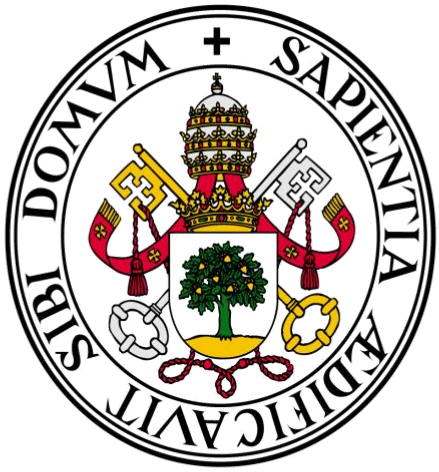

Universidad de Valladolid

Facultad de **Derecho**

Grado en **DERECHO.**

ASPECTOS PROCESALES DE LOS CIBERDELITOS.

Presentado por:

Ángela López Muriel

Tutelado por:

M.ª Ángeles Gallego Mañueco

Valladolid, 1 de julio de 2024

A mis padres, hermana y pareja,

por celebrar mis pequeños logros como si fueran triunfos.

RESUMEN

En la era digital, las tecnologías de la información y las comunicaciones han dado lugar a una nueva forma de delincuencia: los ciberdelitos. Estos abarcan desde ataques informáticos hasta el acoso a través de internet.

Para abordar esta problemática, se han establecido marcos normativos tanto a nivel nacional como europeo que regulan aspectos como la interceptación de comunicaciones, la identificación de equipos y usuarios mediante direcciones IP, y la cooperación judicial en casos de ciberdelincuencia internacional.

En el ámbito procesal, la investigación de los ciberdelitos presenta desafíos tecnológicos constantes. Las fuerzas de seguridad, como la Guardia Civil y el Cuerpo Nacional de Policía, desempeñan un papel crucial en la prevención y persecución de estos delitos. Además, el trabajo explora los órganos encargados de la investigación de ciberdelitos a nivel europeo.

La lucha contra los ciberdelitos requiere una adaptación constante debido a la evolución tecnológica. Las fuerzas de seguridad deben mantenerse actualizadas en las últimas tendencias y técnicas utilizadas por los delincuentes cibernéticos. La colaboración entre agencias nacionales e internacionales es fundamental para abordar la naturaleza transfronteriza de estos delitos.

En resumen, la ciberseguridad ha transformado la forma en que se cometen y se investigan los delitos en la era digital.

PALABRAS CLAVE

Tecnologías informáticas (TIC), delito informático, ciberdelito, internet, ciberseguridad, Eurojust, Europol y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), Instituto Nacional de Ciberseguridad (INCIBE), Ley de Enjuiciamiento Criminal (LECrim), *notitia criminis,* GDT (Grupo de Delitos Telemáticos), IOCTA (Internet Organised Crime Threat Assessment), Centro Europeo de Delitos Financieros y Económicos (EFECC), Artículo (Art.), Ley de Seguridad Nacional (LSO), Unión Europea (UE).

ABSTRACT

In the digital era, information and communication technologies have given rise to a new form of crime: cybercrimes. These range from computer attacks to online harassment. To address this issue, regulatory frameworks have been established at both national and European levels, covering aspects such as communication interception, identification of devices and users through IP addresses, and judicial cooperation in cases of international cybercrime.

In the procedural context, investigating cybercrimes presents constant technological challenges. Law enforcement agencies, such as the Guardia Civil and the National Police Corps, play a crucial role in preventing and prosecuting these offenses. Additionally, European-level bodies involved in cybercrime investigation are explored.

The fight against cybercrimes requires constant adaptation due to technological evolution. Security forces must stay updated on the latest trends and techniques used by cybercriminals. Collaboration between national and international agencies is essential to address the cross-border nature of these crimes.

In summary, cybersecurity has transformed how crimes are committed and investigated in the digital age.

KEY WORDS

Phishing, spyware, malware, ransomware, bullying, cyberbulling, software, rootkits, cracking, Internet Organised Crime Threat Assessment, hacking, child grooming, sexting, Cross Site Scripting.

ABREVIATURAS

Ley de Enjuiciamiento Criminal (LECrim),

GDT (Grupo de Delitos Telemáticos),

IOCTA (Internet Organised Crime Threat Assessment),

Centro Europeo de Delitos Financieros y Económicos (EFECC),

Artículo (Art.),

Ley de Seguridad Nacional (LSO),

Unión Europea (UE),

Tecnologías informáticas (TIC),

capítulo (Cap.)

INDICE

1 INTRODUCCIÓN

En las últimas décadas, hemos sido testigos del avance tecnológico y su impacto en la sociedad desde una perspectiva social y jurídica. La informática ha experimentado innovaciones significativas y, hoy en día, estas herramientas son fundamentales para la comunicación tanto social como comercial.

El crecimiento vertiginoso de Internet ha convertido la red en un gran globalizador, conectándonos con personas de todo el mundo sin importar su ubicación geográfica. Actualmente, existen más de 1. 964. 814. 295 sitios web en la red y aproximadamente 4.660.000.000 de personas tienen acceso a internet, lo que representa el 59,5% de la población (Digital 2022 Global Overview Report, enero 2022).[1]

Aunque el ciberespacio ofrece oportunidades, también presenta amenazas como la ciberdelincuencia. [2]

En este contexto, es crucial analizar los aspectos procesales relacionados con la investigación, persecución y sanción de los delitos informáticos. Los procedimientos legales desempeñan un papel fundamental en la protección de la sociedad digital, abordando desafíos específicos que surgen en el ciberespacio.

Por este motivo los aspectos procesales en la lucha contra los ciberdelitos no solo son esenciales para la justicia, sino también para garantizar la confianza en la sociedad digital. La adaptación constante de las leyes y los procedimientos a la evolución tecnológica es un desafío continuo para proteger nuestros espacios virtuales.

En resumen, el avance tecnológico ha transformado nuestra sociedad y la forma en que nos comunicamos. Internet, con su crecimiento exponencial, ha conectado a personas de todo el mundo, pero también ha dado lugar a amenazas como la ciberdelincuencia. Para proteger nuestra sociedad digital, es crucial analizar y adaptar constantemente los aspectos procesales

[1] VERA, M. D. B. “El Ciberdelito, desafíos para la ley penal y civil. Marco jurídico nacional y comparado”. *Revista Jurídica*, *7*(1). 2023.

[2] SANTOS, C. P., GUISADO, Á. C., & MORÁN, J. J. D. “El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito”. *Revista policía y seguridad pública*. 2017.. Pp: 239-240.

relacionados con la investigación y sanción de delitos informáticos. La confianza en el ciberespacio depende de una justicia eficiente y leyes actualizadas que aborden los desafíos específicos que surgen en este entorno virtual.

2 EVOLUCIÓN DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, SU IMPACTO EN LA CRIMINALIDAD Y LA CREACIÓN DE NUEVAS FIGURAS DELICTIVAS

En las últimas décadas el avance de las tecnologías informáticas (en adelante TIC) ha sido notable. Aunque su desarrollo comenzó en los años sesenta y setenta, con la creación de internet fue cuando realmente experimentaron un gran impulso y se volvieron imprescindibles para el día a día de muchas personas. Es impactante la velocidad a la que emergen nuevas tecnologías en la actualidad y, además, todo sugiere que esta tendencia persistirá en el futuro.

Al igual que estos cambios y evolución tecnología tienen un impacto en nuestra sociedad, también lo tienen en la criminalidad. La evolución de estos delitos ha seguido un curso paralelo a los cambios sociales y tecnológicos[3].

Todo esto hace que estemos en un panorama adverso, debemos hacer frente a un nuevo reto, y es que la veloz evolución de la tecnología supera con creces la capacidad de adaptación de nuestro ordenamiento jurídico. La consecuencia de este desarrollo y la aparición de los nuevos métodos delictivos a través de las TIC han requerido cambios en las leyes existentes, incluso la creación de nuevas normativas.

En algunos países, como Estados Unidos y Chile, se ha optado por establecer nuevas leyes específicas para tipificar estos delitos emergentes. Por otro lado, países como España y Austria han priorizado modificar las normas existentes, ampliando su alcance para abarcar los nuevos tipos de delitos [4].

[3] MIRÓ, F. “Delincuencia asociada al uso de las TIC”. [Recurso de aprendizaje textual]. *Fundación Universitat Oberta de Catalunya (FUOC)*, 2013.pp. 7-38.
[4] HERNÁNDEZ, S. O. La regulación de los delitos con origen tecnológico. *Revista Aranzadi Doctrinal*, (9), 6, 2022.

Según Eloy Velasco Núñez, Magistrado-Juez del Juzgado Central de Instrucción 6 de la Audiencia Nacional, el concepto de Delito Informático abarca tanto las infracciones tradicionales cometidas mediante ordenadores o Internet[5] como los delitos específicamente dirigidos contra la informática. Estos últimos afectan a los datos o sistemas informáticos y las vías telemáticas de comunicación, especialmente a través de Internet[6].

Fernando Miró Llinares, como consecuencia de esta penetración de las TIC en la sociedad, y paralelamente en derecho penal, expone tres amplios grupos de ciberataques en el ciberespacio, cada uno con sus propias características y objetivos, sobre los cuales profundizaré más adelante.

En primer lugar, los ciberataques puros. Este grupo engloba acciones como el hacking, las infecciones de malware, la ocupación o uso no autorizado de redes y las redes antisociales. Estos ataques se centran en la manipulación o interrupción de sistemas informáticos.

Otro grupo son los ciberataques réplica. Encontramos aquí actividades como el ciberfraude, el robo de identidad, la suplantación de identidad, el espionaje cibernético, el blanqueo de capitales y la extorsión cibernética, así como el acoso cibernético. Estos ataques a menudo buscan obtener beneficios económicos o perjudicar a individuos.

Y, por último, los ciberataques de contenido. Se trata de la difusión de contenidos ilícitos. Incluye áreas sensibles como la pornografía infantil en internet, la ciberpiratería intelectual y la difusión de otros contenidos ilícitos.[7]

Como señala Camacho Losa, “En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia”[8]. Entonces ¿por qué razón la informática habría de ser diferente?

---

[5] Como las injurias por correo electrónico

[6] Por ejemplo, daños informáticos causados por virus.

[7] MIRÓ, F. “Delincuencia asociada al uso de las TIC”. [Recurso de aprendizaje textual]. *Fundación Universitat Oberta de Catalunya (FUOC)*, 2013.
pp. 7-38.

[8] HUERTA MIRANDA, M y LÍBANO MANZUR, C *Los Delitos Informáticos*, Editorial Jurídica Cono Sur. 2016.

3 MARCO NORMATIVO

Es crucial empezar analizando qué legislación afecta a la ciberdelincuencia. Debemos aclarar que, como se ha mencionado, el avance de las TIC ha transformado diversos aspectos de la sociedad. Esto ha generado un debate entre los expertos sobre si estamos frente a una forma autónoma de delincuencia, lo que implicaría la existencia de un "delito informático" independiente, o si simplemente estamos tratando los mismos delitos, pero cometidos mediante las TIC. Aunque no hay consenso absoluto, en España, el delito informático ha impulsado al legislador a modificar la normativa existente para ampliar su alcance y afrontar los nuevos hechos delictivos.

Aunque como hemos visto los delitos informáticos no se consideran una categoría específica de delito en la legislación española, existen diversas normativas vinculadas a este tipo de comportamientos.

Antes de abordar esa cuestión, es fundamental realizar un examen de las normas legales que pueden tener repercusiones en España. Para ello, debemos considerar tanto la legislación a nivel nacional como los tratados internacionales y los acuerdos establecidos en el contexto de la Unión Europea, los cuales vinculan nuestro sistema jurídico nacional.

En el ámbito de la ciberseguridad, es esencial comprender el marco normativo nacional que regula los delitos informáticos o ciberdelitos en España. A lo largo de esta exploración, analizaremos de manera general las leyes y regulaciones específicas que rigen estas conductas ilícitas en nuestro país.

Además, nos adentraremos en la Estrategia de Seguridad Nacional en materia de ciberseguridad, examinando cómo España aborda los desafíos digitales y protege la seguridad cibernética en un entorno cada vez más interconectado.

3.1 CÓDIGO DE DERECHO DE LA CIBERSEGURIDAD

Existe un Código de Derecho de la Ciberseguridad, que contiene las normas vinculadas al ámbito digital entendido en sentido amplio y

especialmente dirigido a la salvaguarda de la seguridad nacional, las infraestructuras críticas, la seguridad ciudadana, las telecomunicaciones y el comercio electrónico. Además, se hace referencia a las leyes especiales que pueden estar relacionadas con la imputación por ciberdelitos, como la Ley de Protección de Datos, la Ley General de Telecomunicaciones y la Ley de Seguridad Nacional.

