con este adulto.

Dentro del child grooming, también aparece otra figura delictivas como lo es el sexting mencionada anteriormente, dado que el menor (al principio) envía ese contenido de carácter sexual de manera totalmente voluntaria. Sin embargo, al considerarse un requisito elemental para este ciberdelito no se estima como otra conducta, sino que se subsume en el mismo.

4. Problemática

Todas las infracciones legales tienen sus consecuencias para las víctimas, y sus dificultades, tanto a nivel preventivo como de actuación, para las fuerzas y cuerpos de seguridad. No obstante, los delitos cibernéticos, a pesar de ser un grupo muy amplio en cuanto a tipología, poseen unas características comunes que facilitan y motivan su

[50] En Cibercrimen, Cibercriminales y Cibervíctimas (UOC)
[51] Este material, en ocasiones, es difundido o vendido pornografía infantil, aunque el menor acceda a las demandas del ciberagresor.

comisión, a la misma vez que suponen una problemática para los investigadores y la propia justicia, además de causar un gran daño a las cibervíctimas.

El principal problema (ventaja para los delincuentes) se trata de la gran internacionalidad de comisión del delito. Dicho de otro modo, se pueden llevar a cabo sin necesidad de estar físicamente en el lugar en el que se quiere cometer. La existencia del mundo virtual es como una recreación del mundo real, más concretamente, cada persona, empresa, banco, hospital etc tiene su presencia en la red, ya sea mediante una página web, instagram, facebook o blog, entre otras. De esta manera se facilita enormemente la posibilidad de que personas hábiles en el uso de las nuevas tecnologías puedan introducirse en dicho mundo y perturbarlo. Supone un reto ya que para encontrar al transgresor no se puede limitar el lugar de comisión, puesto que el hecho de que se haya denunciado en Finlandia, no es sinónimo de que éste se halle operando allí, sino que puede estar en China.

Ligado con el párrafo anterior se encuentra el asunto legislativo mundial. Como es comprensible, cada país tiene su territorialidad y sus normas que en infracciones físicas pueden suponer menos inconvenientes, pero a nivel virtual resulta casi imposible su enjuiciamiento, puesto que solamente se tienen dos opciones. La primera sería extraditar al acusado al país en cuyas fronteras hubiese delinquido, pero ¿qué ocurre si los afectados han sido distintos países? y ¿en la situación en que hubiese algún testigo o los propios agentes de la ley tuviesen que testificar ante el juez? Resulta realmente complejo, ya que se deberían celebrar distintos juicios, movilizar personas y, además, no se ha contado con las diferencias penales entre estados. La otra opción sería juzgarle en el país en el que resida, para lo cual sería fundamental el traslado de pruebas por parte de los oficiales del país que haya llevado a cabo la investigación. Como se comprueba, ambas situaciones suponen escenarios espinosos y eso que el ejemplo trata únicamente de un delincuente, ni siquiera se ha comentado el ciberterrorismo u organizaciones de pornografía compuestas por decenas de personas.

Un punto clave es la confianza que aporta el anonimato, puesto que es un factor que suele motivar y crear una “falsa” sensación de seguridad para el criminal. Se debe al realizar las actividades delictivas a distancia, dado que al no estar presente en el lugar físico, siente que es invisible y que sus acciones quedarán impunes, ya que

nadie le reconocerá gracias al uso de pseudónimos. Esta tranquilidad está presente en todos los diferentes tipos de delitos cibernéticos, no obstante es más evidente en los delitos de odio a través de las redes sociales, en especial en Twitter[52], debido a que su eficacia en cuanto a la eliminación de sus tweets es más que cuestionable, en comparación con Youtube y Facebook[53].

Por otra parte, un ataque cibernético es más económico y requiere menos preparación, considerando que los materiales base que se precisan apenas son un dispositivo electrónico (normalmente ordenador o móvil) y una conexión a internet[54]. Pero en ocasiones no hace falta que sea propio, es tan simple como conectarse a una red Wifi pública o utilizar los ordenadores de una biblioteca. Se elimina así las largas horas de vigilancia de bancos o de seguimiento a personas, el gasto en armas o en billetes de transporte para acudir al lugar, incluso el tiempo invertido en acondicionamiento físico, puesto que no es tanto un trabajo físico como intelectual.

Asimismo adquirir esas habilidades informáticas puede no ser tan complejo como puede parecer a primera vista, porque existe una importante facilidad de conocimiento y mejora en comparación con los delitos no cibernéticos. En primer lugar, esto sucede ya que no existe ninguna escuela legal en la cual se enseñe a estafar o a asesinar, por el contrario en muchas universidades de nuestro país se oferta el grado en ingeniería informática (sin ninguna finalidad delictiva), permitiendo que aquellas personas interesadas en actividades criminales puedan incorporar esos conocimientos informáticos y transformarlos en las herramientas precisas para cometer delitos en el mundo virtual y evitar ser identificado por las FFCCS. Además, ni siquiera es necesario acudir a una enseñanza tan superior, mediante escasas búsquedas en google[55] se encuentran numerosos recursos, tanto a nivel manual (libros), blogs, vídeos e incluso cursos, algunos de ellos gratuitos, lo que hace más atrayente iniciarse en el hacking (ejemplo).

