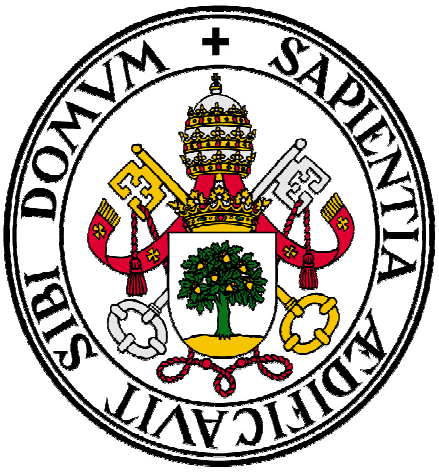

Universidad de Valladolid

Facultad de Derecho

Grado en Criminología

La Ciberdelincuencia y sus consecuencias jurídicas.

Presentado por:

D. Andrés Mesa Millán

Tutelado por:

Dra. Dª. Beatriz Sainz de Abajo

Valladolid, julio de 2017

Reconocimiento-No comercial-Sin obras derivadas.

Usted es libre de:

- Copiar, distribuir y comunicar públicamente la obra, **bajo las condiciones siguientes**:
- **Reconocimiento**: debe reconocer los créditos de la obra de la manera especificada por el autor, pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra;
- **No comercial**: no puede utilizar esta obra para fines comerciales;
- **Sin obras derivadas**: no puede alterar, transformar o generar una obra derivada a partir de esta obra.
- Si reutiliza o distribuye esta obra, tiene que dejar bien claro los términos de la licencia.
- Alguna de estas condiciones puede no aplicarse si obtiene el permiso del titular de los derechos de autor.
- Esta licencia no menoscaba ni restringe los derechos morales del autor.

CONVOCATORIA: JULIO 2017

TÍTULO:

La Ciberdelincuencia y consecuencias jurídicas

AUTOR: D. Andrés Mesa Millán

TUTORA: Dra. Dª. Beatriz Sainz de Abajo

COMISIÓN EVALUADORA:

PRESIDENTE: Dra. Dª. Beatriz Sainz de Abajo

VOCAL 1: Dr. D. Miguel López-Coronado Sánchez-Fortún

VOCAL 2: Dra. Dª. Isabel de la Torre Díez

SUPLENTE 1º: Dr. D. Carlos Gómez Peña

SUPLENTE 2º: Dr. D. Jesús Poza Crespo

SUPLENTE 3ª: Dra. Dª. María García Gadañon

RESUMEN:

Con la realización de este Trabajo de Investigación, se pretende analizar la ciberdelincuencia en España, aproximarnos a la definición de delito informático, analizar la casuística en nuestro país, el marco jurídico que contempla la lucha de la misma tanto de ámbito nacional como a nivel europeo, las organizaciones e instituciones competentes así como la valoración de las medidas de investigación tecnológica con la que se cuenta en la actualidad en España, tras la últimas reformas realizadas en el año 2015.

ABSTRACT:

This research aims to analyze the cyber-delinquency in Spain, as we approach its definition and analyze their characteristics, in the same way as the legal framework that regulates the fight both at national and European level such as organizations and institutions involved, as well as evaluation of the technological research measures that is currently in Spain, motivated by the recent reforms carried out in the year 2015.

PALABRAS CLAVE:

Ciberdelincuencia, Criminal, Delito, Informática, Ciberdelito, Internet, Red.

KEY WORDS:

Cyber-delinquency, Criminal, Crime, Computer science, Cybercrime, Internet, Network.

AGRADECIMIENTOS:

En primer lugar, agradecer a mis tres mujeres el apoyo incondicional que me prestan, puesto que son las que marcan mi camino.

Agradecer también a mi tutora Dra. Dª Beatriz Sainz, el seguimiento y asesoramiento en la confección del presente trabajo para aportar mayor calidad en el mismo.