El Código de Derecho de la Ciberseguridad en un compendio normativo publicado por el Instituto Nacional de Ciberseguridad (INCIBE) y la Agencia Estatal del Boletín Oficial del Estado, cuya última actualización es de mayo de 2024, con el objetivo de facilitar el acceso a la normativa vigente en materia de ciberseguridad. Este Código no es una ley en sí misma, sino una recopilación de normas y disposiciones dispersas en diferentes textos legales, tanto nacionales como internacionales. [9]

El Código se estructura en torno a cinco grandes bloques. En primer lugar un marco normativo general que incluye la normativa básica sobre ciberseguridad, como la Ley de Seguridad Nacional, la Ley que establece medidas para la protección de las infraestructuras críticas, y el Esquema Nacional de Seguridad. El segundo bloque es el de la protección de la información y de los sistemas de información. Recoge la normativa sobre la protección de datos, seguridad de la información y seguridad de las redes y sistemas.

El tercer bloque incluye la normativa sobre defensa nacional en el ciberespacio, como el Código Penal y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. La ciberdefensa comprende el cuarto bloque que trata sobre defensa nacional en el ciberespacio, como la Estrategia Nacional de Ciberseguridad. Por último, incluye el bloque de la

[9] Instituto Nacional de Ciberseguridad (INCIBE) & Boletín Oficial del Estado (BOE). (2024*). Código de Derecho de la Ciberseguridad.* Edición actualizada a 3 de mayo de 2024. [Publicación electrónica]. <https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad> *). [Consultado el 20 de mayo de 2024].*

cooperación internacional en materia de ciberseguridad, como el Convenio de Budapest sobre ciberdelincuencia. [10]

La importancia de este Código la encontramos en la necesidad de recopilar normas dispersas en un único documento, en el fomento del buen uso de las TIC y en fortalecer el marco legal de nuestro país.

En resumen, el Código de Derecho de la Ciberseguridad es una síntesis normativa que reúne regulaciones relacionadas con la ciberseguridad.

3.2 MARCO LEGAL: CONJUNTO DE REGULACIÓN EUROPEA

Para completar el marco legal debemos hablar también de la normativa europea. Este tipo de delitos cibernéticos no solo han ido en aumento en toda Europa, sino que también hay que destacar su elaboración y sofisticación.

Según la web oficial del Consejo Europeo *"se espera que 41.000 millones de dispositivos en todo el mundo estén conectados a la internet de las cosas de aquí a 2025"*, por lo que esta tendencia incrementara en los años venideros.

Uno de los instrumentos normativos más importantes en el contexto europeo es el Convenio sobre Ciberdelincuencia, también conocido como Convenio de Budapest, fue firmado en Budapest, Hungría, el 23 de noviembre de 2001.[11] Este tratado es relevante en materia de ciberdelincuencia y pruebas electrónicas.

El convenio tiene como objetivo lograr una mayor unidad entre los Estados miembros del Consejo de Europa y fomentar la cooperación internacional en la lucha contra la ciberdelincuencia. Reconoce los cambios profundos causados por la digitalización, la convergencia y la globalización en las redes.

---

[10] Campus Stellae. (s.f.*). ¿Qué es el Código de Derecho de la Ciberseguridad*? [en línea]. Recuperado de https://campus-stellae.com/que-es-el-codigo-de-derecho-de-la-ciberseguridad/ [20 de mayo de 2024]

[11] *Parlamento Europeo. (2001). Convenio sobre Ciberdelincuencia [documento en línea]. Consejo de Europa. Budapest: Oficina de Publicaciones del Consejo de Europa. Enlace. (Número de documento: 7 Conv. Budapest). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221 [Consultado el 20 de mayo de 2024].*

Además, busca proteger la confidencialidad, integridad y disponibilidad de sistemas informáticos, redes y datos. Proporciona disposiciones para la criminalización de conductas relacionadas con el uso indebido de estos sistemas y la cooperación internacional en la detención, investigación y enjuiciamiento de los delitos cibernéticos.

El Convenio busca un equilibrio adecuado entre los intereses de la aplicación de la ley y el respeto de los derechos humanos fundamentales, como la libertad de expresión y la privacidad. [12]

Otra regulación europea importante es la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, que se refiere a los ataques contra los sistemas de información y sustituye a la Decisión Marco 2005/222/JAI del Consejo.[13] Su objetivo es armonizar las normas penales en los Estados miembros relacionadas con los ataques a sistemas de información. Establece definiciones de infracciones penales y sanciones aplicables, así como la mejora de la cooperación entre autoridades competentes y organismos especializados de la Unión, como Eurojust, Europol y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA). La seguridad de los sistemas de información es crucial para el desarrollo del mercado interior y una economía competitiva e innovadora.

4 CONCEPTO Y CLASIFICACIÓN DE LOS CIBERDELITOS EN NUESTRO CÓDIGO PENAL.

4.1 APROXIMACIÓN AL CONCEPTO

En primer lugar, abordaremos el tema definiendo qué es un ciberdelito. Se trata de un ilícito penal para cuya consumación son necesarios los medios tecnológicos sin autorización ni consentimiento, pudiendo afectar a bienes

[12] *Consejo de Europa. "20th anniversary Budapest Convention - Cybercrime" [en línea]. Consejo de Europa. Noviembre de 2001. <https://www.coe.int/en/web/cybercrime/20th-anniversary-budapest-convention> [Consultado el 20 de mayo de 2024].*

[13] Unión Europea. (2013). 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. Diario Oficial de la Unión Europea, L 304/18. <https://www.boe.es/doue/2013/218/L00008-00014.pdf > *[Consultado el 20 de mayo de 2024].*

jurídicos individuales o supraindividuales. Constituyen acciones típicas, antijuridicas, culpables y punibles que se distinguen por las complejidades de la investigación y la prueba de este tipo de delitos, debido a su regularidad, el grave daño que pueden causar y la dificultad para atrapar a los delincuentes, ya que operan en varios países.[14]

Este tema ha generado algún que otro problema terminólogo en la doctrina. Por un lado, existen los que defienden que los delitos tecnológicos han de considerarse delitos independientes. Sin embargo, la corriente doctrinal mayoritaria (Claudio Magliona, Macarena López, Romeo Casabona y Davara Rodríguez) se inclina más hacia la noción de "criminalidad informática" en lugar de referirse a "ciberdelitos"; esto es así porque no se puede hablar solamente de un único delito informático, sino más bien de varios; y aunque todos estén caracterizados por el uso de medios tecnológicos, el bien jurídico afectado no es uniforme, ni tampoco lo es la forma de comisión. [15]

Pese a esto, el término empleado en el marco internacional es "ciberdelito" tras el Convenio de Ciberdelincuencia, a través del cual hace referencia a aquellos delitos cometidos a través de las TIC, ya sean utilizadas como medio o como objetivo del delito y siempre que las nuevas tecnologías sean imprescindibles para su ejecución. [16]

La delincuencia encuentra nuevas vías para manifestarse, dando lugar a la ciberdelincuencia, un fenómeno que abarca dos realidades, en primer lugar, los ciberdelincuentes dirigen sus acciones directamente contra sistemas informáticos, datos o redes de comunicación.

Su objetivo es dañar, bloquear, alterar o eliminar información crucial para el funcionamiento de estos sistemas. Entre sus métodos más comunes se encuentran el bloqueo de sistemas, la destrucción de programas, los daños a dispositivos de almacenamiento, la alteración o eliminación de datos y el uso ilícito de información. Internet se convierte en su principal campo de batalla, aunque no es el único, ya que estos ataques también pueden darse en otros entornos informáticos.

---

[14] MARTÍNEZ ATIENZA, G. *Ciberdelitos: Instrucción y prueba*. Ulzama Digital. España. 2022.
[15] HUERTA MIRANDA, M y LÍBANO MANZUR, C *Los Delitos Informáticos*, Editorial Jurídica Cono Sur. 2016.
[16] MARTÍNEZ ATIENZA, G. *Ciberdelitos: Instrucción y prueba*. Ulzama Digital. España. 2022.

En segundo lugar, la ciberdelincuencia se nutre de delitos preexistentes que ahora se llevan a cabo utilizando herramientas informáticas. Fraude, robo de identidad, tráfico de drogas o pornografía infantil son solo algunos ejemplos de cómo los delincuentes tradicionales han encontrado en internet un nuevo aliado para sus actividades ilícitas. En este caso, internet o un ordenador se convierten en la herramienta que facilita o ejecuta el delito, aprovechando las vastas posibilidades que ofrece el mundo digital.

En definitiva, la ciberdelincuencia representa dos caras de una misma moneda; por un lado, ataques directos a la infraestructura informática y, por otro, la comisión de delitos tradicionales mediante herramientas digitales. [17]

En nuestro derecho no existe una definición legal ni una tipificación autónoma del ciberdelito, más bien se considera un medio para la comisión de delitos ya recogidos en el Código Penal, pero para los que ahora se recogen específicas formas de comisión.

4.2 CLASIFICACIÓN

La característica de los delitos cometidos a través de las TIC es la facilidad en su ejecución, pues en ocasiones no son necesarios grandes conocimientos técnicos ni recursos materiales para llevarlos a cabo.

El daño que pueden causar los delitos informáticos es muy desproporcionado en comparación con los recursos que se necesitan para cometerlos. Además, los delincuentes pueden aprovechar las lagunas legales que existen en algunos países, conocidos como “paraísos cibernéticos”, donde este tipo de delitos no se tipifican o sancionan adecuadamente.[18]

La categorización de los ilícitos informáticos constituye una materia de considerable complejidad, tal como he mencionado previamente, sujeta a un desarrollo incesante. Los delitos perpetrados mediante el uso de tecnologías de la información y comunicación representan un reto significativo para la legislación penal.

---

[17] VELASCO NÚÑEZ, E., DELITOS *TECNOLÓGICOS. Cuestiones penales y procesales*. Wolters Kluwer, España, S.A. 2021. pp. 23-25

[18] DE LA CUESTA ARZAMENDI, J. L., PÉREZ MACHÍO, A. I., & SAN JUAN, C. *Aproximaciones criminológicas a la realidad de los ciberdelitos.* Editorial Aranzadi, S.A.U. 2010.

La catalogación de este grupo delictivo es diversa y algo compleja, dada la naturaleza cambiante y el desarrollo incesante de las tecnologías digitales. Sin embargo, podemos categorizarlos en tres grandes grupos, delitos contra la propiedad, delitos contra la intimidad y privacidad y delitos contra el Gobierno.

La importancia de los ciberdelitos en el panorama actual es indiscutible. Vivimos en una era donde la digitalización de la sociedad ha aumentado la dependencia de los sistemas informáticos, lo que a su vez ha incrementado la superficie de ataque para los ciberdelincuentes.

Los ciberdelitos tienen un impacto significativo en la economía global, con pérdidas millonarias cada año, y afectan a la seguridad y privacidad de individuos y organizaciones.

Además, como he mencionado previamente, la ciberdelincuencia plantea desafíos para la legislación y la aplicación de la ley. La ciberseguridad se ha convertido en una prioridad para proteger gobiernos y empresas, buscando proteger la integridad de los datos y la confianza en los sistemas digitales.

Dentro de este amplio concepto, se ha considerado desarrollar una clasificación tripartita: los delitos económicos patrimoniales relacionados con la informática, los atentados contra la intimidad y privacidad, perpetrados mediante medios informáticos, así como los ataques a intereses supraindividuales a través de dichos medios.

4.2.1 DELITOS ECONÓMICO- PATRIMONIALES VINCULADOS A LA INFORMÁTICA.

En el ámbito de la informática, se presentan delitos que afectan directamente al patrimonio de terceros. Estos actos tienen como objetivo obtener beneficios económicos o apoderarse de bienes a través de medios digitales.

Según Eloy Velasco Núñez *“esos tipos penales estadísticamente suponen cerca del 80% de los delitos informáticos que se denuncian”*

En el marco de nuestro sistema legal, el Código Penal tipifica las siguientes conductas con la modalidad de ciberdelito:

- Robo inutilizando sistemas de guardia criptográfica (Art. 238 CP), en su quinto apartado considera que el uso de sistemas específicos de alarma o guarda será considerado robo con fuerza.

- Estafa informática (Art. 249 CP), esta modalidad específica de estafa habla de las manipulaciones informáticas utilizadas en perjuicio de terceros siendo el engaño el medio empleado para logarlo.
- La defraudación de telecomunicaciones informáticas (Art 255 CP), según este artículo, será castigado con una pena de multa de tres a doce meses quien cometa defraudación utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos.
- El uso no autorizado de terminales informáticos (Art 256 CP), sancionando a quienes lo realicen sin consentimiento y causen perjuicio económico, dependiendo la gravedad del monto del perjuicio económico.
- La extorsión informática mediante ransomware (Art. 243 CP), sancionando a quienes, con ánimo de lucro, coaccionan a otros para realizar o evitar acciones perjudiciales para su patrimonio o el de terceros.
- Los daños informáticos (Art. 264 bis CP), sancionando la obstaculización de sistemas informáticos ajenos y contemplando diversas situaciones y penas según la gravedad y las circunstancias.
- Los delitos contra la propiedad intelectual o industrial informática (Arts. 270-275 CP), incluyen la piratería (copia y distribución sin permiso), la exportación ilegal de obras, la venta ambulante de obras sin autorización, la fabricación o importación de software para eludir protecciones de derechos de autor y la responsabilidad penal de las empresas en estos casos.
- El espionaje informático de secretos de empresa (Arts. 278-280 CP). Estos artículos sancionan el apoderamiento y difusión de secretos de empresas, protegiendo la confidencialidad y capacidad competitiva de las organizaciones.
- La publicidad engañosa (Art. 282 CP). Establece que fabricantes o comerciantes que realicen alegaciones falsas o manifiesten características inciertas sobre productos o servicios en su publicidad serán castigados.

