FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

Ciberdelincuencia; marco normativo y respuesta policial

Autor/a: José Antonio Salazar Mendoza
Director/a: David Seoane

Madrid
2022/2023

RESUMEN

En un mundo cada vez más informatizado, nuestras vidas han evolucionado, de igual manera las TIC han provocado la evolución en la comisión de delitos. Los delitos tradicionales han evolucionado hasta tal punto de considerarse la principal amenaza a la seguridad nacional.

Las TIC proporcionan grandes ventajas, no obstante, puedes utilizar esas ventajas para cometer delitos que deben estar tipificados y cuyas consecuencias jurídicas deben estar claramente reguladas. A este nivel, la preocupación de España como del resto de países se ha centrado en encontrar unas claves para proporcionar una navegación segura en la Red.

En este trabajo de investigación se analiza el concepto de ciberdelincuencia, las características que merecen especial atención a la hora de regularlos. Por otro lado, se presenta el marco normativo a nivel europeo y nacional, que protege a los usuarios de la Red a nivel legislativo, y las instituciones que se encargan de perseguir tales delitos.

PALABRAS CLAVE: Ciberdelincuencia. Ciberdelitos. TIC. Marco legislativo. Convenio de Budapest. Estrategia de Ciberseguridad. Delitos informáticos.

ABSTRACT:

In an increasingly computerised world, our lives have evolved, just as ICTs have led to an evolution in the commission of crime. Traditional crimes have evolved to the point where they are considered the main threat to national security.

ICTs provide great advantages, however, you can use those advantages to commit crimes that must be criminalised and whose legal consequences must be clearly regulated. At this level, Spain's concern, like that of other countries, has focused on finding keys to provide safe surfing on the Internet.

This research work analyses the concept of cybercrime and the characteristics that deserve special attention when it comes to regulating them. On the other hand, it presents the regulatory framework at European and national level, which protects Internet users at the legislative level, and the institutions in charge of prosecuting such crimes.

KEY WORDS: Cybercrime. ICT. Legislative framework. Budapest Convention. Cybersecurity strategy. Cyber-crime.

INDICE

1. **INTRODUCCIÓN**.

Actualmente no podemos concebir el mundo y nuestro futuro sin el desarrollo tecnológico que hemos alcanzado y que nos queda por alcanzar. Las nuevas tecnologías se han abierto camino en prácticamente todas las facetas de nuestro día a día, la comunicación, los servicios, la economía, etc., todo gira en torno al desarrollo tecnológico que se posea, creando sociedades en gran medida dependientes de estas tecnologías.

Se trata de un área en continuo desarrollo, en enero de 2022 había 4950 millones de usuarios de internet en el mundo, lo que hace una cifra cercana al 62,5% de población mundial con acceso a internet. Atendiendo al tiempo dedicado al día está cerca de 7 horas diarias a nivel mundial. Estas cifras, según la agencia "*We Are Social*" en su informe anual Digital 2022.

Este desarrollo en las tecnologías de la información y telecomunicación (TIC) ha abierto un nuevo espacio donde relacionarse al que se ha denominado "ciberespacio", para la Real Academia Española, el ciberespacio se entiende como el "ámbito artificial creado por medios informáticos", en este espacio o realidad virtual creada por medios informáticos es donde se agrupan los usuarios, webs, redes sociales y todo el conjunto de servicios de los que dispone Internet. Se trata de un espacio global donde no hay fronteras por lo que debemos ser conscientes de todos los peligros que este nuevo espacio puede abrir.

Gracias estas nuevas formas de relacionarnos, a través de la web, dejamos una gran cantidad de información de nuestra vida personal fuera de nuestra intimidad, esta información se está volviendo un bien cotizado por diferentes entidades, desde únicamente conocer nuestros gustos y mandarnos anuncios para satisfacer ciertas necesidades hasta información más delicada que puede suponernos un gran agravio.

Atendiendo a Informe de Criminalidad informática en España (2021) el uso de Internet llega al 99,7% en población entre 16 y 24, siendo un porcentaje mayor de 90% en todos los rangos de edad salvo la franja de 60 años en adelante. Los menores de 15 años llegan al 95,1%.

Por esta razón, paralelo al avance de la tecnología han ido desarrollándose comportamientos delictivos cada vez más elaborados y peligrosos que atentan sobre un gran número de personas, estos datos expuestos anteriormente nos hablan de un importante número de usuarios conectados que pueden ser potenciales víctimas de un nuevo nicho delincuencial como es el uso de las nuevas tecnologías, puesto que, dotan al

infractor de un espacio de anonimato y de indeterminación geográfica que provoca unas grandes dificultades a la hora de la investigación policial.

Las nuevas tecnologías han generado un espacio donde la relación se vuelve más rápida y sencilla, rompiendo las barreras físicas de la distancia y el tiempo.

La vida en la "Sociedad de la Información", según Acurio del Pino, hace patente que los delitos informáticos pueden suponer un gravísimo daño a nuestra forma de vida, por lo que la importancia que debemos otorgar a nuestros equipos informáticos es cada vez mayor con el objetivo de que seamos capaces de defendernos. Los delitos informáticos siguen características comunes; el bajo coste, los bajos conocimientos que son necesarios para delinquir, el bajo riesgo que tiene el agresor y la gran efectividad que tienen este tipo de delitos, si a todo esto le unimos el alto número de víctimas potenciales es necesario la atención desde el ámbito criminológico para estudiar esta tipología delincuencial.

Por tanto, habrá que atender a la forma de perseguir y castigar los delitos, legislando a favor de una mayor protección de los usuarios en la red, buscándose una ley efectiva que ayude a castigar y prevenir la delincuencia informática. Uno de los principales obstáculos que se encuentran a la hora de legislar es que los gobiernos de todos los países deben trabajar de forma coordinada ante esta amenaza, puesto que una de las características de esta delincuencia es que existe una indeterminación geográfica, la dificultad de localizar el delito, unido a la disparidad de leyes que pueden encontrarse entre los países hace que se abran cada vez más oportunidades para las conductas delictivas.

Por otro lado, además de la seguridad jurídica necesaria, habrá que atender a los medios y recursos que deberán formalizarse en nuestros Fuerzas y Cuerpos de Seguridad del Estado para investigar de forma óptima tales actos.

Es, por todo lo mencionado, cada vez más necesario el hecho de educar en una cultura informática puesto que no vamos a poder hacer desaparecer tales delitos ni el medio que usan ya que las nuevas tecnologías han venido para quedarse y aprovecharnos de todo su potencial.

Con esto me planteo una serie de objetivos que apoyen lo que considero que es necesario saber para empezar a entender la gravedad de la ciberdelincuencia, además de exponer en este texto las posibles leyes que nos protegen y medidas policiales que se encargan de salvaguardar nuestra información personal en el ciberespacio.

En primer lugar, el objetivo base sería hacer una breve descripción de la evolución que ha sufrido la ciberdelincuencia. Atendiendo a datos nacionales e internacionales a cerca de las víctimas de este tipo de delitos.

En segundo lugar, el objetivo será recoger la normativa europea y nacional en la que se encuadran esta tipología delictiva, así como las estrategias adoptadas por la Unión Europea y por España para ver cómo estas pueden coordinarse con el fin de brindar una estrategia más completa de defensa de los usuarios de Internet.