Mencionar también que la escala criminal es exponencialmente mayor. Esto significa que las personas que pueden intervenir en un ciberdelito se multiplica por miles, en comparación con una acción ilícita común. Consecuencia del alcance casi

[52]Véase El País https://elpais.com/tecnologia/2018/11/01/actualidad/1541030256_106965.html
[53] Véase RTVE http://www.rtve.es/las-claves/el-odio-en-las-redes-sociales-2018-04-26/
[54] Dependiendo el tipo de delito se tendrá que añadir un perfil en una red social, página web, creación de un virus, correo electrónico etc
[55]Veáse https://www.blog.andaluciaesdigital.es/sitios-para-practicar-y-aprender-hacking/

mundial (determinados pueblos, tribus indígenas, ciudades subdesarrolladas etc a los que aún no ha llegado) que posee internet, lo que le permite una masificación del contenido. Así pues, se logra que una fotografía íntima llegue a manos de personas de otros países, e incluso continentes y que éstas puedan, si lo desean, reenviarla y continuar con la cadena, ampliando potencialmente su audiencia.

En relación con la difusión está la rapidez con la que se expande, al tratarse de acciones tan simples como enviar un mensaje. Sobre todo sucede con el cyberbullying, ciberstalking y algunos tipos de estafa informática, en la que, en los primeros ejemplos los comentarios son públicos y eso facilita que otros sujetos puedan unirse a este tipo de acciones o que viralicen la situación, pudiendo llegar miles de personas en pocos minutos, y en cuanto al engaño es debido a que a la hora de mandar correos electrónicos, se pueden seleccionar a más de un destinatario, dando lugar a una propagación mucho más veloz que con un delito físico.

Otro de los inconvenientes de la ciberdelincuencia es la permanencia. En ocasiones se olvida, pero la realidad es que todo lo que es subido a una plataforma, siempre va a estar ahí, incluso, sin que sea necesario compartirlo, al realizar una fotografía se queda almacenada en la memoria del dispositivo. Es cierto que existen aplicaciones que permiten eliminar las publicaciones o los mensajes, pero esto no es exactamente verdad. Lo que ocurre es que las personas "corrientes[56]" no podrán volver a acceder a ellas, no obstante, eso no es sinónimo de que no hayan existido, ha quedado un rastro, el necesario para que aquellas personas que tienen la capacidad de introducirse en esas bases de datos, puedan recuperarlos y apropiarse de ellos. Además, de ello, vinculado a los párrafos anteriores, cuando una imagen es difundida a millones de personas (p.ej. sexting) éstas pueden apropiársela, y aunque posteriormente una sentencia ordene su destrucción y borrado de internet, jamás se podrán eliminar todas las reproducciones, siempre, en algún dispositivo, esa imagen seguirá existiendo.

Por último, a pesar de que no se ha indagado mucho sobre este asunto, es necesario destacarlo, puesto que está muy asociado con las actividades

[56] Referencia a aquellas que no tienen las habilidades necesarias o que las poseen pero no tienen finalidades delictivas.

cibercriminales. Esto es la llamada Deep Web y Dark Web[57], una parte de internet utilizada, normalmente, para usos ilícitos. Se accede a través de las conocidas Darknet como TOR[58], I2P y Freenet, son servicios de búsqueda que abren al internauta casi el 100% del ciberespacio. Como bien se ha dicho, el uso de esta web es más ilegal que legal, ya que contiene cientos de mercados, desde drogas o armas hasta pornografía, sin olvidarse del blanqueo de capitales, los hackers de alquiler o el reclutamiento terrorista. Gracias a ella se pueden obtener servicios para perpetrar cientos de delitos y ciberdelitos, con una mayor seguridad en los últimos, al tratarse de una mayor protección del anonimato. A pesar de ello, también contiene zonas útiles para la justicia, como lo es la comunicación protegida y secreta entre disidentes políticos (regímenes represivos) o la información proporcionada por personas a periodistas sobre la realidad de su país, además de servir para los ciberactivistas y defensores de los derechos humanos que temen por su vida.

5. Criminología Transforma

Después de todo lo anteriormente mencionado, de ser conscientes de los males que internet ha ayudado a nacer, es normal que se nos venga a la mente la incógnita de si la vida era mejor antes de las nuevas tecnologías. Dicho de otra manera, si mediante internet se ha inducido al suicidio a niños por el ciberbullying, si las redes sociales han proporcionado todos los datos necesarios para asesinar a otra persona y la informática ha suministrado las herramientas necesarias para que los hackers destrocen el mundo virtual, desde el punto de vista preventivo ¿no sería más conveniente restringir su uso y acceso para minimizar estos ciberdelitos?. La Criminología se hizo esta pregunta, y su respuesta fue un rotundo no, por el simple hecho de que fue inteligente y se percató de que podía utilizar esta arma a su favor, mediante algunos de los usos que se enumeran a continuación.

[57] En español sería la Web profunda y la Web oscura. Se debe diferenciar, ya que la Deep Web engloba a la Dark Web, puesto que mientras la primera es considerada benigna, debido que lo único que proporciona son páginas web que los propios motores de búsqueda usuales (google, firefox, explorer…) no pueden identificar, la segunda, por el contrario es la que contiene los sitios comerciales con contenido ilegal.

[58] Servicio desarrollado por David Goldschlag, Mike Reed, y Paul Syverson, integrantes del Laboratorio de Investigación Naval de los Estados Unidos (NRL) con la finalidad de preservar las comunicaciones secretas. Es la más utilizada.