- Las manipulaciones en aparatos en perjuicio del consumidor (Art. 283 CP). Penaliza la alteración o manipulación de aparatos automáticos cuando se factura más de lo debido al consumidor.
- Las manipulaciones informáticas de precios de cotización de instrumento financiero, contrato de contado sobre materias primas o índice de referencia (Art. 284.1. 2º CP). Sanciona las manipulaciones informáticas de precios en el ámbito financiero, castigando a quienes alteren los precios de instrumentos financieros, contratos de contado sobre materias primas o índices de referencia mediante operaciones fraudulentas o información engañosa.
- Los delitos contra el mercado televisivo (Art. 286 CP). Sanciona la facilitación no autorizada de acceso a servicios de radiodifusión o televisión, castigando a quienes, sin consentimiento del prestador de servicios, con fines comerciales, permitan el acceso inteligible a dichos servicios o suministren acceso condicional a los mismos.
- El blanqueo informático de capitales (Art. 301 CP). Sanciona a quienes adquieran, posean, utilicen, conviertan o transmitan bienes sabiendo que provienen de una actividad delictiva. Las penas incluyen prisión de seis meses a seis años y multa del tanto al triplo del valor de los bienes. Si los hechos se cometen por imprudencia grave, la pena es de prisión de seis meses a dos años y multa del tanto al triplo.
- La falsedad documental en soporte electrónico (Art 390 CP). Establece las penas para la falsificación de documentos públicos, oficiales y mercantiles, así como de los despachos transmitidos por servicios de telecomunicación. La pena para autoridades o funcionarios públicos que cometan falsedad en el ejercicio de sus funciones es de prisión de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial de dos a seis años.[19]

[19] VELASCO NÚÑEZ, E., DELITOS *TECNOLÓGICOS. Cuestiones penales y procesales*. Wolters Kluwer, España, S.A. 2021. Pp. 25

4.2.2 ATENTADOS POR MEDIOS INFORMÁTICOS CONTRA LA INTIMIDAD Y LA PRIVACIDAD.

Consiste en los ataques contra el bien jurídico de la privacidad**.** Este concepto, que incluye la intimidad, va más allá y abarca todas las modalidades protegidas en el artículo 18 de la Constitución Española**.** Se considera que interesa al delincuente obtener información sobre aspectos de la vida privada de otras personas, especialmente en lo que respecta a la sexualidad. Además, se añade el uso de la informática y las redes para difundir ideas que inciten a la violencia.

Según Eloy Velasco Núñez "suponen el 18% aproximado de los delitos que se denuncian".

Nuestro Código Penal regula este tipo de delitos:

- Las amenazas y coacciones informáticas (Art. 169 y 172 CP). Abarcan aquellas conductas que se realizan a través de internet, teléfonos, mensajes, etc.
- La posesión y distribución de material pornográfico y pornografía infantil (Art. 189 CP). Serán ciberdelitos cuando tanto la posesión como la distribución se lleven a cabo a través de internet o dispositivos electrónicos.
- El child grooming y el sexting (Art. 183 ter CP). El primero es un delito por el cual un adulto utiliza internet y las TIC para establecer una relación con un menor. Mientras que el segundo implica el envío, recepción o posesión de imágenes o videos de contenido sexual a través de medios informáticos, ambos, afectando a menores.
- El acoso o stalking (Art. 172 ter CP). Ambos comparten la intimidación a la víctima, el acoso puede incluir acciones que incluyan stalking si el acoso se lleva a cabo a través de mensajes amenazantes o difusión no autorizada de imágenes intimas.
- El descubrimiento y revelación de secretos, espionaje informático o hacking (Art. 197- 200 CP), relacionados íntimamente con la obtención y divulgación de información.

- Las injurias y calumnias informáticas (arts. 205- 216 CP). Mientras que las primeras solo son delito si son públicas, las segundas siempre se consideran delito. En el tema que nos ocupa, se consideran ciberdelitos siempre y cuando se realicen a través de materiales informáticos.
- La cesión inconsentida de datos ajenos (Art. 417, 418 y 423 CP), afectando a la privacidad o confidencialidad de las personas a través de medios informáticos.
- El delito de incitación conta el orden público agravado (Art. 559 CP), cuando se realice a través de las redes sociales, foros y otras plataformas.[20]

4.2.3 ATAQUES POR MEDIOS INFORMÁTICOS CONTRA INTERESES SUPRAINDIVIDUALES.

Nos referimos a ataques de mayor gravedad que afectan indiscriminadamente a los intereses generales de la población. La intención detrás de estos ataques es generar pánico y terror con el objetivo de subvertir el orden constitucional, suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas, económicas o sociales del Estado. Además, buscan forzar a los poderes públicos a llevar a cabo un acto específico o abstenerse de hacerlo. Estos ataques también pueden alterar gravemente la paz pública, desestabilizar el funcionamiento de una organización internacional o provocar un estado de terror en la población.

Según Eloy Velasco Núñez “Apenas tiene incidencia estadística, pero su intención genera mucha intranquilidad”.

Algunas acciones que se relacionan con el terrorismo informático específico (Art. 573.2, 577.2 y 578 del CP) pueden considerarse similares al mismo. Estas incluyen la usurpación de funciones públicas (Art. 402 del CP) y la revelación de secretos relacionados con la defensa nacional (Art. 598 y 603 del CP).[21]

[20] VELASCO NÚÑEZ, E., DELITOS *TECNOLÓGICOS. Cuestiones penales y procesales*. Wolters Kluwer, España, S.A. 2021. pp. 26

[21] VELASCO NÚÑEZ, E., DELITOS *TECNOLÓGICOS. Cuestiones penales y procesales*. Wolters Kluwer, España, S.A. 2021. pp. 26-27.

4.3 CONDUCTAS ESPECÍFICAS

4.3.1 PHISHING

La suplantación de identidad en internet, conocida como “phishing”, tiene como objetivo apoderarse de datos confidenciales de los usuarios para perjudicar su patrimonio. Este delito implica obtener información, como números de tarjetas de crédito, contraseñas o datos bancarios, mediante engaños. El “phishing” se lleva a cabo principalmente a través de correos electrónicos o ventanas emergentes. En estos caso el estafador se hace pasar por una entidad de confianza, como un banco, y obtiene información confidencial de forma fraudulenta. Posteriormente, puede utilizar estos datos para realizar transferencias bancarias no autorizadas.[22]

La mayoría de los métodos de phishing emplean técnicas engañosas en su diseño para que los enlaces en correos electrónicos parezcan organizaciones legítimas. La efectividad del anzuelo depende de la habilidad del phisher. En todos los casos se puede evaluar la gravedad del delito cometido, similar a como sucede en las estafas. Además, la víctima suele contribuir con cierta negligencia, y es importante considerar las circunstancias subjetivas que influyen en ella.

En otro método común de phishing, el atacante utiliza el propio código de programa del banco o servicio al que pretende representar. Este tipo de ataque es especialmente problemático, ya que lleva al usuario a iniciar sesión en la página del banco o servicio, donde la URL y los certificados de seguridad parecen legítimos. En este ataque, conocido como Cross Site Scripting, los usuarios reciben un mensaje que les insta a “verificar” sus cuentas, seguido de un enlace que parece auténtico. Sin embargo, el enlace ha sido modificado para llevar a cabo el ataque, y es difícil de detectar sin conocimientos especializados.

Otro aspecto relevante es el blanqueo de dinero. Actualmente, empresas ficticias intentan reclutar teletrabajadores a través de correos electrónicos, chats y otros medios, ofreciéndoles la oportunidad de trabajar desde casa y

[22] RODRÍGUEZ-MAGARIÑOS, F. (2009). Nuevos delitos informáticos: phishing, pharming, hacking y cracking. *Práctica Penal*, *48*, 14-32.

otros beneficios atractivos. Sin saberlo, quienes aceptan estas ofertas se convierten en víctimas de un grave delito: el “lavado de dinero” obtenido mediante el acto fraudulento del phishing.

El spear phishing es una variante más específica y dirigida del phishing. En este tipo de ataque los ciber delincuentes se enfocan en objetivos concretos, como individuos o grupos dentro de una organización. A diferencia del phishing genérico, el spear phishing personaliza los mensajes según la información pública que los atacantes han recopilado sobre la víctima. Esto puede incluir detalles como su especialización, funciona en la organización, intereses personales y datos residenciales.

El objetivo es hacer que el mensaje parezca más legítimo y aumentar la probabilidad de que la víctima haga click en enlaces maliciosos o descargue de archivos adjuntos. [23]

En cuanto a su regulación, tras la Ley Orgánica 14/2022, de 22 de diciembre de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso, se han incorporado nuevas conductas típicas, además de una reforma sobre la estafa informática. En el Preámbulo de la Ley se refleja el crecimiento exponencial de los delitos informáticos en los últimos años como consecuencia de un crecimiento paralelo del ciberespacio y de la población que interactúa en él, es decir, la ciber-población.

El legislador ha introducido nuevas figuras penales junto a las ya existentes para adaptar los tipos penales a las tecnologías emergentes. Según el Preámbulo de la Ley, se busca simplificar la incorporación de las regulaciones derivadas de la Directiva (UE) 2019/713, de 17 de abril. [24]

Centrándonos en la jurisprudencia, el Alto Tribunal ha ido analizando durante varios años el delito de estafa informática. En la sentencia 2 de diciembre de 2014 (RJ 845, 2014)[25], el Tribunal Supremo clasifica las

[23] RODRÍGUEZ-MAGARIÑOS, F. Nuevos delitos informáticos: phishing, pharming, hacking y cracking. *Práctica Penal*, *48*, 2009. Pp 3-4.
[24] ALMIRÓN, F. R. “El delito de estafa informática.: ¿es posible determinar la responsabilidad civil de la entidad financiera en base al artículo 120?3 del código penal como consecuencia del «phishing»”. *Revista de Derecho Penal y Criminología*, *30*(JUNIO). 2023.pp 283-284.
[25] STS de 2 de diciembre de 2014, (ECLI: ECLI:ES:TS:2014:5632)

conductas de phishing bancario como una estafa del art. 249.2 a) CP. En estos casos, la conducta básica consiste en enviar correos electrónicos fraudulentos desde direcciones que aparentan ser de entidades bancarias. Estos correos solicitan datos personales, como las credenciales de acceso a las cuentas (nombre de usuario y contraseña) que las víctimas tienen en la entidad. Además, se utilizan enlaces a sitios web casi idénticos o muy similares a los de las entidades bancarias para engañar a los usuarios y obtener beneficios económicos ilícitos mediante transferencias a cuentas controladas por los autores del delito

Además, la sentencia de la Audiencia Provincial de Vizcaya 10 de noviembre de 2016 (RJ 429/2016)[26] destaca que en el phishing bancario es común que los internautas reciban correos electrónicos que le instan a verificar sus cuentas, seguidos de enlaces que parecen ser de la página web oficial de la entidad bancaria.

La sentencia emitida por la Audiencia Provincial de Valencia el 25 de enero de 2017 (RJ 37/2017)[27] ahonda en los conceptos de “phishing” y “mulero” analizando un caso en el que Bankia S.A., como entidad que ofrece servicios de pago en línea, logró detener las transferencias realizadas por el autor del delito. La institución actuó con diligencia y no se generó responsabilidad contractual, ya que había tomado las medidas necesarias para prevenir el delito.

El phishing, según la Audiencia Provincial de Valencia implica “enviar una oferta de trabajo a la cuenta de correo electrónico de un usuario. Desde su propio domicilio, el usuario puede acceder a cuentas corrientes de personas desconocidas. Estas personas han proporcionado voluntariamente sus datos al recibir el correo, lo que resulta en ingresos ilegales. El dinero obtenido generalmente proviene de la sustracción de cuentas bancarias a las que se ha tenido acceso. Este dinero llega a cuentas difíciles de identificar o localizar.”

La Audiencia también se pronuncia sobre el phishing bancario, una técnica de ingeniería social que busca obtener información confidencial de forma fraudulenta. Esto se logra mediante la suplantación de páginas web o el

[26] SAP de Vizcaya de 10 de noviembre de 2016 (ECLI: ES:APBI:2016:2070)
[27] SAP de Valencia de 25 de enero de 2017 (ECLI: ES:APV:2017:1066)

envío de correos electrónicos aparentemente oficiales en nombre de empresas o entidades de confianza. Estos correos solicitan datos del usuario, como contraseñas de acceso a servicios de pago en línea.