El tercer objetivo será definir aquellos organismos, instituciones o actuaciones que están trabajando en España, ofreciendo un pequeño análisis sobre las mismas de forma que se encuentren concentrados los recursos de los que podemos beneficiarnos los ciudadanos frente a la tipología delictiva descrita.

Y, por último, el objetivo más ambicioso y a modo de conclusiones, atender a la prevención de estos delitos, dando posibles formas de acción para evitar la victimización.

2. CONCEPTO DE CIBERDELINCUENCIA

Las Tecnologías de la Información y de la Comunicación (TIC) hacen referencia al conjunto de herramientas y recursos tecnológicos que permiten procesar, almacenar, recuperar y presentar información, son los canales o los soportes que utilizamos para transmitir y almacenar información. Lo primero que deberemos entender para comprender la importancia del presente trabajo es que la información ha pasado a convertirse en un valor económico (Acurio del Pino). Es por esto por lo que los países han ido introduciendo en sus legislaciones políticas para controlar tal flujo de datos con el objetivo de proteger los derechos e intereses de sectores públicos y privados.

Estas nuevas tecnologías y su implantación en nuestra sociedad hacen florecer su uso con intenciones maliciosas como ocurre con toda actividad humana. La informática, por tanto, no es ajena al uso indebido de ella misma por parte de la sociedad.

Para entender los ciberdelitos es necesario partir de una definición que recoja la complejidad de tal tipología delictiva.

Definiciones.

La definición más sencilla de ciberdelincuencia, atendiendo a esto, sería el uso de las nuevas tecnologías de la información para la comisión de crímenes tales como fraude, robo, espionaje, suplantación, etc. Esta sería la definición más común, pero existen multitud de ellas como expone en su artículo "Delitos Informáticos. Generalidades" del Dr. Acurio, por ejemplo:

- Según Tiedemann, delincuencia informática no sería más que el conjunto de actos antijurídicos ante la ley vigente que utilizan medios informáticos de procesamiento de datos.
- Para María Cinta del Castillo y Miguel Ramallo el delito informático sería "*una acción dolosa que provoque un perjuicio a una persona o entidad en cuya comisión intervienen dispositivos utilizados en actividades informáticas*"
- Para Marcelo Huerta y Claudio Libano, la definición de delitos informáticos sería el conjunto de acciones u omisiones tipificadas en el código penal como antijurídicas y dolosas, cometidos por una persona o una persona jurídica realizadas mediante un sistema de tratamiento de la información con el objetivo de producir un perjuicio en la victima a través de "atentados a la sana técnica informática", produciendo lesiones a distintos valores jurídicos y un beneficio en el agresor sea o no de carácter patrimonial, actuando con o sin ánimo de lucro.

De todas las definiciones nos quedaremos con la conclusión que obtiene el Dr. Acurio del Pino, definiendo la ciberdelincuencia como "acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en riesgo un bien jurídico cualquiera".

La definición más aceptada es la que se obtiene del Convenio sobre cibercriminalidad de Budapest, el cual definía los ciberdelitos como "actos que atentan contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos"

Miró Llinares (2012) menciona que el término "delitos informáticos" se ha sustituido por cibercrimen o cibercriminalidad. Estos términos están compuestos por la palabra "Cyber"

que proviene del término ciberespacio, siendo este el espacio virtual que en el que se ubican todos los usuarios, redes sociales, etc., creado con medios cibernéticos.
Como se puede ver en esta breve muestra, las definiciones de este fenómeno son diversas y no hay un consenso claro. Es por esto que las normas penales aplicadas no se pueden ajustar a una definición tan indeterminada el objetivo de los legisladores es tipificar todas las conductas delictivas para dotar de respuestas claras y proteger a la sociedad.

Tipologías de delitos informáticos.

El Convenio sobre la Ciberdelincuencia de 2001 separa los delitos informáticos en cuatro tipologías:

I. Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Serían las conductas de acceso ilícito a sistemas, intercepción e interferencia de datos y abuso de dispositivos. Artículos del 2 al 6.
II. Delitos informáticos. Donde encontraríamos delitos como la falsificación informática y el fraude informático, en los artículos 7 y 8.
III. Delitos relacionados con el contenido. Comprende las conductas relacionadas con la pornografía infantil en la Red. En el artículo 9.
IV. Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines. En el artículo 10.

En el año 2003, se desarrolló el Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos dando un encuadre a los tipos delictivos racistas y xenófobos que se hallaban en crecimiento, este protocolo fue incluido dentro de los delitos relacionados con el contenido.
La creación de este convenio fue por una necesidad social, las TIC destacan positivamente en que permiten la comunicación instantánea entre personas de todo el mundo eliminando fronteras, pero, igual que son características positivas, la masividad, inmediatez y anonimato forman un combinado de características que potencian el delito. Las mismas características que consideramos positivas son las que aprovechan los delincuentes para delinquir, ya que cometer esta tipología delictiva puede otorgar un mayor beneficio que la comisión de delitos considerados tradicionales.

Los delitos clásicos como puede ser el acoso sexual ya existía previo a Internet, sin embargo, mediante este medio, a día de hoy el delincuente puede realizarlo de forma masiva, instantánea, ocultando su localización y de forma anónima.

Características de los ciberdelitos.

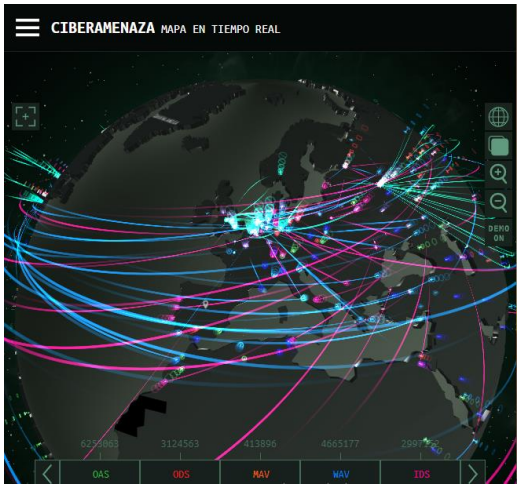
Los ciberdelitos comparten las siguientes características:

I. Anonimato.

El uso de las TIC, en especial en redes sociales, permite la creación de perfiles que dificulten la identificación de los usuarios, quedando oculta su identidad real. Para esta característica no es necesario tener una gran habilidad o conocimientos en materia de internet. No obstante, el conocer de informática permite además de cometer el hecho delictivo de forma anónima, encubrir tal delito. Esto provoca dificultad en su persecución quedando en muchas ocasiones impune.

II. Indeterminación geográfica.

Las TIC permiten el intercambio de mensajes, el intercambio de información, de manera instantánea, desde cualquier lugar del mundo. De tal forma, el delincuente puede encontrarse lejos de la víctima, en otro país, puesto que no hay regulación en este sentido. Es por ello que el derecho internacional cobra gran importancia a la hora de legislar materia común para todos los países con el fin de regular esta indeterminación geográfica ya que la ausencia de regulación es una de los aspectos que los delincuentes informáticos aprovecharán. De igual manera, los diferentes tipos de normativas según el país en el que se encuentre la víctima y el agresor favorecen la comisión de los delitos al tener disparidad de leyes.



Uno de los ejemplos más visuales para entender esta característica nos la puede dar la web Cybermap (https://cybermap.kaspersky.com/es) donde se puede ver el flujo de amenazas en línea que sufren los diferentes países en tiempo real. (Captura realizada de la web "Cybermap" el día 31 de enero de 2023)

III. Inmediatez.

El delito puede ser cometido de manera muy veloz, en el mismo momento en el que el delincuente esté llevando a cabo la acción el delito se está consumando, es cuestión de segundos. De igual manera que es inmediato el hecho de enviar y recibir mensajes es inmediato la capacidad de hacer desaparecer las huellas de tal delito. Provocando dificultades en su seguimiento.