INDICE

INDICE DE FIGURAS

1. INTRODUCCIÓN

Actualmente no es posible vivir de espaldas a todo cuanto el desarrollo tecnológico y la evolución de este significa, puesto que está presente en muchas facetas como el comercio, suministro de servicios, la comunicación y relación con nuestro entorno, etc., que van evolucionando al mismo ritmo debido a la dependencia de la sociedad de esas tecnologías y del entramado de sistemas y redes que las sustentan; proceso en constante crecimiento tanto en servicios como en usuarios. Esta evolución y la globalización, traen consigo un nuevo ámbito de relación, el ciberespacio, "*dominio global y dinámico compuesto por las infraestructuras de tecnología de la información (incluida Internet, las redes y los sistemas de información y de telecomunicaciones"*[1], espacio virtual y global, por el que desaparecen fronteras y en el que es evidente que al igual que reconocemos el valor e importancia de las Tecnologías de la Información y la Comunicación (TIC), debemos ser conscientes de los riesgos que nos pueden suponer.

Internet es un claro ejemplo de lo hemos reseñado, está en constante evolución y no cesa en su crecimiento en cuanto a usuarios, de esta forma debemos señalar que el ámbito Europeo, el poder de penetración se encuentra en un 77,4 % de la población[2], correspondiendo a España un 76,9% y centrándonos en el marco español, diversos estudios y encuestas de opinión realizadas por organismos públicos como puede ser el Instituto Nacional de Estadística (INE) y el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), que nos indican que "*el uso de TIC es del 80,6 % en personas mayores (16 a 74 años), situándonos en el 95,2% si hablamos del*

[1] GOBIERNO DE ESPAÑA. *Estrategia de Ciberseguridad Nacional.* [En línea]. Madrid, 2013. Pág.9. <http://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20ciberseguridad%20nacional.pdf> [Consulta: 6 marzo 2017].

[2] Información obtenida de <http://www.internetworldstats.com/stats.htm>. Datos actualizados a fecha 31 de marzo de 2017. [Consulta: 3 julio 2017].

uso de internet entre los menores de 10 a 15 años"[3], o que "*más del 41% de los usuarios confían mucho en Internet, aunque realmente no apliquen las medidas de seguridad que debieran"*[4].

Este incremento del uso de Internet o las TIC por los usuarios es el reflejo del uso de éste por los otros sectores de la sociedad en la que se ubican los mismos usuarios, Gobierno, Industria, empresas, Servicios, etc…

Las posibilidades que ofrece el ciberespacio, son numerosas como decimos, lo que puede ser aprovechado por algunos con los conocimientos apropiados para la comisión de actividades ilícitas, aprovechando el anonimato que le ofrece ese espacio virtual, esa "*indeterminación del ámbito geográfico*"[5], así como la supuesta impunidad que le aporte las dificultades para su investigación por competencia o por la disparidad legislativa en los distintos países.

La **justificación del presente trabajo** se basa en sus implicaciones sociales y observamos cuantitativamente que nos encontramos ante un fenómeno creciente por el aumento exponencial del número de usuarios de las TIC; las propias características de los delitos (sobre todo su accesibilidad y ubicuidad) hacen que la persecución de éstos sea más compleja que otras tipologías que no vinculadas a las TIC como medio para la comisión delictiva o fin de las misma, entendiéndose que las ventajas que proporciona el ciberespacio superan a las formas del delito tradicional.

El gran número de usuarios nos lleva a pensar en la figura de la "víctima", puesto que nos convertimos en sujetos pasivos potenciales en este tipo de delincuencia, cada uno de estos usuarios tienen mayor o menor "cultura digital"; siendo cada vez mayor la

[3] INSTITUTO NACIONAL DE ESTADISTICA. *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares. Año 2016*. [En línea]. Madrid, 2016. <http://www.ine.es/dyngs/INEbase/es/operacion.htm?c=estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608> . [Consulta: 11 marzo 2017].

[4] OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN. "*Estudio sobre la ciberseguridad y confianza en los hogares españoles"*. [En línea]. Madrid, 2017.< http://www.ontsi.red.es/ontsi/es/Ciberseguridad-y-confianza-en-los-hogares-españoles-abril-2017 >. [Consulta: 28 abril 2017].

[5] DÍAZ GÓMEZ, Andrés. *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*, REDUR 8. [En línea]. Diciembre 2010, pág. 173. <http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf > [Consulta: 14 marzo 2017].

demanda social en ciberseguridad[6], sobre todo por lo que venimos a denominar como ciberdelito, lo que provoca que los Gobiernos de los países se preocupen para cubrir sus necesidades en ciberseguridad legislando, de forma que en esta evolución "negativa" de las tecnologías, alguno ve una manifestación más de la sociedad del riesgo y con ello el necesario Derecho Penal del Riesgo[7], según el cual como consecuencia de la evolución de la ciberdelincuencia es necesario demandar una mayor seguridad a las Autoridades.