5.1 Geoprevención

Esta técnica consiste en un estudio a nivel espacial de los delitos que se cometen, y de esta manera se crean, mediante estadísticas obtenidas a partir de los datos introducidos en una base de datos y analizados por un algoritmo, los puntos calientes. Éstos hacen referencia a aquellos lugares donde se producen el mayor número de casos, pudiendo así, ampliar la vigilancia y prevenir, ya que se hace un aproximación de la hora en la que el delito se llevará a cabo, dando un margen de tiempo a la propia policía para hacer acto de presencia y así disuadir a los criminales. Estados Unidos es el pionero en este tipo de prevención, puesto que lleva años implantado en algunos estados como California, es el denominado Predpol[59], el cual crea mapas conceptuales a partir de los informes aportados de las patrullas policiales y facilita una hora y lugar.

Por otra parte, mediante la geoprevención también se estudian las ciudades y su geografía, es decir, se analizan las características arquitectónicas de las ciudades y sus medidas de seguridad, dando lugar a la obtención de resultados tales como que actualmente se cometen más delitos en las zonas urbanas que rurales, no porque en éstas últimas no hayan delincuentes, sino que se debe a la masificación de las ciudades y el desarrollo de sus características. Un ejemplo claro lo explica Robert Muggah[60] quien tras numerosos estudios y la creación del Instituto Igarapé en Río de Janeiro llegó a la conclusión de que la problemática delictiva se debía a determinados factores[61] como la desigualdad de ingresos, el desempleo juvenil, la urbanización, la informalidad y la impunidad y debilidad institucional. Estos parámetros hacen que algunas ciudades de América Latina tengan una alta tasa de violencia y le han servido a Muggah para mejorar tanto la urbanización como la calidad de vida, reduciendo enormemente el porcentaje de actos violentos.

5.2 Predicción de delitos

La predicción delictiva ha sido y será la herramienta más perseguida por la Criminología y los agentes de la ley, puesto que delito que no ocurre, víctima que no sufre, delincuente que no requiere pena y juicio no celebrado. A pesar de la existencia

[59]Veáse https://www.predpol.com/
[60] https://www.ted.com/talks/robert_muggah_how_to_protect_fast_growing_cities_from_failing
[61] Véase https://la.network/gastamos-mucho-en-seguridad-publica-pero-lo-hacemos-de-forma-ineficiente-robert-muggah/

de numerosas teorías que han contribuido a lo largo de los años a entender la mente criminal y cómo éste va a operar, entre las que cabe destacar la teoría de las actividades rutinarias[62] (Felson y Cohen,1979) y la del patrón delictivo[63] (Brantingham y Brantingham, 1993), con la existencia de la Inteligencia Artificial (IA), se están diseñando programas que podrían predecir el delito antes de que sucediese. Se trata de Minority Report[64] extrapolado a la vida real, con la diferencia de que en lugar de utilizar a personas que posean un don, se usan las cámaras de seguridad. Esta iniciativa fue probada hace un par de años en China, mediante la instalación de un software en las oficinas policiales y numerosas cámaras a lo largo de las calles. También colabora la compañía Cloud Walk, especializada en reconocimiento facial, lo que permite que se pueda seguir a una persona sospechosa o analizar los lugares de alto riesgo frecuentados por delincuentes. Tiene diversos usos, y supuestamente sólo es utilizada con aquellas personas que posean un perfil de alto riesgo, como por ejemplo exconvictos. Un ejemplo sería alertar de la adquisición de productos peligrosos o considerados necesarios para la comisión de un crimen, es decir, que una persona decida comprar una pala parece una situación común si tienes un jardín, pero que además compre guantes, cinta americana, cloroformo y cuerdas, resulta un poco sospechoso, y si a todo eso se le añade que se ha cambiado de ropa y las compras las ha realizado en distintas tiendas, parece que la actividad que vaya a realizar no estará relacionada con la jardinería, sino con el asesinato. En este supuesto, la policía sería alertada y gracias a la denominada “reidentificación personal” detectada aunque se modifique algún aspecto físico como el pelo o se ponga gafas. También proporciona la posibilidad de reconstruir el camino que ha hecho alguien y así descartarle como sospechoso.

[62] Intenta explicar los elementos necesarios para la comisión de un acto contrario a la ley. Éstos son un objeto deseado, un delincuente motivado y un guardián incapaz. Sin la presencia de una de las figuras, el delito no se cometería. Por ejemplo, en el supuesto de un hurto, si no existiese algo que pudiese ser deseado por la persona, aunque hubiese un guardián incapaz, el delincuente motivado no hurtaría, porque no quiere ese objeto. Si por el contrario, este sujeto tiene una buena motivación y el objeto es de su agrado, pero el guardián es capaz, no sucederá ya que éste último lo impediría. Por último, si a pesar de existir un objeto deseable y de un guardián incapaz, el delincuente no tiene esas ganas de hurtar, tampoco ocurrirá, puesto que no va a llevar a cabo ninguna acción.

[63] Expone que los lugares delictivos no son producto del azar, sino una elección del criminal de manera tanto consciente como inconsciente, ya que en este proceso se tiene en cuenta el factor ambiental que diferenciaba los espacios de actividad rutinaria de los delictivos, pero que daba lugar a que el criminal eligiese lugares conocidos o donde se sentía cómodo.

[64] Película protagonizada por Tom Cruise en la cual, gracias a la capacidad mental de tres hermanos la policía veía el crimen antes de que se cometiese, ya que éstos les proporcionaban el lugar, el nombre y la hora en la que iba a suceder, ofreciendo la oportunidad de que los delincuentes fuesen detenidos antes de ejecutar su crimen.