IV. Masivo.

Característica que hace referencia a la difusión masiva de información que permiten las TIC.

V. Pluriofensivo.

Es posible afectar a más de un bien jurídico protegido a la vez en una misma acción.

VI. Facilidad de comisión de delitos.

Este tipo de delitos son muy fáciles de cometer, puesto que se necesitan muy pocos recursos y conocimientos para que el infractor delinca. Con tener un dispositivo electrónico y conexión a Internet es sencillo realizar una acción delictiva.

Perfil del delincuente informático.

Con el fin de comprender mejor los diferentes tipos de delincuentes informáticos, conocidos como “Hackers” se enumeran los perfiles más comunes según su comportamiento. El objetivo de estos delincuentes es encontrar vulnerabilidades y fallos en la seguridad de los sistemas informáticos y aprovecharlos para su propio beneficio.

Atendiendo a la ética con la que operan podemos encontrarnos tres tipos; Black Hat Hacker, Grey Hat Hacker y White Hat Hacker. (*7 tipos de hackers*, 2022)

Los Black Hat Hackers hacen referencia a aquellos que no tienen ningún tipo de ética de comunidad, buscan su propio beneficio. Por lo contrario, los White Hat Hackers son aquellos que encuentran los fallos de los sistemas informáticos e informan de ellos a las autoridades para solucionarlos. Se diferencian de los Grey Hat Hackers en que estos informan a las autoridades y llegan a acuerdos económicos para solucionarlos, tienen los conocimientos de un Black Hat Hacker, pero no buscan aprovecharse de los fallos para cometer delitos.

Según el tipo de delito que cometen podemos diferenciar diferentes tipos de hackers, los más comunes serían:

- Instaladores de Bots, quienes buscan controlar equipos informáticos a través de la instalación de software maliciosos.
- Carders, buscan robar la identidad y cometer fraudes mediante la suplantación de identidad, como puede ser fraude por medio de tarjetas de crédito. Consiguen la información y realizan transacciones encubriendo su identidad, causando perjuicio a la víctima a la que suplanta la identidad.
- Ciberpunks, se dedican a alterar sistemas informáticos públicos, ridiculizando a las víctimas y alterando tales sistemas públicos.
- Insiders, son empleados o antiguos empleados que actúan desde dentro de la compañía utilizando su conocimiento en el sistema informático para acceder y obtener información confidencial para perjudicar a su empresa.
- Phisher, son aquellos que utilizan correos electrónicos o mensajes para comunicarse con sus víctimas, engañando a las víctimas haciéndose pasar por fuentes confiables como bancos.

3. MARCO JURIDICO DE LA CIBERDELINCUENCIA

a) El Convenio sobre la Ciberdelincuencia o Convenio de Budapest

Motivado por las amenazas que implica el desarrollo de la informática y el abanico de posibilidades de delinquir que presenta, junto con las características mencionadas anteriormente que permiten actuar al delincuente de forma masiva, instantánea, ocultando su localización y de forma anónima, surge el Convenio del Consejo de Europa sobre Ciberdelincuencia, llevado a cabo en Budapest, Hungría, el 23 de noviembre de 2001. Con ello se pretendía realizar una base común con la que legislar en los países que lo ratificaron, para hacer frente de manera común esta tipología delictiva.

El Convenio entró en vigor el 1 de julio de 2004, dando respuesta a una necesidad imperiosa de buscar medios para luchar, de manera comunitaria entre todos los países miembros, contra los ataques informáticos, permitiendo adoptar políticas penales comunes para dotar de seguridad a la sociedad. Lo que consiguió tal convenio fue crear una política común que funcionara de modelo para que todos los países que estuvieran adheridos, fueran europeos o no, creasen una legislación propia en sus países desde la

base de la cooperación internacional (Ballesteros & Hernández, 2014) especialmente motivado por la indeterminación geográfica que caracteriza a estos delitos.

Según el Consejo de Europa, 68 Estados son parte del Convenio, tanto europeos como no europeos, dos países lo han firmado, pero no lo han ratificado y trece han sido invitados a adherirse. En total, 81 Estados participan como miembros (partes) u observadores (signatarios o invitados) en el Comité del Convenio sobre la Ciberdelincuencia.

El Convenio sobre la Ciberdelincuencia está conformado por un preámbulo y cuarenta y ocho artículos, divididos en cuatro capítulos.

- En el *preámbulo* aparecen los valores que han fundamentado el Convenio, reflejándose los objetivos que persigue; adoptar legislación adecuada para mejorar la cooperación internacional, garantizar una lucha eficaz contra ciberdelincuencia mejorando la investigación y consecuencias penales, aportando mayor calidad a las investigaciones. También pone como objetivo la cooperación entre el Estado y los sectores privados y utilizar medios de investigación adecuados proporcionando mecanismos rápidos y eficaces de cooperación internacional. Todo esto recogido bajo el manto de garantizar los derechos humanos y los intereses de la acción penal, manteniendo un equilibrio entre ambos.

- En el *primer capítulo*, encontramos el título de "Terminología" donde se definen los conceptos de "sistema informático", "datos informáticos", "proveedor de servicios" y "datos relativos al tráfico".

- En el *segundo capítulo*, con el título de "Medidas que deberán adoptarse a nivel nacional", dividido en tres secciones, la Sección 1, sobre Derecho penal sustantivo, donde se establecen los tipos de ciberdelitos:

    A) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
    B) Delitos informáticos.
    C) Delitos relacionados con el contenido.
    D) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

También recoge en esta sección la tentativa, la complicidad, la responsabilidad de las personas jurídicas y las sanciones y medidas relativas a estos delitos.
En la Sección 2, sobre el Derecho procesal, donde se habla del procedimiento, las condiciones y las medidas de protección, es decir la forma de conservación y revelación de los datos, cómo se presentan, cómo se registran, etc.
En la Sección 3, referida a la jurisdicción donde se describen los criterios para aplicarla.

- En el *tercer capítulo*, bajo el título "Cooperación internacional", trata sobre principios generales sobre la cooperación internacional, la extradición, la asistencia mutua o, en su defecto, procedimientos a seguir y acuerdos internacionales aplicables. También se refiere al intercambio de datos y sobre el establecimiento de una red 24/7, es decir, un punto de contacto que sea localizable 24 horas al día los siete días de la semana para garantizar asistencia inmediata para investigaciones sobre delitos informáticos.

- Por último, el *cuarto capítulo*, contiene las disposiciones con las que se determina el acceso de otros países, la firma y entrada en vigor, la adhesión al Convenio, cómo se aplica, los efectos, forma en la que se declara, se denuncia, notificaciones, etc.

Está considerado como una de las normas internacionales más completas hasta la fecha puesto que proporciona un marco legal coherente contra el ciberdelito, siento una guía para todos los países que busquen desarrollar políticas sobre esta tipología delictiva, además de proporcionar un instrumento de cooperación internacional entre los estados parte.
España formó parte del convenio desde que se firmó en 2001 y no sería hasta 2010 cuando se ratificó por el BOE.
Alguno de los beneficios con los que cuentan los países que forman parte del tratado son:

- Proporcionar un marco legal para la cooperación internacional frente a la tipología delictiva de la ciberdelincuencia, estableciendo disposiciones generales y específicas para la cooperación entre las partes.
- Aquellos Estados que forman parte pueden ser miembros del comité, lo que permite compartir información y experiencias, evaluando la implementación del Convenio.