Por lo tanto, a modo de conclusión, la entidad bancaria tiene la responsabilidad de implementar diversas estrategias o acciones para prevenir el robo de datos personales relacionados con transacciones económicas estableciendo una responsabilidad cuasi-objetiva para las entidades bancarias basándose en la falta de diligencia de los bancos.[28]. Frente a estas actuaciones fraudulentas se abren dos posibles vías judiciales: la denuncia para intentar que se identifique al autor de los hechos (que rara vez será solvente y podrá abonar la responsabilidad civil derivada del delito), y la reclamación en vía civil a la entidad bancaria por deficiente control de sus medios telemáticos de gestión.

4.3.2 SPYWARE

El spyware, también conocido como “software espía”, es un tipo de software malicioso que se instala en un dispositivo informático sin el conocimiento del usuario. Su función principal es espiar al usuario, recopilando información confidencial y datos de uso de internet para transmitirlos a terceros, como anunciantes o empresas de datos.

El spyware puede robar información como números de tarjetas de crédito, contraseñas y hábitos de navegación web. Además, puede afectar negativamente al rendimiento del sistema, ralentizando el dispositivo y generando ventanas emergentes no deseadas.

El spyware ha evolucionado con el tiempo, incorporando sofisticados mecanismos propios de los rootkits (un software que facilita a un intruso obtener control especial sobre un sistema comprometido)[29]. Estos mecanismos permiten al spyware ocultar su presencia a administradores o a software

[28] GARCÍA GARCÍA, D. E. El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016). *Iuris Tantum Revista Boliviana de Derecho*, (25), 650-661. 2018. Pp 6-10

[29] CONDE, M., RODRIGUEZ, G., & ORTIZ, J. A. Soporte de red en rootkits de linux. (s.f).

destinado a su detección. Además, estrategias como la ocultación de procesos, archivos o conexiones de red, junto con técnicas antidebugging o de criptografía, son características comunes en el spyware actual. Para evitar ser eliminado del sistema infectado, también se incluyen estrategias que dificultan su desinstalación.

Sin embargo, estas metodologías evasivas, junto con los mecanismos de recopilación de información, a veces pueden provocar inestabilidad en el sistema y comportamientos inesperados en algunas aplicaciones.[30]

A modo de ejemplo, España ha sido víctima de espionaje a través de esta figura, en abril de 2022, el Citizen Lab, un laboratorio multidisciplinario de la Universidad de Toronto enfocado en la investigación, desarrollo de información y comunicación en tecnología, derechos humanos y seguridad global, denunció que al menos 65 teléfonos pertenecientes a figuras políticas catalanas, sus familiares, abogados, representantes de la sociedad civil y organizaciones no gubernamentales vinculadas al independentismo catalán, habían sido objeto de espionaje. Pocos días después, el Gobierno hizo público que Pedro Sánchez (Presidente del Gobierno), Margarita Robles (Ministra de Defensa) y Fernando Grande-Marlaska (Ministro del Interior) también habían sido víctimas de esta vigilancia. El espionaje se llevó a cabo mediante el spyware conocido como Pegasus.

Tras el escándalo del "caso Pegasus", ocurrido el 26 de mayo de 2022, el Jefe de Gobierno español anunció la aprobación en el Congreso de una nueva Ley de Seguridad Nacional (LSO) y la reforma de la Ley Orgánica que regula el control judicial del Centro Nacional de Inteligencia (CNI). El proyecto de ley de información clasificada fue aprobado en el Congreso el 1 de agosto de 2022, con el objetivo de armonizar la legislación española con los estándares de gestión de información clasificada de las democracias más desarrolladas de la Unión Europea y la OTAN. Esta ley busca establecer un equilibrio entre la transparencia y el derecho a la información, por un lado, y la seguridad nacional, por otro.[31]

---

[30] CASTILLO-PÉREZ, S., ANDRÉS, J. A. M., & GARCIA-ALFARO, J. El Spyware como amenaza contra navegadores web. (s.f).

[31] BETRÁN, Y. (2023). El secreto oficial en la legislación y la jurisprudencia española.: Análisis y crítica. *Derecom*, (34), 2023. Pp 10-21.

4.3.3 MALWARE Y RANSOMWARE

El malware es un tipo de software que se ejecuta en un equipo sin que el propietario o usuario lo sepa o lo haya autorizado. Este programa realiza acciones en el sistema que pueden ser dañinas tanto para el usuario como para el propio sistema.[32]

En Ransomware “secuestro de datos”, es un software malicioso que limita el acceso a distintas áreas o archivos del sistema infectado solicitando un rescate para eliminar esta restricción.[33]

En Ransomware, en la actualidad, representa la amenaza de malware más alarmante. Se espera que esta tendencia continúe, lo que ha llevado a las fuerzas de seguridad y a la industria a centrarse en minimizar sus riesgos a través de campañas de concienciación y prevención.

El incremento en la utilización de teléfonos móviles ha fomentado la creación de malware diseñado específicamente para estos dispositivos. Anteriormente, el ransomware solía afectar principalmente a usuarios individuales, pero en la actualidad su enfoque ha cambiado. Ahora, su objetivo principal es bloquear la información en organizaciones y empresas. Un ejemplo notable de un ciberataque de ransomware a gran escala ocurrió el 13 de mayo, afectando sistemas informáticos en numerosos países, incluyendo la sede de Telefónica en Madrid, el sistema de salud británico y el Ministerio del Interior ruso, entre otros. [34]

El ámbito legal considera la existencia de una nueva generación de delitos perpetrados a través de los sistemas informáticos, internet y otras tecnologías de la información y comunicación (TIC). Los estados incluyen disposiciones sobre ciber delitos en sus códigos penales, como es el caso de España, o en leyes penales específicas como en Estados Unidos o Reino Unido.

---

[32] INCIBE. (s.f.). Malware. INCIBE. [en línea] <https://www.incibe.es/aprendeciberseguridad/malware>. [Consulta: 21 junio 2024.]

[33] Noticia relativa a “la respuesta del Derecho frente a los ataques de “ransomware” [en línea]< https://cincodias.elpais.com/cincodias/2019/11/06/legal/1573063068_861999.html> [Consulta: 22 de junio 2024]

[34] Noticias relativa al ataque de “ransomware” de mayo 2017. [En línea]. <http://elpais.com/tag/ataques_informaticos/a> [Consulta: 22 junio 2024].

Además, existen acuerdos internacionales, como el convenio sobre la ciberdelincuencia adoptado en Budapest el 23 de noviembre de 2001. La Unión Europea también ha promulgado directivas para armonizar la regulación dentro de su territorio.

En este contexto la categoría de ciber delitos aborda las particularidades de este tipo de actividad criminal y las consecuencias derivadas de la naturaleza de internet como medio para cometer delitos. Esto incluye desafíos como la determinación del lugar de comisión de los ilícitos (necesaria para establecer jurisdicción y competencia penal), la localización y obtención de pruebas, las lagunas en la tipificación de ciertas conductas y el impacto de la investigación policial en este sentido protegiendo los derechos fundamentales de los ciudadanos.

Los ataques de ransomware, en particular, se ajustan al perfil de los delitos de daños y sabotajes (conocidos como 'cracking') contemplados en nuestro Código Penal. El artículo 264 actual del Código Penal (CP) penaliza las acciones dirigidas contra datos, programas informáticos o documentos electrónicos ajenos, mientras que las relacionadas con el funcionamiento normal de sistemas informáticos ajenos se sancionan en el nuevo artículo 264 bis CP. Además, el artículo 264.2 CP establece penas más severas cuando estos delitos se cometen en el contexto de una organización criminal, cuando se han causado daños graves o cuando se han afectado los intereses generales.

Sin embargo, identificar y castigar a los ciberdelincuentes no es tarea fácil. Las dificultades surgen en parte debido a la naturaleza transnacional de la ciberdelincuencia, con sus desafíos específicos. Pero, sobre todo, los mayores obstáculos provienen de las características fundamentales de Internet: su descentralización, universalidad, posibilidad de anonimato y la falta de una autoridad central con competencias suficientes para regular toda la actividad en el ciberespacio.[35]

[35] Noticia relativa a "la respuesta del Derecho frente a los ataques de "ransomware" [en línea]< https://cincodias.elpais.com/cincodias/2019/11/06/legal/1573063068_861999.html> [Consulta: 22 de junio 2024]

4.3.4 CYBERBULLING

Desde que el fenómeno del bullying se comenzó a investigar en los años 70 se ha venido debatiendo sobre las características y elementos que forman parte de su definición, incluyendo quién debe ser el autor de la agresión (ya sea un grupo de compañeros o una sola persona), o las diferentes formas en las que se puede producir la agresión ya sea físicas, psicológicas o verbales. Elementos importantes de esta definición es el desequilibrio de poder entre el agresor y la víctima, que el daño se repita durante un largo tiempo, la nota de la intencionalidad por parte del agresor y los efectos de estas conductas sobre las personas involucradas.

En la actualidad, el problema del bullying trasciende los entornos tradicionales y requiere considerar también el cyberbullying, según Patchin e Hinduja se define como "daño intencional y repetido infligido a través del medio del texto electrónico". Smith lo define como "una acción agresiva e intencional, desarrollada por un grupo o un individuo, usando formas electrónicas de contacto, repetidas veces a lo largo del tiempo contra una víctima que no puede defenderse fácilmente".

El cyberbullying se sigue definiendo por acciones destinadas a atormentar, intimidar, degradar o acosar, pero el lugar donde se desarrollan estas actitudes ya no son espacios únicamente físicos, si no que se traslada al ciberespacio. Según la mayoría de los expertos que han estudiado este fenómeno, esto también implica cambios en los perpetradores, causas y las consecuencias de este tipo de acoso.[36]

La ausencia de una regulación específica sobre el cyberbullying en el Código Penal no impide sancionar muchos de los ataques que los menores pueden sufrir en el ciberespacio. De manera lógica, la jurisprudencia ha adaptado diversas conductas, que podríamos llamar "acoso a menores en línea", a diferentes tipos penales. Esto se ha logrado, como era de esperar, basándose en los distintos bienes jurídicos de los menores que son dañados o

[36] LLINARES, F. M. "Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio. *IDP: revista de Internet, derecho y política" = revista d'Internet, dret i política*, 2013. Pp 63-64.

puestos en riesgo por los ciberataques. La gravedad de la sanción penal se determinará según el impacto en los diferentes intereses protegidos del menor.

En su mayoría, los tribunales recurren a los delitos contra la integridad moral para sancionar estos cibercrímenes sociales, siguiendo el mismo criterio que se aplica al bullying tradicional. La integridad moral, como bien jurídico, se ve afectada cuando el acoso es continuo o permanente, lo que lleva a la aplicación del artículo 173 del Código Penal. Así lo establece claramente la Sentencia de la Audiencia Provincial de Ávila 146/2008, de 20 de octubre[37], que además señala que el tipo básico de estos delitos se aplicará junto con los tipos penales correspondientes de lesiones, amenazas o coacciones, incluyendo las infracciones previstas en los artículos 617 y 620 del Código Penal (vigentes a fecha de publicación de esa sentencia). Así, publicar fotos comprometedoras de una menor en un sitio web, permitiendo que los visitantes las valoren y comenten, y difundirlas entre compañeros de escuela, causando humillación, ha llevado a la aplicación del artículo 173 del Código Penal.

La SAP de Valencia n.º 488/2009, de 10 de septiembre, aborda un caso de sexting en el que la víctima permitió que un amigo grabara un vídeo, el cual luego fue difundido en Internet con la intención de humillarla. La resolución establece que, para aplicar el delito del artículo 173.1 del Código Penal, no es necesario que haya múltiples actos o una continuidad en el tiempo; una sola acción con suficiente gravedad y con intención de humillar es suficiente. En este caso, aunque la acción fue única, la difusión progresiva del vídeo y el sufrimiento de la víctima justifican la aplicación del artículo 173.1 CP.

La SAP de Cádiz n.º 23/2011, de 26 de enero[38], trata sobre un menor que obligó a otro menor con discapacidad psíquica a correr cuesta arriba con los cordones de las zapatillas atados, grabándolo y subiendo el vídeo a YouTube. La resolución menciona la jurisprudencia del Tribunal Supremo, que establece que las conductas no graves requieren repetición para ser sancionadas. Además, señala que para que una conducta sea punible, debe ser habitual o representar un riesgo para la integridad moral de la víctima.

[37] SAP de Ávila de 20 de octubre de 2008 (ECLI:APAV:2008:297)

[38] SAP de Cadiz de 26 de enero de 2011 (ECLI:ES:APCA:2011:1884)

Las resoluciones mencionadas sugieren una interpretación acertada sobre la gravedad de ciertos ataques en el ciberespacio respecto a la dignidad. Como he indicado antes, la naturaleza del ciberespacio permite que acciones que en el mundo físico son instantáneas y efímeras, permanezcan en internet indefinidamente, afectando la dignidad de manera continua.