A pesar de todos los beneficios que aportaría esta tecnología, se debe reflexionar sobre la limitación que sufren las libertades individuales y el derecho a la intimidad. Estas han sido algunas de las críticas que ha recibido este sistema, puesto que la Policía puede ser conocedora de las rutinas, ubicación, lugar de trabajo, productos comprados e incluso amistades de una persona. Es más, los sospechosos detectados por este método pueden llegar a ser acusados en grado de tentativa, aunque se esté hablando de un mecanismo muy reciente, cuyo índice de fiabilidad y probabilidad de error aún no ha sido estudiada.

5.3 Reconstrucción de escenarios de crímenes

Esta herramienta radica en la posibilidad de grabar o fotografiar el escenario del crimen con drones pilotados por los propios especialistas y posteriormente reproducirlo. El dron permite obtener imágenes desde distintos ángulos de visión y sobre todo, desde el cielo, aportando una fotografía dificultosa hasta la invención de éstos. Esto es factible gracias al posterior uso de las gafas de realidad virtual, la cuales están equipadas con una tecnología capaz de mostrar en 3D el lugar del delito en ilimitadas ocasiones, conservando siempre los detalles tal y como fueron encontrados. Se considera una buena herramienta en el campo de la criminología, más concretamente en la criminalística, puesto que estando en un lugar distinto del crimen, por ejemplo en el laboratorio, pueden repetir infinitas veces la inspección técnico ocular. Además, es realmente útil en aquellos casos en que el delito se cometa en un espacio público como la carretera, vías de tren etc o surjan condiciones climatológicas adversas que provocarían la pérdida de numerosas pruebas, dado que siempre se podría volver al escenario virtualmente.

También existen programas que recrean de manera animada la narración del crimen según las pruebas recogidas. Para utilizar esta técnica se requiere una sala con ocho cámaras que capturan el movimiento y una persona que vista unos sensores que le permiten reproducir las acciones llevadas a cabo tanto por las víctimas como por el agresor. De esta manera se logra construir un vídeo que muestra de manera gráfica lo ocurrido, lo cual es muy positivo en la fase de juicio oral para que el tribunal o el jurado tenga una versión lo más parecida a la realidad de lo sucedido. La Policía Nacional cuenta con esta tecnología y la ha utiliza en aquellos casos que presentan

una gran complejidad como un tiroteo que terminó en un doble homicidio en un club de alterne en Valladolid[65].

5.4 Autopsias virtuales

La autopsia es el procedimiento que se lleva a cabo por los profesionales de Medicina forense, que consiste en la identificación de la causa de la muerte de la víctima, además, de la recolección de pruebas que se encuentren en el cadáver. Obviamente, dicho proceso conlleva la apertura de las distintas partes del fallecido para poder analizar los hallazgos y así determinar el motivo de su defunción, al igual que descubrir al responsable.

Hace más de una década se unieron dos disciplinas de la medicina para hacer posible la realización de una inspección corporal interna no invasiva, éstas son la radiología y forense, que juntas crearon la denominada "virtopsy[66]" o "virtopsia" en español. Es una técnica virtual que comenzó a utilizarse hace más de una década, en el Instituto Radiológico de la Universidad de Berna (Suiza) por el patólogo forense Michael Thali. Su finalidad era realizar autopsias sin necesidad del bisturí, únicamente utilizan técnicas propias de la medicina tradicional como la resonancia magnética, radiología, ultrasonido y tomografía computada. Una vez examinado el cuerpo, los datos son archivados en las memorias de los ordenadores y se crea una imagen virtual, en unas ocasiones en la propia pantalla del dispositivo, y en otras a nivel 3D.

Sus beneficios son infinitos, puesto que permite ejecutar la autopsia tantas veces como se desee, sin necesidad de preocuparse por los procesos de putrefacción ni tener que exhumar un cadáver antiguo. Además, resalta hematomas ocultos, facilita el estudio de trayectorias en caso de armas de fuego o punzantes, e incluso en las primeras si el proyectil resulta fragmentado como consecuencia del impacto con algún hueso, los diferentes trozos de metal serán observables en las imágenes, ya que este mecanismo localiza el metal. Asimismo, como toda la documentación obtenida a través de la autopsia virtual es almacenada, en el supuesto de tratarse de un asesino

[65] Véase La Sexta (2020) "Crímenes en 3D: la técnica de la Policía para reproducir a la perfección el escenario de un hecho delictivo"
[66] Véase La Razón https://www.larazon.es/historico/6687-autopsia-virtual-analizar-cadaveres-sin-mancharse-de-sangre-FLLA_RAZON_310863/

en serie, se simplificaría la comparación de las lesiones, porque únicamente se necesitará hacer uso de la superposición de imágenes.

6. Posibles soluciones o mejoras

A lo largo de este trabajo se ha ido mostrando la problemática que supone el ciberdelito para el mundo y para las propias víctimas. Por ello se constata que es imprescindible que se realicen cambios de manera inmediata, tanto con el propósito de aumentar la detención de los sujetos, como con la disminución de los casos mediante la prevención. Así pues, para que esta mejora sea real y eficiente es fundamental que se ejecute en los distintos grados existentes, es decir, a nivel global, nacional-autonómico e individual.