- Pueden negociar nuevos instrumentos para mantener el convenio en continua modificación atendiendo al desarrollo de las TIC.
- Los servicios privados cooperan en mayor medida con los Estados que forman parte del Convenio.

Una de las críticas fundamentales que le realizaban a tal Convenio era que dejaba de lado la problemática del racismo, xenofobia y explotación sexual en menores, actos muy repetidos en las redes, por lo que se elaboraron protocolos adicionales tipificando delitos racistas y xenófobos y otro convenio destinado a la protección del menor en la explotación y abuso sexual.

El Protocolo adicional al Convenio sobre la Ciberdelincuencia, redactado en 2003, proporcionó una penalización de actos relacionados con actos racistas y xenófobos cometidos mediante el uso de las TIC, entró en vigor en 2006.
El Protocolo adicional surge como respuesta a un problema social frecuente especialmente en redes sociales. Aprovecha las herramientas propuestas en el Convenio sobre Ciberdelincuencia acerca de cooperación internacional y tras observar la armonización, surgida mediante el mismo, en materia penal sobre la delincuencia informática.
Por tanto, se desarrolla un protocolo donde se tipifica toda aquella difusión, amenaza o insultos de contenido racista o xenófobo, además de definir aquellos delitos relacionadas con la justificación de genocidios o crímenes contra la humanidad. España lo ratificó en 2014.

A modo de conclusión, el Convenio sobre Ciberseguridad, o Convenio de Budapest, fue fundamental en la tipificación de conductas relativas a la delincuencia mediante medios informáticos. Permitió aunar criterios para la lucha internacional respetando ordenamientos jurídicos propios de cada Estado miembro debido a que el Convenio se ideó como una columna vertebral desde la cual cada país pueda legislar desde una base común, con unos mínimos. La clave de tal convenio fue el aunar y dar herramientas de cooperación internacional frente a la lucha de una tipología delictiva que por sus propias características traspasaba fronteras favoreciendo que el número de víctimas potenciales fuera muy elevado.

b) Regulación jurídica en España

Debemos tener en cuenta que en el Código Penal español no hay mención al concepto de ciberdelito, esto se debe a que tal concepto es utilizado para categorizar un grupo de conductas cuyo punto en común es el uso de las TIC. Por tanto, toda aquella conducta tipificada que utiliza un sistema o dispositivo informático con conexión a Internet será susceptible de ser denominada como ciberdelito pese a no encontrarse tal concepto en la normativa española.

Si atendemos al apartado anterior, al Convenio sobre la Ciberdelincuencia, o de Budapest, España formó parte desde el primer momento, en 2001, pero no fue hasta 2010 cuando entró en vigor tras su ratificación.

Código Penal.

Para comprender cómo es la regulación de estos delitos en España primero tenemos que atender a que el Código Penal vigente fue publicado en 1995. Ya entonces se le dio importancia a la regulación de delitos cometidos mediante medios informáticos, aunque por el contexto temporal no se esperaba la evolución tan rápida de las nuevas tecnologías ni la importancia en la vida cotidiana que tendrían en el corto plazo de 28 años, si nos fijamos en nuestra actualidad. En 2013 se llevó a cabo la Directiva 2013/40/UE, donde se incorporaron delitos contra la intimidad como el *Hacking*, contra el patrimonio (*Cracking*) o la libertad sexual (*Grooming*) Viendo el continuo avance y mejora que se conseguía en la tecnología, en 2015se llevó a cabo una reforma donde se realizaron modificaciones sobre la delincuencia informática.

Dos de estas modificaciones en relación a la ciberdelincuencia fueron la inserción en el mismo Código Penal de dos nuevas tipologías delictivas, el *Sexting* y el *Stalking*. Reguladas en el apartado siete del art. 197.7 y 172 respectivamente.

El Sexting está tipificado en el Código Penal (2015) como aquella conducta que "*sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella 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".* Esta conducta atenta contra el Bien Jurídico de la intimidad de las personas, debemos tener en cuenta que obtener imágenes de una persona con su consentimiento no nos da el derecho de difundirla, especialmente porque una vez publicada perdemos control sobre ella, impidiendo conocer el alcance de su difusión.

El Stalking (Artículo 172.ter Código Penal) hace referencia a la conducta de *"acosar 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:*

1.ª La vigile, la persiga o busque su cercanía física.

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

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.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella."

La importancia de estos dos delitos se basa en que gracias a ello podemos observar una continua evolución, el Código Penal fue capaz de renovarse puesto que hacía 20 años cuando entró en vigor el actual Código no existían tantos medios para la comisión de este delito. El avance de las redes sociales como puede ser Whatsapp o Instagram que en aquél entonces no existían unido al avance tecnológico como relojes inteligentes o los propios dispositivos móviles que son una parte fundamental de nuestra vida exponen constantemente a los ciudadanos a ser víctimas de estos delitos.

Igualmente, con la reforma del 2015 se permitió prestar la debida atención a delitos de índole sexual relacionados con menores, igual que el Convenio de Budapest necesitó dar respuesta a la explotación sexual de la infancia, el Código Penal respondió a delitos relacionados con la pornografía infantil, castigando la mera adquisición de tales contenidos. También se tipificó el delito conocido como *Grooming,* contactar con un menor de edad con el fin de obtener material pornográfico.

Legislación vigente:

I) Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

Con respecto a la Legislación acerca de ciberseguridad, una de las principales leyes es la Ley Orgánica 3/2018 de Protección de Datos y de Garantía de Derechos Digitales

(LOPDGDD), que establece las normas para la protección de datos personales y regula el uso de las tecnologías de la información. La LOPDGDD establece sanciones para aquellos que cometen infracciones en materia de protección de datos, como el robo de información personal o el espionaje informático. Buscaba proporcionar unas claves para el uso de empresas de las nuevas tecnologías, con el fin de que no se vulneraran los derechos fundamentales de los ciudadanos. Esta ley también buscaba dotar de protección a los propios ciudadanos dándoles un mayor control sobre sus propios datos personales.

II) Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico

Otra ley importante es la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), que regula el comercio electrónico y establece sanciones para aquellos que cometan delitos como el fraude en línea o la estafa en internet. La LSSICE también establece medidas para combatir la piratería y la infracción de derechos de autor en internet.

III) Ley de Ordenación de las Telecomunicaciones

La Ley de Ordenación de las Telecomunicaciones (LOT) también tiene disposiciones relacionadas con los delitos informáticos, como la regulación de la interceptación de comunicaciones y la protección de la privacidad en las redes.

En resumen, en España existen varias leyes que regulan los delitos informáticos y establecen sanciones para aquellos que cometan estos delitos. Estas leyes incluyen la LOPDGDD, la LSSICE, la LOT, y el Código Penal español. Estas leyes regulan una amplia gama de delitos informáticos, desde el robo de información personal hasta la infracción de derechos de autor en internet, y buscan proteger a las personas y sus datos personales de los peligros de la tecnología de la información.

Por otra parte, nos encontramos con la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores, que busca dotar de responsabilidad penal a menores mayores de catorce años.

c) Estrategia de Seguridad Nacional.