Al abordar este fenómeno en el ciberespacio, no cabe duda que para que sea efectivo es necesario contar con alianzas, colaboración y cooperación transfronteriza, ya que no podemos obviar que la desaparición de las fronteras "*afecta a la competencia jurisdiccional, a la ley penal aplicable y al procedimiento que se tramitará para su investigación y enjuiciamiento*"[8] , que viene a demostrar que en este ámbito, ciberseguridad y ciberdelincuencia, es el derecho internacional el que debe armonizar las legislaciones nacionales preexistentes, impulsando la adopción de medidas pertinentes.

Parece evidente que, como venimos reseñando en los últimos años han surgido nuevos retos y amenazas relacionadas con las TIC, definiéndose como amenazas a la Ciberseguridad, suponiendo un nuevo espectro que puede ser delincuencial y en el que las Autoridades deben llevar cabo no solo su función investigadora (desde la perspectiva penal, investigación de delitos), sino que también debe abordar labores de prevención y actuaciones proactivas en este nuevo ámbito de actuación que es el Ciberespacio.

Para alcanzar el objetivo de mejorar la calidad en ambas facetas (tanto la preventiva como la represiva), es punto de partida la formación del personal, así como desarrollar a su vez protocolos de actuación. En este aspecto es de resaltar la dispersión de esfuerzos y entidades cuya función principal o adicional es la lucha y mitigación de estos fenómenos.

---

[6] Ver glosario.

[7] ANARTE BORRALLO, Enrique. "Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información". *Derecho y Conocimiento, Anuario Jurídico sobre la Sociedad de la Información*, Volumen 1, Universidad de Huelva: Facultad de Derecho, 2001, Págs. 191 y ss.

[8] RAYÓN BALLESTEROS, María Concepción y GÓMEZ HERNÁNDEZ, José Antonio. *Cibercrimen: particularidades en su investigación y enjuiciamiento.* Anuario Jurídico y Económico Escurialense. [En línea]. XLVII (2014) pág. 215. ISSN: 1133-3677. <https://dialnet.unirioja.es/servlet/articulo?codigo=4639646 > [Consulta: 14 marzo 2017].

En este sentido, resulta precisa la coordinación de esfuerzos investigadores, amén de contar con una estrategia clara y definida que permita aunar esfuerzos y recursos con el objetivo de optimizar los mismos. Igualmente, se hace necesario conocer la realidad del fenómeno delictivo informático, de las empresas o instituciones actores en el proceso de investigación informática, de las necesidades de cooperación y coordinación internacional, y de las necesidades legislativas, para de esta manera poder conocer mejor lo referido a la ciberdelincuencia e investigación tecnológica, en la que no solo se ve afectado el Ministerio de Interior. A esto, hay que añadir el riesgo o temor a un dimensionamiento del delito contra sistemas de información de infraestructuras críticas, que afectan a la Seguridad Nacional o actuaciones con fines políticamente desestabilizadores, entrando de lleno en el campo del Ciberterrorismo y, consecuentemente, de estructuras policiales adicionales, que se suman al escenario de la necesaria coordinación y cooperación técnica policial.

Dada la extensión de los aspectos a tratar, así como el tiempo y el espacio limitado de que se dispone, se marca como **objetivo de este trabajo**, dentro de los distintos aspectos de los que integran un tema de la magnitud de posibilidades de estudio que ofrece, realizar un análisis de la evolución de la ciberdelincuencia en España. Por lo que se hace necesaria la acotación del tema a analizar, así como centrar el universo de estudio. Por lo que respecta al primer punto, se ha focalizado la atención en el análisis de lo que supone la ciberdelincuencia, ver sus características, como la misma a medida que evoluciona provoca cambios significativos en las Autoridades encargadas de asegurar la protección a los ciudadanos, por lo que deben establecer o redefinir estrategias y legislar al respecto; establecer organismos o instituciones para afrontar tales actividades, etc. de forma que se aboga por concentración de recursos y esfuerzos, para lograr una mayor eficacia. En lo relativo al universo de estudio, se ciñe al ámbito Nacional, aunque como es normal y característico de la ciberdelincuencia no se puede obviar la influencia del ámbito internacional que nos repercute al abordar los fenómenos de la ciberdelincuencia y la ciberseguridad.