6.1 Nivel Global

No se debe de olvidar que el mundo está formado por diversos países, con sus consiguientes culturas y normas acorde a ellas. Existe una distinción entre cada una de las naciones con el resto, pero en nuestros días nos encontramos con un motivo que requiere una unión internacional, como lo es el vacío legal en la ciberdelincuencia. Éste es un enemigo común que sólo acaba de llegar, ya que tiene pensado quedarse y evolucionar hasta que se le frene. Pero, poco útil es que un estado obstaculice su desarrollo, si el resto no se implican. Por lo cual, la primera propuesta sería una legislación conjunta de todos los países en la que se establecieran las diferentes modalidades delictivas a través de la tecnología, su penología y de qué modo se debe proceder cuando se cometa una infracción internacional. De esta manera no existirían las lagunas jurídicas y todas las naciones se apoyarían, evitando así que los delincuentes eludiesen la justicia, además de que facilitaría enormemente su enjuiciamiento y detención, de igual modo que las víctimas sentirían que el sistema judicial realmente funciona.

En el supuesto en que esta legislación se redactase, también se podría instituir un equipo de especialistas provenientes de aquellos países que hubiesen firmado dicha declaración que fuesen los encargados de perseguir esta delincuencia. Se trataría de un grupo internacional con estudios o experiencia en diferentes ámbitos (criminología, informática, policía, derecho, psicología…) que se responsabilizarían de la detención de aquellas personas que cometiesen delitos informáticos en otros países distintos al

propio, es decir, a nivel global. Esto no significaría que las naciones perdiesen sus leyes propias ni que no tuviesen posibilidad de realizar juicios en casos de ciberdelincuencia, sino que en aquellos supuestos en que los afectados son organismos o personas de distinto estado o estados que el infractor, y que ello supone una ardua tarea en cuanto a detención y enjuiciamiento, operarían estos especialistas evitando problemas de jurisdicción.

6.2 Nacional y autonómico

En el caso de España, nos encontramos ante un sistema dividido en autonomías, con un gobierno centralizado. Esto significa que determinadas competencias pueden ser exclusivas del Estado y otras compartidas, por ese motivo se ha decidido agrupar estos dos niveles, ya que además, en este país existen las FFCCSS que operan a nivel nacional, como la Policía Nacional y Guardia Civil, mientra que la Local y Autonómica son propias de cada comunidad, dando lugar a la existencia en Cataluña de los “Mossos d’Esquadra”, mientras que en Madrid no se ha utilizado esa posibilidad.

Lo primordial, al igual que ocurre en el ámbito anterior, es una legislación acorde a la evolución de la sociedad. En estos momentos, tras las última reformas del CP se puede afirmar que España está bastante actualizada respecto a la ciberdelincuencia, pero esto no es sinónimo de que no haya asuntos que deba vigilar, como el creciente uso de drones, vehículos autónomos o el desbloqueo facial y dactilar de los smartphones. Es más, si las leyes no están equiparadas, y un tipo de delito no se haya contemplado en la normativa sucede un desamparo legislativo para las cibervíctimas, causando así una falta de seguridad que es lo opuesto a la finalidad del principio de legalidad, por el cual nos regimos. Hasta hace apenas unos 5 años eso ocurría, y los afectados por determinada delincuencia informática eran testigos de cómo sus casos se sobreseían, aunque ello les hubiese supuesto problemas psicológicos, a la vez que la justicia comprobaba como un delincuente quedaba libre sin ningún tipo de pena. Por todo ello es realmente imprescindible que se cambie la manera de añadir nuevos artículos, es decir, se ha acostumbrado a que las medidas de protección siempre ocurran después de que haya sucedido el incidente, cuando perfectamente se era consciente de que esos delitos iban a existir, y no se encontraban tipificados en el marco normativo. Así pues, sería recomendable que se estudiase la situación actual y se adquiriesen esas modificaciones antes de la desgracia.

Obviamente para lograr el anterior objetivo, es necesario la colaboración de las creadoras de los dispositivos, dicho de otro modo, las propias empresas. El legislador carece de los conocimientos informáticos, por ello precisa documentación de quienes desarrollen los avances tecnológicos. Existe la figura del Compliance que es el encargado de que todo el personal que conforma una organización, cumpla la normativa y en especial el código ético, actuando siempre acorde al derecho vigente. Sin embargo, también anticipan la responsabilidad penal, por lo que si cada vez que se inventara un nuevo artefacto o a uno antiguo se le añadiesen características innovadora, esto fuese puesto en conocimiento del legislador, éste podría analizar si la legislación contempla esas conductas, o si por el contrario se requiere una ampliación.

Por otra parte, sería muy positivo la inclusión de asignaturas o contenidos relacionados con la ciberdelincuencia en el plan formativo de determinados grados universitarios asociados a esta problemática, especialmente en materia de derecho, criminología e informática, además de psicología y sociología, entre otras, ya que las primeras son las responsables de construir barreras que logren frenar este fenómeno, mientras que las segundas se centran más en la comprensión de sus autores. Pero con la educación no es suficiente, se debe exigir, de igual modo, el reconocimiento de las advertencias y conclusiones que se extraigan de las investigaciones, y no obviarlas, como ha ocurrido en otras ocasiones (ejemplo de ello, en 2014 cuando el informático y hacker Jan Krissler alertó de las deficiencias de seguridad en la biométrica, e incluso reprodujo las huellas dactilares de la Ministra de defensa alemana, haciendo uso únicamente de un programa informático y fotografías públicas de ésta[67]).