Por último, la Estrategia de Seguridad Nacional, de 2013, fue un documento que realizó el Gobierno de España para analizar cómo era la seguridad española, observando las mayores debilidades, riesgos y amenazas.

Esto mostró que las ciberamenazas eran uno de los peligros más destacados de España, basándose en que la comisión de estos delitos era muy fácil, no se podía localizar el lugar desde el cual surgía la amenaza, eran anónimos y tenía una ratio muy favorecedor riesgo-beneficio, podían beneficiarse mucho a un coste muy bajo.

Tras detectar estas amenazas se establecieron los campos de actuación para tratar de minimizar el riesgo.

Se propuso neutralizar la amenaza del terrorismo y la vulnerabilidad de la sociedad frente a ataques terroristas atendiendo a los procesos de radicalización. Garantizar un Internet seguro fortaleciendo la capacidad de prevención, detección y respuesta a ataques cibernéticos y, por último, impedir que se establecieran grupos criminales organizados en el territorio español.

Para alcanzar el objetivo de un Internet seguro se promovió desde la Estrategia que se desarrollara una normativa adecuada y que todas las instituciones actuasen de forma coordinada para mejorar sus capacidades.

Las líneas de actuación que pretende seguir la Estrategia de Ciberseguridad Nacional fueron aumentar la capacidad de prevenir, detectar, responder y recuperarse frente a ciberamenazas, mejorar la seguridad de los sistemas de información y Telecomunicaciones de la Administración Pública y de las Infraestructuras Críticas, mejorar la capacidad de investigación y persecución del ciberterrorismo y ciberdelincuencia, impulsar la resiliencia y la seguridad de las TIC en el sector privado, aumentar una cultura de ciberseguridad, el compromiso de cooperación internacional y aumentar el conocimiento y desarrollo en materia de Ciberseguridad.

d) Estrategia de Ciberseguridad Europea.

A nivel europeo, en 2013 se elaboró por parte de la Comisión Europea una estrategia de ciberseguridad, en la cual se buscaba que los países amparados bajo el Convenio de Ciberdelincuencia colaborasen con los sectores privados para llevar a cabo una

cooperación efectiva. Para ello se propuso que los gobiernos necesitaban establecer una normativa eficaz cumpliendo normas comunes, en la Estrategia de Ciberseguridad de la Unión Europea de 2013 se insta a que todos los países ratifiquen el Convenio.
El segundo punto que tratan es que todos los estados miembros del Convenio cuenten con unidades especializadas en la lucha contra la ciberdelincuencia y, por último, señala la importancia de trabajar coordinadamente, trabajando de manera coordinada todos los países, las autoridades policiales y judiciales, así como los sectores públicos y privados.
En la Directiva 2013/40/EU relativa a los ataques contra los sistemas de información se buscó establecer normas mínimas relativas a infracciones penales en ataques a sistemas de información, de tal forma que se llegue a una armonización en la tipificación de conductas delictivas; entre los artículos 3 y 8 de la directiva encontramos:

I) Acceso ilegal a los sistemas de información, acceder de manera intencionada violando medidas de seguridad.
II) Interferencia ilegal en los sistemas de información, tomarán medidas ante la obstaculización o interrupción del funcionamiento de un sistema informático, haciendo inaccesibles datos informáticos.
III) Interferencia ilegal de datos, castiga borrar, alterar, suprimir o hacer inaccesibles contenidos de un sistema de información.
IV) Interceptación ilegal, castiga quien por medios técnicos captase información interceptando transmisiones no públicas de datos informáticos.
V) Instrumentos utilizados para cometer infracciones, los estados miembros deberán castigar la producción, venta, adquisición, importación, etc., de instrumentos como programas informáticos para cometer infracciones o contraseñas, códigos de acceso o datos que permitan acceder a sistemas de información privados.
VI) Inducción, complicidad y tentativa, la Directiva menciona que la inducción, complicidad o tentativa de violación de las anteriores infracciones sean sancionadas como infracciones penales.

Por último, a nivel de la Unión Europea, se estableció la Directiva 2016/1148 del Parlamento Europeo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. Donde se

establecieron los requisitos comunes en seguridad y notificación que deben cumplir operadores de servicios y proveedores de servicios digitales; la Directiva obliga a los países miembros a identificar a los operadores de servicios digitales, a quienes pone unos requisitos mínimos de seguridad informática. Fija la obligación de recibir notificaciones de incidentes significativos por parte de los operadores de servicios. Obliga también a designar autoridades competentes y puntos de contacto en temas de redes y sistemas de información. Concluye estableciendo medidas para garantizar la cooperación en el ámbito nacional e internacional estableciendo el Grupo de Cooperación, donde se asumirán las funciones de cooperación estratégica, intercambiando información entre los diferentes estaos miembros.

4. ORGANISMOS Y UNIDADES IMPLICADAS

Tras realizar un análisis bibliográfico acerca de cómo se encuentra la regulación en materia de ciberdelincuencia en España y Europa se observar cómo uno de los objetivos que marcan las diferentes normativas es la necesidad de designar autoridades que sean competentes y que puedan intercambiar sus informaciones para coordinarse a nivel internacional. Las Fuerzas y Cuerpos de Seguridad del Estado son muy importantes para la lucha contra la ciberdelincuencia a nivel español. En este aspecto, el Cuerpo Nacional de Policía y la Guardia Civil tienen la labor de perseguir a aquellos delincuentes que mediante las TIC cometen alguno de los delitos mencionados en las anteriores páginas.

A) Cuerpo Nacional de Policía.

Podemos encontrar la Unidad de Investigación Tecnológica, según la web de *Oposiciones nacionales y Formación Profesional,* la unidad que investiga y persigue las actividades delictivas que se lleven a cabo mediante las TIC y los ciberdelitos relacionados con el patrimonio, los menores, los delitos sexuales, delitos contra el honor y la intimidad, la propiedad intelectual e industrial y la seguridad lógica. También actúa como Centro de Prevención y Respuesta de E-Crime, dentro de ella se encuentran dos diferentes unidades como:

I) La Brigada Central de Investigación Tecnológica; investiga actividades que se cometen a través de las TIC como la protección de los menores, delitos contra propiedad intelectual o los fraudes, obteniendo pruebas y persiguiendo a sus autores.

II) Brigada Central de Seguridad Informática; su trabajo es la investigación de actividades que afecten a la seguridad lógica.

Estas brigadas de la Policía Nacional buscan la colaboración ciudadana especialmente en la denuncia de todas las actividades delictivas que son sufridas a través de la Red, al igual que todas aquellas páginas, webs o perfiles de redes sociales que puedan ser peligrosas.

B) Guardia Civil

Dentro de este cuerpo nos encontramos el Grupo de Delitos Telemáticos, atendiendo a su propia web, la unidad fue creada para investigar aquellos delitos realizados a través de Internet. Su origen data de 1996 bajo el nombre de Grupo de Delitos Informáticos. A través del crecimiento exponencial de las TIC el grupo cambia de nombre al que tenemos hoy en día, creándose también los Equipos de Investigación Tecnológica (EDITEs) en cada provincia del territorio español.

El objetivo de ambas secciones es la investigación de la delincuencia en la Red y los sistemas de información, además de la prevención dotando a la población de información para fomentar un uso adecuado de las tecnologías. La unidad tiene un papel fundamental en la cooperación internacional trabajando con Interpol o Europol, participando en foros internacionales sobre el cibercrimen. Es el encargado de ser el punto de contacto en la cooperación internacional requerido desde el Convenio de Ciberdelincuencia.