Para conseguir este objetivo, es necesario contar con un método de trabajo adecuado al tipo de estudio a realizar. El análisis documental, como consecuencia del aspecto documental del objetivo marcado, unido a la imposibilidad de establecer muestras de poblaciones sobre las que aplicar las hipótesis y evaluar los resultados, obliga a realizar una investigación Cualitativa; utilizando para ello una técnica Descriptiva, basada en el método Hipotético-Deductivo. Aunque este marco también se podría complementar con

las reflexiones y experiencias de profesionales que desarrollan sus actividades en el ámbito del presente estudio.

Una vez fijado el objetivo y el método que se va a emplear en este estudio, el siguiente paso sería determinar las líneas principales de investigación que se van a seguir. Estas líneas se van a centrar en el análisis y estudio del fenómeno que plantea el problema, así como la normativa legal existente en este ámbito, desde el punto de vista de la investigación de los ilícitos que se cometan.

La primera línea de investigación se centrará en introducir el concepto de ciberdelincuencia, así como representar los diferentes tipos y formas en que esta puede ser clasificada, conocer qué tipo de delitos son los más frecuentes, así como las tendencias futuras.

A continuación, se tratará de manera extensa el análisis del marco normativo relacionado, y en concreto, las estrategias y normas de interés establecidos, tanto a nivel internacional, como europeo y nacional; observando de este prisma como se ha ido evolucionando en la materia. Este punto es fundamental para conocer los límites de las investigaciones, así como las posibilidades que existen según la situación planteada.

En el siguiente punto se revisan los medios con los que cuenta actualmente la Administración General del Estado para combatir este tipo de delitos, los cuales pueden llegar a afectar a la Seguridad Nacional, además de otros organismos de ámbito internacional que pueden participar en la lucha contra este tipo de delincuencia.

En otro apartado se reseñan algunas herramientas de investigación de éste fenómeno delictivo, al observar la problemática que plantea esta tipología delictiva que, debido a la su evolución, en algunos casos se hace necesario la utilización de técnicas que pueden ser distintas a las que se venían utilizando en las investigaciones tradicionales.

Finalmente, se llevarán a cabo unas conclusiones sobre la situación analizada, haciendo una reflexión sobre los puntos abordados en el trabajo.

2. CIBERDELINCUENCIA (DELINCUENCIA INFORMÁTICA).

2.1.- Aproximación al concepto.

Respecto a los delitos informáticos, no hay consenso y además no existe una definición de los mismos en la legislación española, ni siquiera como categoría genérica, comúnmente se ha denominado a los delitos cometidos a través de las nuevas tecnologías con diversos sobrenombres tales como delitos informáticos, criminalidad mediante computadoras, delincuencia informática, o criminalidad informática. Pero está claro que dicha descripción puede llegar a ser insuficiente, la norma penal no puede ser aplicada por derivación o intuición, estando recogido en el artículo 25.1 de la Constitución Española el principio de legalidad, al objeto de impedir la actuación arbitraria en materia sancionadora por parte del Estado y dotando a los ciudadanos de seguridad jurídica.

Por ello, la aparición y evolución de las TIC ha generado que se tipifiquen nuevas conductas de carácter delictivo para poder dar una respuesta adecuada a dichas necesidades y proteger a la sociedad en su conjunto. Prosiguiendo con la aproximación al concepto de delito informático, realmente no existe una definición clara y común del mismo, son numerosos los autores que aportan distintas definiciones, en su obra el Dr. Santiago Acurio, en la búsqueda de esta definición explora la opinión de varios autores[9], algunos se centran para definir el delito informático en los delitos que se dan con "*la ayuda de la informática o técnicas conexas*", otro como los que la acción se realiza mediante la "*utilización del elemento informático o vulnerando los derechos del titular, sea hardware o software*" o aquel que define el delito informático en cuando la acción delictiva tiene a "*las computadores como instrumento o fin*".