Seguidamente, es el turno de aquellos profesionales que ya se encuentran trabajando como policías, jueces, fiscales, magistrados, personal del ayuntamiento… entre otros. Aquí se debe proporcionar una formación, para unos de prevención como sería el caso de un ayuntamiento que pudiese protegerse de posibles hackeos o sabotajes, y para otros de actuación, en el resto de ejemplos. No hace referencia a que estos expertos no estén capacitados, sino a que es una novedad inexistente hace unos años, por lo que personas que llevan ejerciendo un tiempo considerable no han podido recibir estos conocimientos. Asimismo, es indispensable destacar la carencia

[67] Véase El Mundo
https://www.elmundo.es/economia/2014/12/30/54a19eea268e3ec7718b4592.html

de medios que llevan años reclamando las FFCCS españolas[68], y que ello conlleva una mayor dificultad en la lucha contra el cibercrimen, por consiguiente resulta imprescindible una inversión en recursos[69] (tanto técnicos como formativos) para conseguir una equiparación con los ciberdelincuentes, y no estar siempre diez pasos por detrás.

Ligado con lo comentado, sería muy positivo publicitar las distintas maneras que posee la ciudadanía de ponerse en contacto telemáticamente con las diferentes secciones informáticas propias de las FFCCS[70], para informar del conocimiento de un acto ciberdelictivo y que éste fuese investigado. No obstante, aunque estos grupos existen, la sociedad no es conocedora de que tiene a su alcance esta herramienta y que el colaborar notificando, no es equivalente a denunciar ni asistir como testigo al juicio oral, simplemente es alertar para que ninguna persona se convierta en cibervíctima. Por este motivo es recomendable que los medios de comunicación difundan estas técnicas, y que visibilicen notoriamente las detenciones y sentencias dictaminadas sobre un ciberdelincuente, para mostrar a la ciudadanía que cometer un delito cibernético no es sinónimo de impunidad y dar una imagen de ciberseguridad.

Para finalizar, nos centramos en los más vulnerables, los menores. Ellos son las principales cibervíctimas de delitos tan graves como la pornografía, por ello han de estar educados de los peligros de las TICS. En numerosos centros educativos se está llevando a cabo la iniciativa de promover un uso seguro y responsable, tanto de internet como de los dispositivos informáticos, entre la población más joven mediante charlas y conferencias de distintas asociaciones y las propias FFCCS. Aunque este proyecto es una maravillosa idea, también tiene que llegar a las familias, ya que de nada sirve que en los colegios e institutos se enseñe la correcta utilización de los aparatos, si en los hogares se desconoce este asunto o no se establecen normas. Por

[68] Véase El Independiente https://www.elindependiente.com/futuro/2019/11/18/la-lucha-de-la-policia-nacional-contra-el-cibercrimen-los-malos-tienen-mas-recursos/

[69] Resulta importante destacar la figura del agente encubierto informático, el cual siendo un funcionario se infiltra voluntariamente en la Red con la finalidad de obtener información sobre los ciberdelincuentes para poder recopilar pruebas y llevarles ante la justicia. Para ampliar el tema consultar: Bueno de Mata, F. (2012). El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia.

[70] Entre ellas la Brigada Central de Investigación Tecnológica de la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía (C.G.P.J), Grupo de Delitos Telemáticos de la Guardia Civil (GDT), Sección Central de Delitos en Tecnologías de la Información de la Ertzaintza (SCDTI), Unidad Central de Delitos Informáticos de los Mossos d'Esquadra o el Grupo de Apoyo Tecnológico de la Policía Foral de Navarra.

ello, una buena propuesta sería que esta información llegara a todas las personas adultas que estén a cargo de un menor, para que se les instruya cuáles son los límites que se deben de imponer y cómo actuar en el supuesto de que un adolescente sea víctima o agresor.

6.3 Individual

Obviamente, a nivel individual lo idílico sería que aquellas personas que utilizan las herramientas electrónicas para fines ilícitos, dejasen de quebrantar la ley, de esta forma se acabaría con la problemática, puesto que si los delincuentes, no cometen delitos no habría proceso ni víctima. No obstante, esta idea, aunque muy interesante, sigue siendo muy utópica, por lo que, desgraciadamente el poder de actuación recae en las víctimas, aunque, se debe recalcar que una víctima nunca es culpable del delito. Por dicho motivo se recomienda a la ciudadanía[71]:

a) Sexting: evitar facilitar imágenes o vídeos que incluyan contenido sexual, borrarlas en un período ínfimo (favorece que la fotografía no se quede guardada en el teléfono del receptor), no mostrar la cara ni un fondo conocido, en el supuesto de recibir una copia de un tercero no reenviarla,

b) Hackeo y sabotaje: instalar antivirus que contengan protección ante gusanos, firewall, antibanner, evitar acceder a páginas webs poco fiables, intentar no introducir contraseñas en webs no oficiales de entidades bancarias, si se hace uso de una red wifi pública es recomendable que sea para búsquedas no relacionadas con contraseñas o transacciones.

c) Menores: instalar el control parental en los dispositivos que vayan a hacer uso, educar en la prevención y autoprotección, mantener un clima de confianza que anime al menor a sincerarse en caso de que se encuentre en alguna de estas situaciones, supervisar sus búsquedas y perfiles sin llegar a eliminar su intimidad.

d) Cyberstalking: utilizar un pseudónimo, restringir la privacidad a personas conocidas, evitar compartir información personal (dirección, teléfono..),

[71] La pornografía no se enumera porque ha sido incluida en el apartado c)Menores, ya que son éstos quienes lo facilitan por una parte, y por otra los creadores pueden ser los propios cibercriminales mediante programas informáticos, y puesto que no se puede llevar a cabo una prevención con los delincuentes, se ha considerado innecesario su mención en un apartado especial.

bloquear, silenciar o eliminar a aquellos usuarios molestos y reportar este acoso a la red social.

e) Estafa informática: asegurarse de que la página web empieza por https://; si se recibe un email con una dirección de su banco no acceder a través de ella, sino que es mejor escribir la url directamente en el navegador, en caso de sospecha ponerse en contacto con la tienda, entidad etc, de ningún modo enviar dinero a personas que no sean conocidas, tener cautela a la hora de empezar un romance a través de las redes sociales.