Los tribunales han señalado que los delitos contra la integridad moral no requieren habitualidad, sino un menoscabo de la dignidad. Por ello, la difusión de imágenes o textos degradantes en el ciberespacio puede tener un impacto lesivo mayor que en el espacio físico. Sin embargo, no toda comunicación irónica en Internet será delictiva; debe tener suficiente entidad para considerarse una lesión a la integridad moral de la víctima. Muchas resoluciones no consideran el acoso continuado a menores en Internet como delito del art. 173 CP, sino como un delito leve de vejaciones.

No es la integridad moral el único bien jurídico afectado por el cyberbullying. Las amenazas y coacciones a través de internet pueden ocasionar un perjuicio a la libertad, siendo la acción de amenazas la más común en el ciberespacio, aunque este ejercicio es más común entre adultos también observamos casos de acoso a menores para obtener imágenes sexuales, lo que puede constituir delitos sexuales o amenazas.

La SAP de Tenerife n.º 541/2005, de 5 de mayo[39], consideró que un menor que realizó repetidas llamadas amenazantes a la víctima cometió un delito de amenazas. De manera similar, la SAP de Castellón n.º 115/2011, de 12 de abril[40], responsabilizó a un menor por el mismo delito al enviar correos electrónicos intimidatorios. La SAP de La Rioja n.º 8/2006, de 17 de enero[41], encontró culpable a un menor de una antigua falta del art. 620.2 CP por enviar mensajes de texto insultantes y amenazantes.

Sin embargo, no todas estas conductas son siempre consideradas amenazas por los tribunales, a veces se califican como coacciones. Un caso relevante se recoge en la SAP de Barcelona n.º 381/2009, de 14 de abril[42], que condenó a un individuo por difusión de pornografía infantil y coacciones. Este

[39] SAP de Tenerife de 5 de mayo de 2005 (ECLI:ES:APGC:2005:1799A)

[40] SAP de Castellón de 12 de abril de 2011 (ECLI:ES:APCS:2011:442)
[41] SAP de La Rioja de 17 de enero de 2006 ECLI:ES:APLO:2006:9)
[42] SAP de Barcelona de 14 de abril de 2009 (ECLI:ES:APB:2009:3191)

sujeto, haciéndose pasar por un adolescente en Internet, consiguió fotos de una menor de 14 años desnuda y la amenazó con difundirlas si no enviaba más fotos de ella y de su hermana de 9 años. El TS, en la STS n.º 1107/2009, de 12 de noviembre[43], modificó parcialmente esta sentencia, sustituyendo la condena de coacciones por amenazas, argumentando que los hechos no cumplían con los elementos del delito de coacciones, pero sí con los del delito de amenazas condicionales. El tribunal explicó que, aunque ambos delitos protegen el mismo bien jurídico, la coacción requiere violencia y una mayor inmediación entre el coaccionante y el coaccionado.[44]

En resumen, aunque no haya una regulación específica para estos delitos en nuestro Código Penal, se aplicarán los tipos penales que protegen los intereses de los menores. A pesar de esto, existe el impulso de crear una clasificación específica, especialmente en casos dramáticos de suicidio relacionados con el cyberbullying, donde se debate esta necesidad. Sin embargo, el régimen actual ya ofrece una respuesta apropiada y proporcionada a estos delitos.

5 PARTICULARIDADES PROCESALES DE LOS CIBERDELITOS.

El tratamiento procesal de los ciberdelitos presenta peculiaridades debido a su impacto en intereses difusos. Estos delitos afectan a múltiples víctimas, a menudo ubicadas en diferentes localidades o, incluso, en distintos países. Como resultado, se plantea la necesidad de abordar cuestiones como la acumulación de delitos (según el Artículo 17 de la Ley de Enjuiciamiento Criminal) para aplicar agravantes genéricas o considerar el delito continuado (según el Artículo 74 del Código Penal). Además, se busca identificar agravantes específicas y comprender el modus operandi del delito.

Para investigar estos casos, se analiza la reiteración de ataques contra las mismas víctimas con un patrón similar, lo que permite confirmar la existencia de un grupo criminal. Sin embargo, la falta de información sobre el

[43] STS de 12 de noviembre de 2009 (ECLI:ES::TS:2009:6983)
[44] LLINARES, F. M. “Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio. *IDP: revista de Internet, derecho y política” = revista d'Internet, dret i política*, 2013. Pp 65-70

origen y la identidad de los autores anónimos dificulta la investigación. Por lo tanto, los investigadores se centran en rastrear y analizar las huellas digitales dejadas en los sistemas afectados.

La naturaleza técnica de los delitos informáticos dificulta la obtención de pruebas, lo que ralentiza los procesos judiciales. Las pruebas periciales, como capturas de pantalla, análisis de archivos y volcados de disco duro, son costosas y a menudo intrusivas. Esto puede desalentar a las víctimas a la hora de denunciar este tipo de delitos. Es importante destacar que la intervención del juez de instrucción como garante de derechos fundamentales es esencial en estos casos.[45]

Los ciberdelitos, cometidos por individuos que actúan desde el anonimato que ofrece el entorno digital, se caracterizan por su cobardía. Estos delincuentes se aprovechan de las vulnerabilidades de las víctimas a distancia y sin riesgos mayores. Las empresas de telecomunicaciones y los proveedores de servicios de internet (ISP) desempeñan un papel fundamental en la lucha contra estos delitos, colaborando con las autoridades judiciales para obtener pruebas. Las empresas que alojan contenidos en Internet tienen una responsabilidad pasiva y pueden ser sancionadas si no retiran el contenido ilícito de sus sitios web. Además, la naturaleza de los delitos informáticos en internet presenta características que aumentan su gravedad y complejidad.[46] En este contexto, la intervención del legislador se vuelve crucial para adaptar las leyes a la realidad creando agravantes genéricas y específicas.

En este contexto, la intervención del legislador se vuelve crucial para adaptar las leyes a la realidad, creando agravantes genéricas y específicas. La rápida adopción y el uso generalizado de ciertas innovaciones tecnológicas han impulsado la necesidad de reevaluar la protección de ciertos derechos fundamentales,[47] los cuales, sin embargo, mantienen su carácter prioritario y preexistente.

En conclusión, cabe destacar que en España aún persisten vacíos legales en la lucha contra la ciberdelincuencia, debido a la falta de

[45] VELASCO NÚÑEZ, E., DELITOS *TECNOLÓGICOS. Cuestiones penales y procesales*. Wolters Kluwer, España, S.A. 2021. pp. 30- 32.
[46] Difusión y alcance global, victimas múltiples y anonimato.
[47] La intimidad, la propia imagen, la libertad de expresión.

actualización de instrumentos normativos como el Convenio del Cibercrimen del Consejo de Europa y la Directiva 2013/40/UE.

Esta situación genera impunidad para los delincuentes y exige una actualización del Código Penal para incluir como delitos nuevas formas de comportamiento delictivo [48], y de las normas procesales para facilitar una investigación ágil y especializada.

5.1 INVESTIGACIÓN. MEDIDAS DE INVESTIGACIÓN DE LA LECrim

En la mayoría de los casos, la investigación comienza con una denuncia presentada por personas afectadas por actividades delictivas. También puede iniciarse mediante una solicitud policial al tribunal para que emita una orden para realizar determinadas investigaciones dirigida a los proveedores de servicios de Internet. Esta orden busca obtener información sobre los usuarios de direcciones IP y las conexiones realizadas desde esas direcciones, incluyendo sus titulares. A continuación, el tribunal inicia el procedimiento correspondiente y, en algunos casos, puede autorizar una diligencia de entrada y registro en el domicilio o sede del titular de la línea, o la intervención de líneas. Con esta diligencia, se accede a los archivos y al ordenador para obtener copias de la información relevante.

Dado el aumento exponencial de los delitos tecnológicos, se han establecido unidades especializadas de investigación en la Policía Nacional, la Guardia Civil y algunas Policías Autonómicas. Además, en 2011 se creó una Fiscalía especializada en delitos informáticos.

Según el artículo 299 de la Ley de Enjuiciamiento Criminal (LECr), la fase de investigación criminal comprende todas las acciones destinadas a preparar el juicio y a documentar la comisión de los delitos, incluyendo las circunstancias que puedan afectar a su calificación y la culpabilidad de los delincuentes. Además, se pueden adoptar medidas cautelares para asegurar la integridad personal de los implicados y las responsabilidades económicas correspondientes.

---

[48] VELASCO NÚÑEZ, E., DELITOS *TECNOLÓGICOS. Cuestiones penales y procesales*. Wolters Kluwer, España, S.A. 2021 pp. 32 - 35.

En un mundo tan avanzado tecnológicamente como el actual, es evidente que se requiere la asesoría de expertos para llevar a cabo investigaciones eficientes. Esto implica mayores costos y tiempo, pero es esencial para abordar la delincuencia informática y satisfacer las demandas de la sociedad.[49] También a nivel europeo nos encontramos con la Europol, EuroJust y Agencia Europea de Seguridad de las Redes y la Información. [50]

La Ley de enjuiciamiento Criminal ha tenido que actualizar su regulación para regular de forma expresa, entre otros medios, de prueba, la intervención de las comunicaciones.

En el ámbito del procedimiento abreviado, el art. 773.2 LECrim permite al Ministerio Fiscal practicar él mismo u ordena a la Policía Judicial practicar diligencias para averiguación de los hechos incluso antes de la apertura de las diligencias judiciales. Y, una vez iniciadas éstas, puede igualmente solicitar al Juzgado la práctica de diligencias.

El art. 777 LECrim regula, con carácter general la función de Juez instructor para recabar indicios probatorios, de modo que ordenará a la policía judicial o practicará por si mismo las diligencias necesarias encaminadas a determinar la naturaleza y circunstancias del hecho, y los participantes.

Estas obligaciones y competencias se regulan también en el Libro II de la LECrim, arts. 301 bis, 303, 336 …

Pero la LO 13/2015, de 5 de octubre, de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de los medios de investigación tecnológica, modificó el título VIII del Libro II para actualizar los medios de investigación de determinados delitos, especialmente los de terrorismo, tráfico de drogas y los cometidos por medios telemáticos. Este título VIII pasa a denominarse: De las medidas de investigación limitativas de los derechos reconocidos en el art. 18 de la Constitución (el derecho a la intimidad).

---

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

[50] MIRANDA, J. J. C. *Factor Humano: La Teoría de las Actividades Cotidianas en la Ciberseguridad*. (s.f). Pp. 25-26.

- ENTRADA Y REGISTRO EN LUGAR CERRADO: Se mantiene la necesidad de autorización judicial para la entrada y registro en lugar cerrado mediante auto motivado y a presencia del LAJ (Cap. I), salvo expresa autorización del titular. La Policía, igualmente, deberá dar inmediata cuenta de los efectos ocupados y, en su caso, las detenciones practicadas.
- REGISTRO DE LIBROS Y PAPELES: En el Cap. II se mantiene el registro de libros y papeles también con autorización judicial e intervención de perito si así fuera necesario.
- DETENCIÓN Y APERTURA DE LA CORRESPONDENCIA ESCRITA Y TELEGRÁFICA: El Cap. III desarrolla la autorización judicial para la intervención de correspondencia escrita y telegráfica (Observación de las comunicaciones postales y telegráficas incluidos faxes, burofaxes y giros). Como particularidad de esta regulación, expresamente se permite utilizar el resultado de esta investigación en otro proceso penal (Art. 579 bis LECrim).

Como se puede comprobar, las nuevas formas de comisión de delitos demandaban la regulación de práctica de prueba acorde con los medios de comisión utilizados. Por eso se amplia en 2015 la regulación de la interceptación de comunicaciones.

- INVESTIGACIÓN TECNOLÓGICA: El Cap IV regula la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos, arts. 588 bis a a k.

La adopción de estas medidas requiere autorización judicial, mediante auto, con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

La medida se puede adoptar de oficio, a instancia del Ministerio Fiscal o de la Policía Judicial, y la petición debe contener (Art. 588 bis b LECrim):

1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.

3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.

4.º La extensión de la medida con especificación de su contenido.

5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

6.º La forma de ejecución de la medida.

7.º La duración de la medida que se solicita.

8.º El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

El auto que, en su caso, lo autorice, debe emitirse en un plazo máximo de 24 horas y concretará los siguientes extremos (Art. 588 bis c LECrim):

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.

d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.

e) La duración de la medida.

f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

g) La finalidad perseguida con la medida.

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

Los resultados de esta investigación podrán ser utilizados como medio de investigación o prueba en otros procedimientos con las reglas establecidas en el art. 579 bis (Art. 588 bis i LECrim).

- INTERCEPTACIÓN DE LAS COMUNUCACIONES TELEFÓNICAS Y TELEMÁTICAS: El Cap. V regula la interceptación de las comunicaciones telefónicas y telemáticas. Esta medida de investigación solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

El objeto de la investigación se ceñirá a:

1. Los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado.

2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario.