Dentro de sus competencias podemos encontrar, además de la persecución de delitos realizados en la red, dar apoyo a investigaciones de la Unidad Central Operativa, quien es el encargado de la investigación de los delitos más graves a nivel territorial y también en ámbitos internacionales siempre que se vean afectados los intereses de España.

La unidad también está encargada de realizar patrullaje en la red pública observando todas aquellas webs que puedan estar cometiendo ilicitudes o atenten contra la seguridad de los usuarios en la Red.

C) Instituciones fuera de las Fuerzas y Cuerpos de Seguridad del Estado.

Fuera de las Fuerzas y Cuerpos de Seguridad del Estado nos encontramos con diferentes instituciones dentro del ámbito nacional que trabajan en la lucha contra la ciberdelincuencia, el correcto uso de la Red y la seguridad de los usuarios que navegan en ella. Entre estas instituciones podemos destacar:

I) Instituto Nacional de Ciberseguridad (INCIBE);

Este es el centro nacional que actúa como referencia en materia de ciberseguridad. Es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital. Trabaja en la investigación y prestación de servicios en materia de ciberseguridad a nivel nacional e internacional. Es el centro que dará respuesta a diferentes incidentes que el usuario de la Red pueda tener, mejorando la ciberseguridad y la confianza de los usuarios en la navegación, protegiendo y defendiendo a los ciudadanos, favorecer el desarrollo de profesionales en materia, potenciando la industria española en ciberseguridad, siendo un motor para la transformación digital de la sociedad española.

II) Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC).

Creado en 2007 para impulsar, coordinar y supervisar aquellas actividades del Ministerio del Interior que dependan de la Secretaría del Estado de Seguridad. Se encarga de proporcionar una red de seguridad en todas aquellas infraestructuras telemáticas. Es de vital importancia para proporcionar los servicios esenciales a los ciudadanos, como la red de salud, seguridad, economía, etc. El funcionamiento de estas redes es importante para que el servicio prestado a los ciudadanos no se vea interrumpido o corrompido. Puesto que son servicios esenciales son blancos principales para actos delictivos por lo que la protección contra todo tipo de agresiones es necesario para seguir disponiendo de todos los recursos que el Estado de Bienestar nos brinda.

III) El equipo de Respuestas ante Emergencias Informáticas.

Está formado por un grupo de expertos en ciberseguridad que se encargan de resolver incidencias relacionadas con las TIC que afecten a organismos públicos, empresas privadas que puedan tener interés estratégico para la nación y a los ciudadanos. El equipo está coordinado por el CNPIC y el INCIBE, y proporciona la resolución técnica de incidentes de ciberseguridad.

IV) Centro Criptológico Nacional (CCN-CERT);

Encargado de coordinar la acción de los organismos de la Administración que utilicen medios cifrados, garantiza la seguridad de las TIC, está adscrito al Centro Nacional de Inteligencia y está encargado del ejercicio de funciones relativas a la seguridad en la Red y la protección de la información clasificada. Es el encargado de mejorar la

ciberseguridad informática, funcionando como centro de alerta y respuesta nacional que responda de forma rápida y eficiente a los ataques realizados mediante las TIC. Su objetivo es conseguir un ciberespacio seguro y confiable, protegiendo la información confidencial y sensible a prueba de posibles ataques, "*defendiendo el Patrimonio Tecnológico español"* (Misión y Objetivos)

España, como hemos recogido en los diferentes apartados del trabajo, ha trabajado junto con otros países por conseguir el trabajo coordinado en materia de ciberseguridad. Por tanto, será necesario recoger qué entidades son las más importantes a destacar en cuanto a trabajo internacional para perseguir y protegerse de los ataques a través de la Red. Hemos visto que una de las características de los ciberdelitos es que son transfronterizos, un claro ejemplo de esto podemos verlo recientemente desde el comienzo de la invasión de Rusia a Ucrania. Aquellos países que han mostrado su apoyo y han dotado de material a Ucrania han visto multiplicados los ataques recibidos con origen ruso (Holgado, revista 20minutos, 2022).

D) Organismos internacionales

Entre las entidades encargadas de proteger a los usuarios y perseguir los ciberataques destaca:

I) Interpol,

La Organización Internacional de Policía Criminal, se trata de la organización policial más importante a nivel internacional que existe, la forman 190 países para hacer frente a la delincuencia internacional. Dentro de la Interpol encontramos el Complejo Mundial de Interpol para la Innovación que permite dotar a la policía de todo el mundo de herramientas necesarias para enfrentarse a la delincuencia a través de las TIC, dando apoyo operativo y formación.

Reúnen especialistas en ciberdelincuencia que permitirá el intercambio de datos y la difusión de información útil sobre peligros detectados en el ciberespacio.

II) El centro Europeo de Ciberdelincuencia (EC3).

Nace en enero de 2013 con el objetivo de proteger empresas y ciudadanos europeos frente a la ciberdelincuencia, centrándose en actividades ilegales del crimen organizado, estafas, actividades financieras, explotación sexual de menores y los delitos que ataquen a infraestructuras críticas de la Unión Europea

III) Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

Fue creada en 2004 para contribuir con la política de seguridad cibernética de la Unión Europea. Su objetivo es mejorar la fiabilidad de los productos y servicios, así como los procesos de las TIC. Siendo conscientes de que la ciberseguridad fomentará la transformación digital de la sociedad europea en todos los sectores es necesario tener una política e iniciativas comunes, creando políticas integradoras, evitando que existan diferentes regulaciones entre los diferentes países de la UE y dando un enfoque común dotando de sus características específicas a cada sector.

5. CONCLUSIONES

A modo de conclusiones, se expondrán una serie de reflexiones sobre cada uno de los puntos tratados con el fin de responder a los objetivos que se planteaban en la introducción;

1º. Realizar una descripción de la evolución de la ciberdelincuencia

2º. Recoger la normativa europea y nacional.

3º. Definir los organismos e instituciones que trabajan contra la ciberdelincuencia en España y a nivel internacional.

El último objetivo, como se mencionaba en la introducción del presente trabajo, era dotar de una forma de actuar para evitar ser víctimas de este tipo de delitos. En este apartado se incluirán unas bases en las que podemos trabajar todos como sociedad para evitar que este tipo de delitos sigan en crecimiento.

Lo primero que queda claro y como forma de empezar este epígrafe, el uso de Internet y las TIC es una realidad de nuestro día a día en la mayoría de personas, concretamente en

España veíamos como un 99’7% de la población joven usaba la Red cada día, por tanto, es necesario saber que igual que proporciona una gran cantidad de beneficios como la eliminación de los límites fronterizos que proporciona una conexión instantánea con cualquier parte del mundo. Pero este mismo beneficio puede utilizarse para la comisión de delitos, por lo que debemos saber que existen ciertos riesgos a los que nos exponemos, en muchas ocasiones, no siendo conscientes.

La ciberdelincuencia se aprovecha del nicho que generan las TIC para la comisión de delitos vulnerando diferentes bienes jurídicos protegidos de diferentes formas, actualizándose continuamente sus conductas para conseguir saltarse las barreras que protegen a los usuarios de la Red. La ciberdelincuencia cuenta con unas características principales, el uso de las TIC para realizar conductas ilícitas permite a los delincuentes el ser anónimos, tener un elevadísimo número de víctimas potenciales, eliminar las fronteras físicas para actuar o la facilidad de comisión, por otro lado, cuentan con una ventaja, que en la gran mayoría de usuarios el conocimiento que poseen de informática es muy limitado de tal manera que aumenta la probabilidad de ser posibles víctimas de delitos informáticos.