Pero sobre todo, lo más importante es que en el instante en que una persona sea conocedora de un delito de esta índole, ya sea víctima o un tercero, interponga una denuncia o ponga en conocimiento de las autoridades policiales la situación, ya que se gracias a esta actuación se agilizará la labor de investigación y posterior enjuiciamiento de los responsables, además de disminuir las consecuencias.

7. Conclusiones

PRIMERA: Las nuevas tecnologías han dado lugar a un traslado delictivo del mundo físico al espacio cibernético.

SEGUNDA: Los casos de delitos informáticos no se van a reducir, al contrario, han aumentado, se están intensificando y se incrementarán hasta niveles inimaginables conforme vayan transcurriendo los años, ya que las actuales generaciones manejan con facilidad estos artefactos y las antiguas tienen a su alcance la formación necesaria para introducirse en este ámbito.

TERCERA: Se ha producido un cambio en el perfil del delincuente, puesto que ya no es tan relevante el componente físico, como el intelectual, dado que en el ámbito de los ciberdelitos, se requieren más las habilidades informáticas que las violentas, intimidantes o manuales.

CUARTA: La ciberdelincuencia es más económica, dañina, rápida y difícil de impedir que la corpórea, consecuencia de que cualquier persona que posea un aparato con conexión a internet puede realizarla. Además, de presentar numerosas complicaciones a la hora de detener a los autores y enjuiciarlos.

QUINTA: Las consecuencias generadas por la comisión de esta tipología delictiva son sumamente perjudiciales tanto a nivel de sociedad (económico) como a nivel personal (víctima directa), pues una caída de los servidores puede comportar la pérdida de millones de euros y la difusión de una foto puede tener una repercusión mundial.

SEXTA: Para una protección eficaz se requiere que todos los países cooperen y colaboren logrando así la redacción de una legislación conjunta que posibilite la detención, y posterior enjuiciamiento, de los ciberdelincuentes. De esta forma, se mostraría a la comunidad que la comisión de un delito, aunque se realice a través de la red no queda impune y que no se pueden aprovechar del anonimato.

SÉPTIMA: Al ser actos recientes es preciso una inversión en la investigación exhaustiva de este fenómeno llevada a cabo por profesionales del derecho, la criminología, sociología, psicología e informática con el fin de entender su origen y motivaciones, y así poder desarrollar perfiles cibercriminales, los cuales perfeccionarán su prevención y mejorarán la actuación de las FFCCS.

8. Bibliografía

Cuerda Arnau, M. L., & Fernández Hernández, A. (2016). *Menores y redes sociales: Ciberbullying, ciberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de violencia en la red*. Valencia: Tirant lo Blanch.

Miró Llinares, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid, Marcial Pons.

Revistas y Recursos Online

Bueno de Mata, F. (2012). El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia. Los retos del Poder Judicial ante la sociedad globalizada. *Dialnet*. Actas del IV Congreso Gallego de Derecho Procesal (I Internacional) A Coruña, 2 y 3 de junio de 2011, Agustín Jesús Pérez-Cruz Martín (dir.), Xulio Ferreiro Baamonde (dir). A Coruña: Universidade, 2012, p. 295-306. ISBN: 978-84-9749-501-1

Carlini, A. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. *Bie3: Boletín Ieee,* (2), p.950-966.

Collell i Caralt, J. y Escudé Miquel, C. “El acoso escolar: un enfoque psicopatológico” extraído de Olweus, D. (1983). “Low school achievement and aggressive behaviour in adolescent boys”. En D. Magnusson y V. Allen (Eds.), *Human Development. An interactional perspective*, New York: Academic Press.

Cuesta González A, Cyberbullying: Perfil del agresor. Agencia Legislativa.

“Cyberbullying: los agresores son amables en persona pero ofensivos en las redes sociales” (2018), Noticias de la Ciencia y la Tecnología.

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology*, *8* (4), 389-406.

Fundación Ayuda a Niños y Adolescentes en Riesgo (ANAR)

García-Pablos de Molina, A. (1989). La aportación de la Criminología. *Eguzkilore, Cuaderno del Instituto Vasco de Criminología*. Número 3,P.79-94.

Interpol

Miró Llinares, F. (2013). “Cibercrimen, cibercriminales y cibervíctimas”. *Universitat Oberta de Catalunya*.

Méndez Gago, S., González Robledo, L., Pedrero-Pérez, E. J., Rodríguez-Gómez, R., Benítez-Robredo, M. T., Mora-Rodríguez, C., & Ordoñez-Franco, A. (2018). Uso y abuso de las Tecnologías de la Información y la Comunicación por adolescentes: Un estudio representativo de la ciudad de Madrid.

Motta-Ramírez, G. A., Alva-Rodríguez, M., & Herrera-Avilé, R. A. (2013). La autopsia virtual (virtopsia): La radiología en la Medicina Forense. *Revista de Sanidad Militar*, *67*(3), 115-123.

Muggah R. (2018). “Gastamos mucho en seguridad pública pero lo hacemos de forma ineficiente”. *LA.Network.*

Muggah R. (2014). How to protect fast-growing cities from failing. Ted Talks.