También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.

A los efectos previstos en este artículo 588 ter b LECrim, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así

como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga.

La solicitud de la autorización debe contener, además de los requisitos mencionados en el artículo 588 bis b, los siguientes:

a) la identificación del número de abonado, del terminal o de la etiqueta técnica,

b) la identificación de la conexión objeto de la intervención o

c) los datos necesarios para identificar el medio de telecomunicación de que se trate.

Para determinar la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos:

a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.

b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.

c) La localización geográfica del origen o destino de la comunicación.

d) El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos.

Y finalmente, en caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

En el art. 588 ter e establece el deber de colaboración y de guardar secreto de todos los prestadores de servicios de telecomunicaciones, de

acceso a la red de telecomunicaciones o de servicios de la sociedad de información así como, en general, de todas las personas que contribuyan a facilitar las comunicaciones.

Este Cap. V desarrolla también otros medios de prueba como:

La incorporación al proceso de datos electrónicos de tráfico y asociados (Art. 588 ter j LECrim): “1.- Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial.

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión”.

El acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad (Art. 588 ter k a m) con menores exigencias formales para recabar la información:

Identificación mediante número IP: Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso

Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes:

1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior.

El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.

Identificación de titulares o terminales o dispositivos de conectividad: Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia

- CAPTACIÓN Y GRABACIÓN DE COMUNUCACIONES ORALES MEDIANTE DISPOSITIVOS ELECTRÓNICOS: El Cap VI regula la identificación de titulares o terminales o dispositivos de conectividad que también exige un auto fundamentado para permitir la medida.
- CAPTACIÓN DE IMAGEN, SE SEGUIMIENTO Y DE LOCALIZACIÓN: El Cap. VII desarrolla la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización

- REGISTRO DE DISPOSITIVOS DE ALAMACENAMIENTO MASIVO DE INFORMACIÓN: El Cap VIII se refiere al registro de dispositivos de almacenamiento masivo de información. El art. 588 sexies a establece limitaciones al acceso de información contenido en los ordenadores o teléfonos incautados en la siguiente forma: “1.- Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente”.

La autorización judicial para el acceso a la información contenida en estos dispositivos fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos, así como las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.

- REGISTROS REMOTOS SOBRE EQUIPOS INFORMÁTICOS: Se recoge en el Cap. IX y es la variante modernizada de la intervención telefónica aplicada a los medios telemáticos. Se establece un deber de colaboración de los prestadores de servicios y podrá ser autorizada por el Juez (Art. 588 septies a LECrim) para la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema

informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que se investiguen, entre otros delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

5.2 COOPERACION JUDICIAL EN CIBERDELIENCUENCIA INTERNACIONAL.

En el contexto de las redes informáticas, la *supraterritorialidad* se refiere a una característica fundamental. A diferencia del mundo físico, donde los delitos ocurren en lugares específicos del territorio, en el espacio digital, el concepto de territorio no es tan relevante. En lugar de ubicaciones geográficas, lo que importa en la Red son los nodos, como terminales, servidores, proveedores y conexiones.

Estos elementos permiten la circulación de información a nivel global, sin estar limitados por fronteras físicas. Sin embargo, establecer conexiones claras entre la Red y el mundo físico puede ser complicado.[51]

Para abordar estos problemas a nivel internacional, se diseñan estrategias globales de solución, como la creación de un Tribunal Penal Internacional en materia de ciberdelincuencia. Sin embargo, esta solución plantea desafíos técnicos debido a la tipificación armonizada de conductas, la definición de competencias, el volumen de trabajo y la eficacia de una jurisdicción universal.

En lugar de crear un nuevo Tribunal, podría considerarse atribuir a la Corte Penal Internacional la responsabilidad de juzgar los delitos más graves relacionados con Internet, como la protección de la propiedad intelectual, la lucha contra la pornografía infantil y los fraudes económicos internacionales en línea.

Esta estrategia selectiva, junto con una cooperación policial y judicial avanzada, permitiría una convergencia entre las jurisdicciones nacionales y la jurisdicción internacional, adaptándose mejor a la gravedad de los delitos y la extensión territorial de las conductas.[52]

En segundo lugar, en el contexto de un movimiento a favor de los Métodos Alternativos de Resolución de Conflictos (ADR), se promueve con fuerza enfoques alternativos a la jurisdicción para resolver conflictos relacionados con el uso de sistemas informáticos.

Estos métodos incluyen el arbitraje, la mediación y la conciliación. Dada su eficiencia, bajo costo y la especialización de los árbitros, se espera que desempeñen un papel crucial en la resolución de disputa legales, especialmente en casos trasnacionales. No obstante, estos medios de solución de conflicto tienen poca o nula aplicación en el ámbito penal.

---

[51] PRADA, I. F. “Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia”. *Revista Electrónica de Ciencia Penal y Criminología*, *17*, 21. 2015. Pp. 21-23. Pp.7.

[52] PRADA, I. F. “Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia”. *Revista Electrónica de Ciencia Penal y Criminología*, *17*, 21. 2015. Pp. 21-23. Pp. 19-20

Aunque las normas internacionales actualmente favorecen al consenso entre los Estados con jurisdicciones concurrentes en la persecución de ciberdelitos, no debemos descartar la posibilidad de avanzar en el futuro mediante la mediación. Este enfoque, sin poner soluciones, podría añadir elementos de eficacia al consenso espontaneo, facilitando la búsqueda de una solución adecuada al conflicto jurisdiccional.

En el panorama actual, la cibercriminalidad emerge como una amenaza global que exige estrategias coordinadas para su efectiva resolución. En este contexto, la cooperación internacional se erige como piedra angular para abordar los conflictos de jurisdicción que surgen en este ámbito.

La visión fragmentada y nacionalista sobre la cibercriminalidad resulta insuficiente para combatirla. Se requiere un enfoque integral y global que reconozca la naturaleza transfronteriza de este fenómeno. La cooperación internacional surge como herramienta indispensable para armonizar los sistemas penales, eliminando zonas de impunidad y unificando la tipificación de delitos.

A través de la cooperación internacional se puede lograr una persecución y castigo eficaces de los ciberdelincuentes, mediante la coordinación de las actividades judiciales y policiales. La colaboración entre naciones permite compartir información crucial, obtener pruebas y llevar a cabo detenciones, fortaleciendo la lucha contra el cibercrimen.

Si bien la cooperación internacional ha avanzado en materia de asistencia judicial y policial, aún quedan pendientes desafíos en la búsqueda de soluciones procesales que eviten procedimientos penales paralelos. Estos procedimientos duplicados no solo son ineficaces, sino que también pueden afectar el principio *non bis in ídem*, un derecho fundamental que protege a las personas de ser condenadas dos veces por el mismo delito.

Para superar estos retos, la comunidad internacional debe avanzar en la búsqueda de mecanismos que fortalezcan la cooperación judicial. Esto implica establecer fórmulas y criterios claros para seleccionar la jurisdicción penal

idónea en casos de litispendencia internacional, así como promover acuerdos de reconocimiento mutuo de resoluciones judiciales.[53]

En resumen, se propone establecer dos medidas para mejorar la cooperación internacional en la persecución de la ciberdelincuencia. Primero, definir criterios para determinar que jurisdicción penal nacional tiene competencia preferente en casos de cibercriminalidad. Segundo, crear un procedimiento simplificado para resolver conflictos de competencia entre jurisdicciones en casos de litispendencia internacional penal relacionados con ciberdelitos.

5.3 PECULIARIDADES EN LA DENUNCIA DE LOS DELITOS INFORMÁTICOS.

Es crucial empezar señalando que la ciberdelincuencia suele tener un alto índice de impunidad. La falta de coordinación internacional entre las autoridades dificulta la investigación y denuncia de ciberdelitos. A menudo, estos pasan desapercibidos debido a la falta de confianza en la policía, desconocimiento de los mecanismos de denuncia, vergüenza y preocupaciones comerciales por desprestigio entre otras.[54]

Existen diversas políticas públicas recomendables para abordar el problema de la desinformación. Algunas de estas políticas incluyen campañas de información, sistemas en línea para presentar denuncias, estrategias de cooperación con el sector privado y mejoras en los sistemas de intercambio de información policial.

Aunque aún no se han evaluado completamente los efectos de estas medidas, en casos que afectan a intereses corporativos, se observa cierta resistencia debido a la posible pérdida de reputación. Esto lleva la implementación de sistemas preventivos y reactivos dentro de las

[53] PRADA, I. F. “Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia”. *Revista Electrónica de Ciencia Penal y Criminología*, *17*, 21. 2015. Pp. 21-23

[54] TÁVORA SERRA, M. J. *Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje*. 2022. Pp 55-57. Pp 55

organizaciones, especialmente en empresas con presencia internacional.[55] Sin embargo, la falta de disposición en el sector privado para reportar los delitos cibernéticos preocupa a las autoridades por ciertas razones. Una de ellas es que, si las empresas no denuncian estos delitos, el delincuente podría volver a atacar a la empresa o usar las mismas técnicas para afectar a otras.[56]

Otro motivo de la gran impunidad a la que nos enfrentamos con este tipo de delitos es la dificultad para obtener pruebas. Esto no solo se debe a la volatilidad de los datos informáticos, sino también a los intereses de otros Estados cuando las pruebas están en su territorio.

Además, la existencia de redes como "*TOR"* o "*Freenet"*, junto con la creciente complejidad de las organizaciones de ciberdelincuencia, dificulta aún más la obtención de resultados. La formación técnica también es crucial para los investigadores en este campo.

Ciertamente, la colaboración entre entidades públicas y privadas, tanto a nivel nacional como internacional se ha postulado como una respuesta esencial ante la creciente globalización de la ciberdelincuencia.

Existen otros factores que contribuyen al alto nivel de impunidad. Por ejemplo, la automatización de las acciones informáticas necesarias para cometer un delito que permite que este se perpetre incluso cuando el autor está lejos. Además, las aplicaciones informáticas puedes reconfigurarse automáticamente para ocultar cualquier rastro, unido a la existencia de diversos sistemas para ocultar la identidad del perpetrador, como el uso de servidores que enmascaran la dirección final de la conexión, complica aún más la obtención de pruebas.[57]

Teniendo esta información en cuenta es relevante destacar que la investigación preparatoria comienza con la *notitia criminis*, la información que se divulga sobre un hecho delictuoso. Es crucial recopilar cuidadosamente la información que se proporciona, dado que quien informa o denuncia es

[55] VELASCO NÚÑEZ, E., "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley*, 8183, 2013, Wolters Kluwer. Pp. 17

[56] VERA, M. D. B. "El Ciberdelito, desafíos para la ley penal y civil. Marco jurídico nacional y comparado". *Revista Jurídica*, *7*(1). 2023. Pp. 182

[57] TÁVORA SERRA, M. J. *Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje*. 2022. Pp 55-57.

portador de diversos datos, el receptor de la denuncia, generalmente los agentes de policía, intentarán recopilar la mayor cantidad posible de detalles: las circunstancias del hecho, las características de los involucrados, los instrumentos utilizados, etc.

En resumen, la *notitia crimis* es fundamental para la investigación cuyo éxito depende de estos elementos en un relato coherente.[58]

En consecuencia, podemos concluir que resulta sumamente complicado alcanzar un desenlace justo en casos de delitos tecnológicos. Desde el momento inicial de la denuncia, nos enfrentamos a múltiples obstáculos; la dificultad para identificar al autor y su ubicación, su habilidad para desaparecer sin dejar rastro y el uso de medios sofisticados. Además, no debemos pasar por alto la incomodidad que sienten las víctimas al denunciar o el daño reputacional que puede sufrir una empresa.

Adicionalmente, la necesidad de recabar suficientes datos para iniciar una fase de investigación por parte de la Policía Nacional o la Guardia Civil agrega el desafío de la obtención de pruebas sólidas y la identificación de patrones en el ciberespacio. Así, enfrentamos un panorama complejo en la lucha contra la ciberdelincuencia.

5.4 FASE DE INSTRUCCIÓN Y PRÁCTICA DE LA PRUEBA.

Antes de la reforma de 2015 (desarrollada en el apartado Investigación, al que nos remitimos), la Ley de Enjuiciamiento Criminal no abordaba técnicas específicas para la Investigación Tecnológica. Para suplir esta carencia, se aplicaban disposiciones generales de la ley procesal, como el artículo 282, mediante analogía con las intervenciones telefónicas, registros y otros procedimientos. La jurisprudencia también había ampliado la interpretación del artículo 579 de la Ley de Enjuiciamiento Criminal para incluir tecnologías modernas, como la colocación de micrófonos o la introducción de troyanos en ordenadores. Sin embargo, dos eventos clave impulsaron la reforma:

[58] HURTADO, M. P. R. “El Proceso Común, Vía Emblemática del Código Procesal Penal del 2004 (CPP) y su Primera Etapa: la Investigación Preparatoria”. *Foro jurídico*, (12), 231-239. 2013. Pp. 235-237.