Observábamos cómo existían diferentes tipos de delincuentes informáticos conocidos como “Hackers”, dando lugar a diferentes tipologías dependiendo de su conducta. Los Black Hat Hackers, aquellos que buscan su propio beneficio. Por lo contrario, los White Hat Hackers son aquellos que encuentran los fallos de los sistemas informáticos e informan de ellos a las autoridades para solucionarlos y los Grey Hat, que informan a las autoridades para conseguir beneficio económico solucionándolos.

La ciberdelincuencia se encuentra en constante aumento pese a que llevan años siendo conscientes de este peligro y que la regulación al respecto ha evolucionado. Las leyes se vuelven cada vez más represivas para estos comportamientos, pero es necesario la concienciación de la población sobre la necesidad de mantener los terminales protegidos frente a posibles ataques, conocer el alcance que pueden tener las publicaciones, la importancia de las medidas de seguridad de las redes sociales, etc. Estas dos últimas cosas cobran un valor aún mayor cuando los usuarios son menores de edad, la educación en el uso correcto de las TIC es un punto a incidir desde jóvenes que debería regularse mediante políticas puesto que favorecería la prevención de la tipología delictiva asociada a las TIC.

Los organismos internacionales atendieron a cómo la ciberdelincuencia actuaba de manera global y decidieron establecer un marco jurídico común a todos los países favoreciendo una regulación clara y una cooperación internacional que no estaba presente previamente, pero era necesaria para realizar una persecución efectiva a los delincuentes. Este marco jurídico y regulación de la cooperación internacional ser recoge en el Convenio sobre la Ciberdelincuencia de 2003, cuyo objetivo claro era que los países miembros colaborasen mediante la armonización de sus legislaciones y la cooperación internacional estableciendo términos, delitos y formas de investigación homogéneas.

La importancia de este Convenio es por ser la base de nuestra legislación en materia de delitos informáticos, pero todos somos conscientes que desde el 2003 que se realizó la informática ha avanzado mucho lo que ha provocado que el convenio haya sido revisado para incluir nuevas tipologías.

No fue hasta 2013 cuando, bajo las premisas del Convenio, España elaboró su Estrategia de Seguridad Nacional y la Estrategia de Ciberseguridad, donde se establecieron objetivos y líneas de actuación que fueran acordes con el Convenio, para fomentar las capacidades de investigación y detección de actividades delictivas en el ciberespacio con un marco normativo eficaz.

Atendiendo al marco normativo nacional en materia de ciberdelincuencia se aprecia que está en continua evolución, introduciéndose nuevos tipos penales mediante reformas como la de 2010 o 2015, con las que se han ido introduciendo Directivas para tipificar conductas como el *Stalking,* el *Sexting*, el *Grooming*, etc. En materia penal la legislación española es bastante completa teniendo en cuenta que se trata de un ámbito en pleno desarrollo por lo que lo que hoy es una legislación completa y acorde con la realidad delictiva que vivimos mañana puede dejar un vacío para una tipología que se desarrolle mediante un nuevo avance de las TIC.

Una de las líneas comunes del Convenio y la Estrategia de Ciberseguridad Nacional es mejorar la capacidad de prevención, detección y persecución a delitos informáticos, por este motivo es que se hacía muy importante el mostrar un esquema de aquellas instituciones unidades de las Fuerzas y Cuerpos de Seguridad del Estado que estaban encargadas de actuar como primera línea de defensa frente a la ciberdelincuencia.

Destacando en este apartado a nivel internacional la Interpol, a nivel europeo el EC3 o el ENISA y a nivel nacional la Brigada Central de Investigación Tecnológica de la Policía Nacional o el Grupo de Delitos Telemáticos de la Guardia Civil.

Además de instituciones nacionales como el Centro Criptológico Nacional, el Instituto de Ciberseguridad Nacional o el Centro Nacional de Protección de Infraestructuras Criticas entre otras.
Gracias a la labor de estas instituciones públicas y a la colaboración de los sectores privados en materia de ciberseguridad se logra uno de los objetivos que marcó el Convenio de Ciberdelincuencia, el objetivo de cooperación.

En definitiva, con la exposición de toda la información previa podemos observar cómo, pese a que podemos pensar lo contrario, a nivel nacional e internacional, la regulación de esta materia delictiva es un tema que está muy presente y que se busca la renovación constante para responder de manera más eficaz a todas las demandas que los usuarios de la red piden para poder tener una navegación en la Red segura. No obstante, uno de los puntos que se repiten, a modo de crítica, es que la evolución de las TIC es constante y muy acelerado por lo que la regulación en materia penal deja en ocasiones tipologías delictivas muy abiertas para que entren dentro de esa norma un grupo amplio de comportamiento mediante los cuales el bien jurídico sea vulnerado. Es por ello que considero como fundamental el objetivo de cooperación nacional e internacional en todas las instituciones de tal forma que se aúnen todos los recursos disponibles para mejorar la experiencia en Internet.

Por último, como se mencionaba previamente, vamos a tratar de encontrar una solución a la problemática de la ciberdelincuencia. Esto provoca que surjan tanto ideas utópicas, de forma que puedan acabarse radicalmente con estos delitos, e ideas más realistas donde un trabajo coordinado y a largo plazo entre todas las instituciones de cada país para reducir todo lo posible estos delitos hasta que llegue un punto donde se consigan erradicar. Empezando por las ideas “utópicas”, podemos pensar que la creación de sistemas de seguridad informática a modo de antivirus o programas de identificación de usuarios muy avanzados que provoquen que nadie que no sea nosotros mismos bajo identificación, incluso biométrica, puedan acceder a nuestros terminales y datos privados que navegan en la red. Esto se conseguiría con un avance muy grande de las nuevas tecnologías desarrolladas por personas cuya ética sea irreprochable de tal forma que no permitan ningún tipo de acceso, conocido en lenguaje de las TIC como “Backdoors”. Actualmente los programadores y desarrolladores de dispositivos, como Smartphone y ordenadores, buscan dejar estas backdoors con el objetivo de poder recabar datos de los usuarios a fin

de poder otorgarles las necesidades que tengan. Esto lo consiguen, por ejemplo, cuando aceptamos las "cookies" de las diferentes webs o aplicaciones, de tal forma que son capaces de invadir nuestra privacidad obteniendo datos de nuestras búsquedas más frecuentes, nuestros gustos, etc. Por tanto, si los desarrolladores fueran éticos y respetasen la privacidad se conseguiría un gran avance frente al problema de no respetar la privacidad en internet. Si todos los encargados de dotar a la población de los dispositivos y diferentes contenidos que se pueden encontrar en la Red fueran éticamente correctos y trabajasen en beneficio de la sociedad la ciberdelincuencia se vería mucho más reducida puesto que habría muchas más dificultades.