Predpol

Real Academia de la Lengua Española

Rodríguez Caro, M. (2015). Estafa informática. El denominado phishing y la conducta del "mulero bancario": categorización y doctrina de la Sala Segunda del Tribunal Supremo. *Noticias jurídicas.*

Tamarit Sumalla Josep M. (2016). «Presentación». En: «Ciberdelincuencia y victimización» [revista en línia]. IDP. Revista de Internet, Derecho y Política. N.º 22, págs. 30-31. UOC.

Vázquez, González C. & Soto, Urpina C. (2013). El análisis geográfico del delito y los mapas de la delincuencia. *Revista de derecho penal y criminología*, (9), p.419-448.

Willard, Nancy E. *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research press, 2007. En Río-Pérez,

Legislación

Auto del Juzgado de Primera Instancia e Instrucción nº 1 de 15 de marzo de 2013.Véase sentencia

Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011.

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. BOE-A-2010-14221

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

Noticias

'Anonymous', ¿quiénes son y cómo actúan? (2012). *Radiotelevisión Española.* Enlace:https://www.rtve.es/noticias/20120228/anonymous-quienes-son-como-actuan/438765.shtml

Chema Alonso, el conocido "hacker" de Telefónica, doctor honoris causa (2020). *El País.* Recuperado de: https://cincodias.elpais.com/cincodias/2020/01/28/companias/1580232696_339551.html

Crímenes en 3D: la técnica de la Policía para reproducir a la perfección el escenario de un hecho delictivo. (2020). *La Sexta*. Enlace:

https://www.lasexta.com/programas/mas-vale-tarde/expediente-marlasca/crimenes-en-3d-la-tecnica-de-la-policia-para-reproducir-a-la-perfeccion-el-escenario-de-un-hecho-delictivo_202001235e29e53a0cf20ef4411c1e7c.html

El INE seguirá los movimientos de los móviles de los españoles durante ocho días para un estudio (2019). *Radiotelevisión Española (RTVE).* Recuperado de: https://www.rtve.es/noticias/20191029/ine-seguira-movimientos-moviles-espanoles-durante-ocho-dias-para-estudio/1986520.shtml

El 'timo' sobre la DGT del que advierte la policía en plena crisis del coronavirus (2020). *Cadena SER.* Recuperado de: https://cadenaser.com/ser/2020/03/29/sociedad/1585497118_052793.html

Facebook reconoce la filtración de datos de más de 120 millones de usuarios (2018). *El Mundo. Recuperado de* https://www.elmundo.es/tecnologia/2018/06/30/5b35f2f4468aeb22438b457d.html

Fiter, M. (2019). La lucha de la Policía Nacional contra el cibercrimen: "Los malos tienen más recursos". *El Independiente*. Recuperado de https://www.elindependiente.com/futuro/2019/11/18/la-lucha-de-la-policia-nacional-contra-el-cibercrimen-los-malos-tienen-mas-recursos/

Les roban todas sus pertenencias por publicar una foto en Facebook (2016). *ABC*. Enlace:https://www.abc.es/recreo/abci-roban-todas-pertenencias-publicar-foto-facebook-201608081854_noticia.html

Llorente, F. & Aguilera, C. (2018). ¿Hay más odio en las redes sociales? *Radiotelevisión Española (RTVE).* Recuperado de: http://www.rtve.es/las-claves/el-odio-en-las-redes-sociales-2018-04-26/

No hay una rica heredera que done su fortuna a desconocidos: es otra estafa (2020). *La Vanguardia.* Recuperado de: https://www.lavanguardia.com/vida/20200416/48565386077/no-hay-una-rica-heredera-que-done-su-fortuna-a-desconocidos-es-otra-estafa.html

Ollero,D. (2014) Un hacker reproduce la huella de la ministra de defensa de Alemania. *El Mundo.* Recuperado de https://www.elmundo.es/economia/2014/12/30/54a19eea268e3ec7718b4592.html

Olvido Hormigos, el caso que cambió el Código Penal sobre la difusión de vídeos sexuales sin consentimiento (2016). *La Sexta.* Recuperado de: https://www.lasexta.com/noticias/sociedad/olvido-hormigos-caso-que-cambio-codigo-penal-difusion-videos-sexuales-consentimiento-video_201905305cef93a50cf21b72629f1c3f.html

Pérez, J. (2018) ¿Cuánto odio hay en Twitter? No mucho, pero es constante y hay para todos. *El País*. Recuperado de: https://elpais.com/tecnologia/2018/11/01/actualidad/1541030256_106965.html

Pérez, P. (2010). Autopsia virtual: analizar cadáveres sin mancharse de sangre. *La Razón.* Recuperado de: https://www.larazon.es/historico/6687-autopsia-virtual-analizar-cadaveres-sin-mancharse-de-sangre-FLLA_RAZON_310863/

Sube una foto de dinero a Facebook y roban su casa (2012). *Antena 3.* Enlace: https://www.antena3.com/noticias/tecnologia/sube-foto-dinero-facebook-roban-casa_201205295754e5454beb2837bbff7363.html

Un alemán obsesionado por Internet mató un británico (2009). *El Economista.* Enlace:https://www.eleconomista.es/empresas-finanzas/noticias/1236890/05/09/Un-aleman-obsesionado-por-Internet-mato-un-britanico.html

Un virus informático utiliza como señuelo a la Policía para cometer estafas (2012). *Radiotelevisión Española (RTVE).* Recuperado de: https://www.rtve.es/noticias/20120130/virus-informatico-utiliza-como-senuelo-policia-para-cometer-estafas/493944.shtml