En primer lugar, la sentencia del Tribunal de Justicia de la Unión Europea (STJUE) del 8 de abril de 2014 anuló la Directiva 2006/24/CE del Parlamento Europeo y del Consejo. Esta directiva se centraba en la retención de datos generados o procesados en relación con servicios de comunicaciones electrónicas y redes públicas. La decisión del STJUE podría tener implicaciones para la legislación española sobre la conservación de datos.

En segundo lugar, la STC 145/2014, emitida por el Tribunal Constitucional, determinó que la interceptación de conversaciones de un detenido en su celda vulneraba el derecho fundamental al secreto de la comunicación. Aunque se contara con una autorización judicial motivada, la falta de una normativa específica para esta práctica generó la necesidad de una reforma legal.

En octubre de 2015, la Ley de Enjuiciamiento Criminal se reformó para abordar la posibilidad de aplicar las nuevas tecnologías en la investigación de delitos, no solo los cometidos por estos medios sino también los de terrorismo y tráfico de drogas, entre otros. Se regularon técnicas específicas de Investigación Tecnológica, que podían justificar la limitación de los derechos reconocidos en el artículo 18 de la Constitución. Estas medidas incluyen:

- Se permite la interceptación de comunicaciones telefónicas y telemáticas como parte de investigaciones criminales relacionadas con delitos en línea (artículo 588 ter y siguientes).
- Se autoriza la grabación de conversaciones orales mediante dispositivos electrónicos (artículo 588 quarter a y siguientes).
- Se puede identificar a través de direcciones IP y códigos de identificación de dispositivos (artículo 588 ter k y 588 ter 1).
- Se permite el uso de tecnologías para rastrear, localizar y capturar imágenes (artículo 588 quinquies a y siguientes).
- Se establece la posibilidad de registrar dispositivos de almacenamiento masivo (artículo 588 sexies a y ss).

Además, se contempla la actuación bajo identidad supuesta en canales cerrados de comunicación telemática, siempre con autorización judicial para proteger la intimidad y el secreto de las comunicaciones (artículo 282 bis apartados 6 y 7).

Es importante destacar que estas medidas no solo se aplican a la investigación de ciberdelitos, sino que también pueden ser útiles en la prevención y persecución de otras infracciones tradicionales.[59]

El Ministerio Fiscal en España desempeña un papel fundamental en la fase de investigación de los delitos, especialmente en el contexto de la creciente criminalidad informática. Aunque no existen órganos judiciales especializados específicamente en ciberdelitos, la Fiscalía ha tomado medidas significativas para abordar este desafío.

La Instrucción 2/2011 de la Fiscalía General del Estado establece un catálogo inicial de delitos relacionados con la criminalidad informática. Estos delitos abarcan una amplia gama de actividades ilícitas que involucran el uso indebido de las nuevas tecnologías, especialmente internet. La generalización de estas herramientas en el desarrollo de las relaciones económicas y sociales ha dado lugar a nuevas formas de delincuencia, así como a dinámicas y mecanismos previamente desconocidos.

Para abordar esta problemática, se ha creado una figura especializada, el Fiscal de Sala de Criminalidad Informática. Este Fiscal tiene competencia en todo el territorio del Estado y se encarga de coordinar y supervisar las investigaciones relacionadas con la criminalidad informática. Sus funciones incluyen:

- Llevar a cabo las diligencias necesarias para investigar los delitos informáticos. Esto implica recopilar pruebas, entrevistar a testigos y analizar la información relevante.
- Cuando un caso tiene una relevancia excepcional, el Fiscal de sala interviene directamente o emite instrucciones a otros Fiscales para garantizar una investigación adecuada. Esto puede incluir delitos graves o aquellos que afectan a un gran número de personas.
- Coordina la actividad de las secciones de criminalidad informática en las fiscalías locales. Esto implica establecer criterios de actuación,

[59] QUEVEDO GONZÁLEZ, J. *Investigación y prueba del ciberdelito*. Sepin. Madrid, España. 2017.

proponer instrucciones y asegurar que las investigaciones se realicen de manera coherente en todo el país.

- Solicita informes a las secciones de criminalidad informática, lo que permite mantenerse al tanto de los avances en las investigaciones y tomar decisiones informadas.
- Anualmente, presenta un informe al Fiscal General del Estado sobre los procedimientos seguidos y las actuaciones practicadas en materia de criminalidad informática. Este informe se incorpora a la memoria anual presentada por el Fiscal General.

En resumen, la figura del Fiscal de Sala de criminalidad informática despliega una labor esencial para combatir los delitos informáticos en España. Su especialización y coordinación contribuyen a proteger a la sociedad en un entorno digital cada vez más complejo.[60]

5.5 FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO Y SU ACTUACIÓN FRENETE A LOS CIBERDELITOS.

5.5.1 LA GUARDIA CIVIL

La Guardia Civil ha establecido unidades especializadas para combatir la delincuencia informática y los delitos cibernéticos. Estas unidades están compuestas por agentes capacitados en ciberseguridad y se dedican a asesorar prevenir y responder a los crímenes que provienen de la Red.

La Guardia Civil cuenta con un equipo especializado en la lucha contra los delitos que se producen en el ámbito digital. Este grupo, conocido actualmente como Grupo de Delitos Telemáticos (GDT), ha experimentado una evolución en su denominación a lo largo del tiempo, reflejando así el cambiante panorama de las ciberamenzas.

En sus inicios, en 1996, se denominaba Grupo de Delitos Informáticos, una época en la que las denuncias por este tipo de delitos aún eran escasas. En 1998, la unidad adoptó la denominación de Departamento de Delitos en Altas Tecnologías, coincidiendo con el auge de los fraudes en el

[60] QUEVEDO GONZÁLEZ, J. *Investigación y prueba del ciberdelito*. Sepin. Madrid, España. (2017) Pp 112- 114.

ámbito de las telecomunicaciones. Este cambio de nombre reflejaba la necesidad de ampliar el enfoque de la unidad para abarcar los nuevos desafíos que presentaba la era digital. Dos años después, en 2000, se volvió a modificar la denominación, pasando a ser Departamento de Delitos Telemáticos. Finalmente, en 2003, adoptó la denominación actual que conocemos Grupo de Delitos Tecnológicos.

La principal función de estos Grupos es investigar todos los delitos que puedan ser cometidos a través de las redes informáticas, es decir, mediante Internet. Además, brindan apoyo a los demás Grupos y Departamentos que conforman la Unidad Central Operativa.

El Grupo de Delitos Tecnológicos (GDT) colabora estrechamente con diversas organizaciones e instituciones que tienen competencias en el ámbito de las Nuevas Tecnologías. Esta cooperación facilita investigaciones más efectivas y ágiles. El trabajo conjunto implica compartir información y experiencias, así como promover la participación en encuentros entre unidades policiales. Esto contribuye a armonizar los procedimientos de investigación y la forma de actuación basada en protocolos establecidos.

Además de su labor a nivel nacional, el GDT también trabaja a nivel internacional. La delincuencia informática no conoce fronteras y requiere una colaboración más amplia para combatir este tipo de delitos. Actualmente, el GDT participa en organismos e instituciones como el Foro Internacional del G-8 centrado en el cibercrimen, los Grupos de Trabajo de Interpol, Europol y Latinoamérica.

La GDT (Grupo de Delitos Telemáticos) lleva a cabo diversas acciones, entre las que destacan su papel como Policía Judicial. En esta función, investiga los delitos cometidos a través de medios tecnológicos y brinda apoyo técnico especializado a los grupos de la Unidad Central Operativa y las unidades de la Guardia Civil. Además, colabora con las autoridades judiciales.

La GDT también realiza tareas de policía administrativa, asegurándose de que se aplique correctamente la normativa relacionada con internet. Esto incluye la tramitación de denuncias y expedientes administrativos, así como el bloqueo de cuentas y perfiles en redes sociales o la eliminación de contenido ilícito en internet.

En cuanto al ámbito de atención al ciudadano, la GDT gestiona diversos canales de colaboración ciudadana a través de medios telemáticos y proporciona información relevante mediante alertas y noticias.

En materia de ciberseguridad, la GDT maneja incidentes que puedan surgir en internet. Además, participa activamente en foros de seguridad, colaborando con diversos organismos para lograr una respuesta más efectiva en este ámbito.

Representando al cuerpo de la Guardia Civil, la GDT asiste a foros internacionales centrados en la colaboración en cibercrimen y ciberseguridad. También planifica y lleva a cabo cursos de formación para su propio personal, la Administración de Justicia y otros organismos relacionados con la ciberseguridad.[61]

5.5.2 CUERPO NACIONAL DE POLICIA

Otro Cuerpo de Seguridad encargado de la investigación de este tipo de delitos es el Cuerpo Nacional de Policía, será la Unidad de Investigación Tecnología de la Comisaria General de Policía Judicial (C.G.P.J) la que investigue y persiga los delitos cibernéticos a nivel tanto nacional como internacional.

Su misión se basa en obtener las pruebas pertinentes y perseguir a los ciberdelincuentes para lograr llevarlos ante la justicia. Además, actúa como centro de prevención y respuesta ante el cibercrimen, abordando temas como la pornografía infantil, fraudes en línea y ataques cibernéticos entre otros.

Dentro de la Unidad de Investigación Tecnológica de la C.G.P.J, destaca la Brigada de Investigación Tecnológica (BCIT). [62]

La BCIT se encarga de llevar a cabo investigaciones que requieren un alto nivel de especialización y conocimiento técnico. Esto puede incluir delitos cibernéticos sofisticados, ataques informáticos avanzados y otros casos complejos.

---

[61] MIRANDA, J. J. C. *Factor Humano: La Teoría de las Actividades Cotidianas en la Ciberseguridad*. (s.f). Pp 28-31.
[62] MIRANDA, J. J. C. *Factor Humano: La Teoría de las Actividades Cotidianas en la Ciberseguridad*. (s.f).Pp 32.

La BCIT trabaja en estrecha colaboración con otras unidades y jefaturas superiores para coordinar operaciones relacionadas con el cibercrimen. Esto puede implicar la colaboración con diferentes departamentos y agencias para abordar casos específicos.

También se dedica a la formación y capacitación en temas relacionados con la ciberseguridad y la investigación tecnológica. Esto incluye proporcionar conocimientos y habilidades a los agentes de policía para enfrentar los desafíos del mundo digital. Además, participa en investigaciones que tienen un alcance internacional. Esto puede implicar colaborar con agencias de otros países, compartir información y coordinar esfuerzo para resolver casos que trascienden las fronteras nacionales.[63]

5.6 ÓRGANOS ENCARGADOS DE LA INVESTIGACIÓN DE LOS CIBERDELITOS EN EL AMBITO EUROPEO.

5.6.1.1 EUROPOL EC3

En el ámbito europeo, la Agencia de la Unión Europea para la Ciberseguridad (European Cybercrime Centre o EC3) se erige como un organismo crucial en la batalla contra el cibercrimen. Integrado en la estructura de Europol y con sede en La Haya (Países Bajos), el EC3 fue establecido en el año 2013 con el propósito de reforzar la capacidad de las fuerzas policiales europeas para combatir este tipo de delitos. Su misión principal reside en la protección de empresas, gobiernos y ciudadanos frente a las amenazas y ataques perpetrados por ciberdelincuentes.

Una contribución significativa al campo de la ciberseguridad por parte de este grupo de operaciones se refleja en el IOCTA (Internet Organised Crime Threat Assessment), un informe estratégico anual sobre las amenazas del crimen organizado en línea.

Este análisis nos proporciona información sobre los descubrimientos realizados, las amenazas y el desarrollo de la ciberdelincuencia que afecta a

[63] *Policía Nacional. (s. f.). Brigada Central de Investigación Tecnológica (B.C.I.T).* [en línea] < *https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php*> [Consulta: 29 mayo 2024].

ciudadanos, gobiernos y empresas, así como sugerencias y pautas claves para las fuerzas de seguridad. [64]

El Centro Europeo de Delitos Financieros y Económicos (EFECC) en Europol se estableció en junio de 2020 para abordar las crecientes amenazas a la economía y la integridad de los sistemas financieros. Estas amenazas incluyen el lavado de dinero, la corrupción, la falsificación generalizada, el fraude y los esquemas de evasión fiscal que afectan a individuos, países y empresas. El EFECC brinda apoyo operativo y estratégico a los Estados miembros de la UE y otras entidades, promoviendo el uso coherente de investigaciones financieras y la incautación de activos. Sus objetivos clave son proporcionar apoyo directo en investigaciones de delitos financieros y económicos, rastrear y confiscar activos criminales, y colaborar con partes interesadas públicas y privadas. [65]

5.6.1.2 EUROJUST

El ámbito de competencia de Eurojust se define en relación con el de Europol y se extiende a las infracciones cometidas en conexión con los tipos de delincuencia y las infracciones que abarca el mismo (según el artículo 4.1 de la Decisión Eurojust). Esto no es una novedad en el ámbito jurídico, ya que muchos instrumentos legales hacen referencia al ámbito de competencia de Europol.