Por otro lado, si atendemos a respuestas mucho más realistas y a largo plazo, las formas de reducir estos delitos se deberían trabajar atendiendo a diferentes factores, como, por ejemplo:

- Fortalecimiento de las leyes y regulaciones: afortunadamente, en España, en materia de ciberseguridad, las instituciones están concienciadas con la lucha frente a delito informáticos y trabajan junto con el resto de países europeos en el fortalecimiento de los sistemas de seguridad y las respuestas que pueden ofrecer si se llegan a cometer. Sin embargo, en otros muchos países, las leyes y regulaciones relacionadas con la delincuencia informática aún están en proceso de desarrollo o no son lo suficientemente estrictas, dejando muchos vacíos en las leyes que los usuarios pueden utilizar para robar información o entrar en dispositivos de personas que se encuentran a kilómetros de distancia. El fortalecimiento de estas leyes y regulaciones puede incluir la implementación de medidas más severas de castigo y la definición más clara de los delitos informáticos. También es importante establecer normas internacionales para la cooperación y el intercambio de información entre países, esto es lo que buscaba el Convenio de Budapest, sin embargo, al no ser un tratado global los países fuera de este Convenio quedan fuera de la cooperación que propone.

- Fortalecimiento de la seguridad informática: La seguridad informática es crucial para prevenir la delincuencia informática. Las empresas y los individuos deben tomar medidas para proteger sus datos personales y confidenciales, así como para evitar la intrusión y el robo de información. Esto incluye la implementación de medidas como la autenticación de dos factores, medida que ya se está empezando a implementar en muchas de las aplicaciones más habituales como "Gmail", la encriptación de datos y

la actualización regular del software de seguridad. Para este apartado, a nivel usuario, es importante el siguiente apartado, puesto que en muchas ocasiones los factores de riesgo que se asocian a este tipo de delitos es la desinformación y desconocimiento de los peligros de internet.

- Educación y concientización: Las personas deben ser informadas sobre los riesgos de la delincuencia informática y cómo protegerse. Las campañas educativas pueden incluir información sobre cómo detectar y evitar correos electrónicos fraudulentos, cómo proteger las contraseñas, cómo identificar sitios web inseguros y cómo utilizar herramientas de seguridad informática. Este aspecto se debe tratar desde las edades más tempranas puesto que son los que más riesgo pueden tener de ser futuras víctimas. Desde mi práctica profesional, la policía local trata mucho este aspecto dando charlas sobre los peligros de la red desde el papel del Agente Tutor, el agente encargado de la prevención de los delitos en menores.

- Cooperación internacional: La cooperación internacional es fundamental para abordar la delincuencia informática, ya que no tiene fronteras. Los países deben trabajar juntos para compartir información sobre los delitos informáticos y las mejores prácticas para prevenirlos. También es importante establecer acuerdos internacionales para la extradición de delincuentes informáticos y para la creación de equipos de investigación conjuntos.

- Desarrollo de nuevas tecnologías: por ejemplo, la tecnología blockchain puede garantizar la seguridad y la privacidad de la información en línea. Las empresas pueden utilizar herramientas de análisis de datos para detectar patrones de comportamiento sospechosos y así prevenir delitos informáticos. Además, la inteligencia artificial y el aprendizaje automático pueden ser utilizados para detectar y prevenir la delincuencia informática. De igual manera, el papel de criminólogos capaces de desarrollar perfiles delictivos puede favorecer una visión más centrada en la prevención de los delitos informáticos.

En resumen, la prevención y la lucha contra la delincuencia informática requieren un enfoque integral que incluya medidas legales, tecnológicas, educativas y de cooperación

internacional. Es importante trabajar juntos para abordar este problema global y proteger nuestra información personal y confidencial en línea.

6. BIBLIOGRAFIA

- 7 tipos de hackers. (2022, 26 Agosto). KeepCoding Tech School. https://keepcoding.io/blog/7-tipos-de-hackers-2/

- Acurio Del Pino, S. (s.f.). Delitos informáticos: generalidades. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

- Ballesteros, M. C. R., & Hernández, J. A. G. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, *47*, 209-234.

- CONSEJO DE EUROPA. Convenio sobre la Ciberdelincuencia. Serie de Tratados Europeos nº 185. Budapest, 2001 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

- Informe sobre la Cibercriminalidad en España. (2021), pg. 19. En Ministerio del Interior Recuperado 2 de diciembre de 2022, de https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout

- Llinares, F. (2012). El Cibercrimen. Fenomenología Y Criminología De La Delincuencia En El Ciberespacio. Marcial Pons Ediciones Jurídicas y Sociales, S.A.

- *Digital Report 2022: El informe sobre las tendencias digitales, redes sociales y mobile.* (2022, 14 febrero). We Are Social Spain. Recuperado 2 de diciembre de 2022,

de https://wearesocial.com/es/blog/2022/01/digital-report-2022-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/

- *Firmas y ratificaciones del tratado nº 185. Convenio sobre Ciberdelincuencia*. Recuperado el 23 de enero de 2023 en http://www.coe.int/en/web/conventions/full-list//conventions/treaty/185/signatures.

- España (2015). Código penal. Artículo 197.7. Recuperado de https://www.boe.es/eli/es/lo/1995/11/23/10/con

- España (2015). Código penal. Artículo 172. Recuperado de https://www.boe.es/eli/es/lo/1995/11/23/10/con

- España (2000). Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.https://www.boe.es/eli/es/lo/2000/01/12/5/con

- España (2018) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/eli/es/lo/2018/12/05/3/con

- España (2002) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. https://www.boe.es/eli/es/l/2002/07/11/34/com

- DIRECTIVA 2013/40/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información. Recuperado el 30/1/2023 http://www.boe.es/doue/2013/218/L00008-00014.pdf

- DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel

común de seguridad de las redes y sistemas de información en la Unión. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

-*Brigada Central de Investigación Tecnológica (B.C.I.T); Policía Nacional*. (s. f.). Recuperado el 30 de enero de 2023 https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php

- *Oposiciones nacionales y Formación Profesional. La Unidad de Investigación Tecnológica*. Recuperado el 30 de enero de 2023 https://www.oposicionesnacionales.com/la-unidad-de-investigacion-tecnologica/

- *GDT - Grupo de Delitos Telemáticos*. Recuperado el 30 de enero de 2023 https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

- INCIBE. Recuperado el 30 de enero de 2023 https://www.incibe.es/

- *CNPIC | Inicio*. https://cnpic.interior.gob.es/opencms/es/inicio/ Recuperado el 28 de enero de 2023

- *Misión y Objetivos*. https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html

- Holgado, R. (2022, 31 marzo). El CNI alerta de posibles ciberataques a España por parte de hackers rusos. *20bits* https://www.20minutos.es/tecnologia/ciberseguridad/el-cni-alerta-de-posibles-ciberataques-a-espana-por-parte-de-hackers-rusos-4979062/

- *El Complejo Mundial de INTERPOL para la Innovación abre sus puertas*. (s. f.). Recuperado el 31 de enero de 2023 https://www.interpol.int/es/Noticias-y-

acontecimientos/Noticias/2014/El-Complejo-Mundial-de-INTERPOL-para-la-Innovacion-abre-sus-puertas

- *European Cybercrime Centre - EC3*. (s. f.). Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

- *Press corner*. (s. f.). European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/es/IP_13_13

- *Acerca de la ENISA - Agencia de la Unión Europea para la Ciberseguridad*. (s. f.). ENISA. https://www.enisa.europa.eu/about-enisa/about/es

- GOBIERNO DE ESPAÑA. Estrategia de Seguridad Nacional. Madrid, 2013. https://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf Recuperado el 30 de enero de 2023
- DIRECTIVA 2013/40/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. https://www.boe.es/doue/2013/218/L00008-00014.pdf recuperado el 28 de enero de 2023