Además, Eurojust solo puede colaborar en investigaciones y actuaciones judiciales a solicitud de la autoridad competente de un Estado miembro (según el artículo 4.2 de la Decisión Eurojust).

En cualquier caso, Eurojust no tiene la capacidad de intervenir en cualquier conducta delictiva dentro del ámbito señalado, sino que se limita a investigaciones y actuaciones en casos transnacionales que afecten a dos o

---

[64] MIRANDA, J. J. C. *Factor Humano: La Teoría de las Actividades Cotidianas en la Ciberseguridad*. (s.f).Pp 27.

[65] Europol. *European Financial and Economic Crime Centre (EFECC)* [en línea]. Unión Europea. (2020) < https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc>. [fecha de consulta: 24 junio 2024]

más Estados miembros de la Unión Europea o, de manera excepcional, a un único Estado miembro y a un tercer Estado o a la propia Unión Europea. [66]

5.6.1.3 AGENCIAS

La Agencia Europea de Seguridad de las Redes y la Información (ENISA) tiene como objetivo principal ayudar a la comunidad a alcanzar niveles especialmente altos de seguridad en las redes y la información. Para lograrlo, la Agencia contribuye al desarrollo de una cultura de seguridad en beneficio de ciudadanos, consumidores, empresas y organizaciones del sector público de la Unión Europea. Además, ENISA presta asistencia a la Comisión, los Estados miembros y la comunidad empresarial para cumplir con los requisitos de seguridad de las redes y la información, incluyendo la legislación actual y futura. Funciona como un centro de asesoramiento técnico y se dedica a tareas como el análisis de datos relacionados con la seguridad y los riesgos emergentes, la cooperación con actores públicos y privados, la sensibilización sobre seguridad cibernética y la promoción de mejores prácticas en la gestión de riesgos. También supervisa el desarrollo de normas para productos y servicios en la sociedad de la información y las redes.[67]

6 CONCLUSIONES

En la actualidad, la constante evolución de los delitos cibernéticos plantea desafíos significativos para la sociedad y el sistema legal, pues la utilización de estos medios para cometer infracciones se ha convertido en la acción dolosa más habitual. Es fundamental que nos adaptemos a estos cambios y estemos preparados para abordarlos de manera efectiva.

Desde mi perspectiva, se están tomando medidas adecuadas para enfrentar esta problemática. Sin embargo, la cooperación internacional es esencial en este ámbito. La dificultad para identificar a los autores de estos

[66] MOREDA, N. A. “Eurojust, a la vanguardia de la cooperación judicial en materia penal en la Unión Europea”. *Revista de Derecho Comunitario Europeo*, *16*(41), 119-157. 2012.
[67] JIMÉNEZ, C. C. La Agencia Europea de Seguridad de las Redes y de la Información. *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, (1), 195-209. 2005.

delitos radica en el ciberespacio, donde las fronteras son difusas y las jurisdicciones se superponen. Por lo tanto, una investigación sólida y colaborativa es crucial para abordar estos problemas de manera eficiente.

La denuncia también juega un papel clave en la lucha contra los delitos cibernéticos. A menudo, las víctimas no denuncian por vergüenza (en el caso de particulares) o por temor a dañar el prestigio de sus empresas. Es importante fomentar una cultura de denuncia y concienciar sobre la importancia de reportar estos incidentes para que las autoridades puedan actuar.

Además, las campañas de prevención son necesarias. Los padres deben estar alerta y utilizar herramientas de control parental para proteger a sus hijos.

En resumen, la lucha contra los delitos cibernéticos requiere una combinación de legislación efectiva, cooperación internacional, investigación sólida y concienciación continua. En concreto resultaría adecuado:

1.- Que la formación telemática que se ofrece desde temprana edad incida en la relevancia tanto de evitar medidas activas o pasivas de acoso como de fraudes o engaños.

2.- Que existan canales sencillos de denuncia de estas conductas. Quizás la carga inicial no solo debe recaer en la policía judicial, sino que también, las entidades privadas que más se sirven de internet para prestar sus servicios: entidades financieras, empresas proveedoras de servicios de energía, de teléfono …. deben mantener canales de rápido acceso para recibir las posibles alertas de fraude. Por supuesto, además de controlar de forma continua la existencia en las redes de páginas que intenten suplantarles.

Especialmente las entidades bancarias deben controlar de forma más rigurosa los movimientos de dinero sospechosos, pues es cada vez más habitual la estafa a particulares mediante suplantación de identidad y transferencias a través de una cuenta “puente” de otro particular que, en ocasiones, tampoco guarda relación con el autor del delito.

Igualmente, padres y centros escolares y Administración docente deben mantener la guardia alta para evitar conductas perniciosas entre los menores

3.- La policía judicial requiere formación permanente y actualizada para la investigación de estos delitos. A pesar de la existencia de unidades

específicas de investigación, debe generalizarse dicha formación para que, al momento de recibir la denuncia, se pueda instar al Juzgado la adopción de medidas para la identificación del autor y la recuperación, en la medida de lo posible, de lo sustraído.

4º.- Sin perjuicio del derecho a la intimidad del art. 18 de la Constitución Española, la investigación de estos delitos requiere la adopción por los Juzgados mediante resoluciones motivadas, de medidas urgentes y prácticas dirigidas no solo a identificar a los autores sino a poder suspender la conducta. En este sentido, asociado a los Juzgados de Guardia debe existir funcionarios con especiales conocimientos telemáticos que auxilien al Instructor en a la adopción de estas medidas.

5º.- Sin cooperación internacional la persecución de los delitos cibernéticos resulta imposible. Es indispensable no solo que la policía europea se coordine en la persecución de estos delitos. Las soluciones deben ser globales, la comunicación entre policía judicial inmediata, así como la ratificación por jueces nacionales de las medidas instadas por los de otros países.

7 BIBLIOGRAFÍA.

LIBROS

DE LA CUESTA ARZAMENDI, J. L., PÉREZ MACHÍO, A. I., & SAN JUAN, C. *Aproximaciones criminológicas a la realidad de los ciberdelitos.* Editorial Aranzadi, S.A.U. 2010.

MARTÍNEZ ATIENZA, G. *Ciberdelitos: Instrucción y prueba*. Ulzama Digital, España. 2016.

QUEVEDO GONZÁLEZ, J. *Investigación y prueba del ciberdelito*. Sepin. Madrid, España. 2017.

VELASCO NÚÑEZ, E., DELITOS *TECNOLÓGICOS. Cuestiones penales y procesales*. Wolters Kluwer, España, S.A. 2021

ARTÍCULOS DE REVISTAS

ALMIRÓN, F. R. “El delito de estafa informática.: ¿es posible determinar la responsabilidad civil de la entidad financiera en base al artículo 120?3 del código penal como consecuencia del «phishing»”. *Revista de Derecho Penal y Criminología*, *30*(JUNIO). 2023.

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

BETRÁN, Y. (2023). El secreto oficial en la legislación y la jurisprudencia española.: Análisis y crítica. *Derecom*, (34), 2023.

CASTILLO-PÉREZ, S., ANDRÉS, J. A. M., & GARCIA-ALFARO, J. El Spyware como amenaza contra navegadores web. (s.f).

CONDE, M., RODRIGUEZ, G., & ORTIZ, J. A. Soporte de red en rootkits de linux. (s.f).

GARCÍA GARCÍA, D. E. El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016). *Iuris Tantum Revista Boliviana de Derecho*, (25), 650-661, 2018.

HERNÁNDEZ, S. O. La regulación de los delitos con origen tecnológico. *Revista Aranzadi Doctrinal*, (9), 6, 2022.

HUERTA MIRANDA, M y LÍBANO MANZUR, C *Los Delitos Informáticos*, Editorial Jurídica Cono Sur. 2016.

HURTADO, M. P. R. “El Proceso Común, Vía Emblemática del Código Procesal Penal del 2004 (CPP) y su Primera Etapa: la Investigación Preparatoria”. *Foro jurídico*, (12), 231-239. 2013.

LLINARES, F. M. “Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio. *IDP: revista de Internet, derecho y política” = revista d'Internet, dret i política*, 2013.

JIMÉNEZ, C. C. La Agencia Europea de Seguridad de las Redes y de la Información. *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, (1), 195-209. 2005.

MIRANDA, J. J. C. *Factor Humano: La Teoría de las Actividades Cotidianas en la Ciberseguridad*. (s.f).

MIRÓ, F. “Delincuencia asociada al uso de las TIC”. [Recurso de aprendizaje textual]. *Fundación Universitat Oberta de Catalunya (FUOC)*, 2013.

MOREDA, N. A. “Eurojust, a la vanguardia de la cooperación judicial en materia penal en la Unión Europea”. *Revista de Derecho Comunitario Europeo*, *16*(41), 119-157. 2012.

PRADA, I. F. “Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia”. *Revista Electrónica de Ciencia Penal y Criminología*, *17*, 21. 2015.

RODRÍGUEZ-MAGARIÑOS, F. Nuevos delitos informáticos: phishing, pharming, hacking y cracking. *Práctica Penal*, *48*, 2009.

SANTOS, C. P., GUISADO, Á. C., & MORÁN, J. J. D. "El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito". *Revista policía y seguridad pública*. 2017.

TÁVORA SERRA, M. J. *Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje*. 2022.

VERA, M. D. B. "El Ciberdelito, desafíos para la ley penal y civil. Marco jurídico nacional y comparado". *Revista Jurídica*, *7*(1). 2023.

RECURSOS WEB

Instituto Nacional de Ciberseguridad (INCIBE) & Boletín Oficial del Estado (BOE). (2024*). Código de Derecho de la Ciberseguridad.* Edición actualizada a 3 de mayo de 2024. [en línea]. <https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad>*. [Consultado el 20 de mayo de 2024].*

Campus Stellae. (s.f.*). ¿Qué es el Código de Derecho de la Ciberseguridad*? [en línea]. [en línea] https://campus-stellae.com/que-es-el-codigo-de-derecho-de-la-ciberseguridad/ [20 de mayo de 2024]

Parlamento Europeo. (2001). Convenio sobre Ciberdelincuencia [documento en línea]. Consejo de Europa. Budapest: Oficina de Publicaciones del Consejo de Europa. Enlace. (Número de documento: 7 Conv. Budapest). [en línea] <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221> [Consultado el 20 de mayo de 2024].

Consejo de Europa. "20th anniversary Budapest Convention - Cybercrime" [en línea]. Consejo de Europa. Noviembre de 2001. [en línea]<https://www.coe.int/en/web/cybercrime/20th-anniversary-budapest-convention> [Consultado el 20 de mayo de 2024].

Unión Europea. (2013). 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. Diario Oficial de la Unión Europea, L 304/18. *[en línea]* <https://www.boe.es/doue/2013/218/L00008-00014.pdf > *[Consultado el 20 de mayo de 2024].*

INCIBE. (s.f.). Malware. INCIBE. [en línea] <https://www.incibe.es/aprendeciberseguridad/malware>. [Consulta: 21 junio 2024.]

Noticia relativa a "la respuesta del Derecho frente a los ataques de "ransomware" [en línea]<https://cincodias.elpais.com/cincodias/2019/11/06/legal/1573063068_861999.html> [Consulta: 22 de junio 2024]

Noticias relativa al ataque de "ransomware" de mayo 2017. [En línea]. <http://elpais.com/tag/ataques_informaticos/a> [Consulta: 22 junio 2024].

Policía Nacional. (s. f.). Brigada Central de Investigación Tecnológica (B.C.I.T). [en línea] <*https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php*> [Consulta: 29 mayo 2024].

Europol. *European Financial and Economic Crime Centre (EFECC)* [en línea]. Unión Europea. (2020) *[en línea]* <https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc>. [fecha de consulta: 24 junio 2024]

8 JURISPRUDENCIA

- STS, 845/2014, de 2 de diciembre de 2014, (ECLI: ECLI:ES:TS:2014:5632)

- SAP de Tenerife, 541/2005, de 5 de mayo de 2005 (ECLI:ES: APGC: 2005:1799A)
- SAP de La Rioja, 8/2006, de 17 de enero de 2006 ECLI:ES: APLO: 2006:9)
- SAP de Ávila, 146/2008, de 20 de octubre de 2008 (ECLI: APAV: 2008:297)
- SAP de Barcelona, 381/2009, de 14 de abril de 2009 (ECLI:ES: APB: 2009:3191)
- STS, 1107/2009, de 12 de noviembre de 2009 (ECLI: ES:TS: 2009:6983)
- SAP de Cádiz, 23/2011, de 26 de enero de 2011 (ECLI:ES: APCA: 2011:1884)
- SAP de Castellón, 115/2011, de 12 de abril de 2011 (ECLI:ES: APCS: 2011:442)
- SAP de Vizcaya, 429/2016, de 10 de noviembre de 2016 (ECLI: ES: APBI: 2016:2070)
- SAP de Valencia, 488/2009, de 25 de enero de 2017 (ECLI: ES: APV: 2017:1066)