Tras su análisis el Dr. Acurio considera que para no concluir en una definición muy cerrada, como sería la de "delito informático", es más interesante definir el fenómeno, siendo esta más amplia y flexible, por tanto define a la delincuencia informática como "*todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir,*

[9]ACURIO DEL PINO, Santiago. *Delitos Informáticos: Generalidades*. [En Línea]. Págs. 10-11. Disponible en:<http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf> [Fecha de Consulta: 22 marzo 2017].

o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera". [10]

Otro de los autores que abordan este tema, y sobre todo desde la perspectiva criminológica, como es Fernando Miró, sobre las definiciones del cibercrimen señala que el aspecto esencial se reduce a la cuestión de si se está adoptando una concepción amplia (cualquier comportamiento delictivo llevado a cabo en el ciberespacio, sea nuevo o delito tradicional) o una concepción restringida (aquellas infracciones en las que la utilización de las TIC tiene que ver con el aspecto esencial del delito), para el autor la ciberdelincuencia o cibercrimen es "*cualquier delito en el que las TIC juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan*"[11], de modo similar a la definición de ciberdelincuencia como cualquier acto ilegal cometido por medio de (o con la asistencia de) cualquier TIC.

Continúa Miró Llinares, en su obra con la categoría de ciberdelincuencia (en la actualidad preferible a la denominación de delincuencia informática), admitiendo que "*tal categoría no engloba tipos penales sino tipologías de conductas peligrosas para dichos bienes y caracterizadas por la utilización de redes telemáticas y demás sistemas, terminales y servicios de las TIC, con los riesgos que ello conlleva*", de esta forma realiza dos clasificaciones fenomenológicas[12] en la que distingue por un lado los cibercrímenes teniendo en cuenta la diferente incidencia de las TIC en la esencia de la conducta criminal, y por otro lado cuando se diferencien los cibercrímenes en el ciberespacio atendiendo a los distintos intereses sociales con trascendencia jurídica que se puedan ver afectados por los mismos (atiende a los sujetos activos y a sus objetivos últimos); resumidas en la figura 1.

[10]Ibíd. Pág. 14

[11] MIRÓ LLINARES, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, 2012. Pág. 44.

[12] Ibíd. Págs. 47-135.

	Ciberataques puros	Ciberataques réplica	Ciberataques de contenido
CIBERCRÍMENES ECONOMICOS	- *Hacking* - *Malware* intrusivo - *Malware* destructivo - Ataques de *insiders* - Ataques *DoS* - *Spam* - Ciberocupación red - *Antisocial networks*	- Ciberfraudes (*phising, pharming, scam*...) - *Cyberspyware* (uso de *sniffers*, y demás *spyware, ciberespionaje de empresa*) - *Identify theft* - *Spoofing (DNS spoofing , ARP, soofing, IP spoofing)* - Ciberblanqueo de capitales - Ciberextorsión - Ciberocupación	- Distribución de pornografía en Internet - Ciberpiratería intelectual
CIBERCRÍMENES SOCIALES		- *Spoofing* - *Cyberstalking* - *Cyberbullying* - *Online harassment* (ciberamenazas, coacciones, injurias, etc.) - *Sexting* (y extorsión con imágenes de *sexting)* - *Online grooming*	
CIBERCRÍMENES POLÍTICOS	- Ataques *DoS (cyberwar)* - Ataques *DoS (cyberhacktivism)* - *Malware* intrusivo	- Ciberespionaje terrorista - Ciberguerra	- *Online hate speech* - Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

Figura 1.-*Tabla tipológica-criminológica de la ciberdelincuencia. (Fuente: Miró Llinares, F., 2012)*

Por tanto y a tenor de lo anterior no existe una definición como tal del concepto de delito informático, que sea unánime a todos los países, es más en el Código Penal español como ya hemos señalado, no viene siquiera definido como tal dicho concepto. Si bien por ascendencia normativa, en España se han ido adoptando diversas modificaciones legislativas al objeto de adecuar la legislación a las directrices comunitarias y evitar problemas a los efectos de cooperación con otros estados en materia penal.

Por todo esto, para poder acercarnos a la definición del delito informático es necesario recurrir al Convenio sobre Ciberdelincuencia, del Consejo de Europa de 2001, ya que en su preámbulo indica que se hace necesario la tipificación como delito de "*los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos*"[13], siendo esta referencia la que goza

[13]CONSEJO DE EUROPA. *Convenio sobre la Ciberdelincuencia.* Serie de Tratados Europeos nº 185. [En línea]. Budapest, 2001. Pág.2
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=

de mayor aceptación por el consenso alcanzado. En el Convenio se acotan los delitos informáticos en cuatro grupos, donde vienen a definirse los tipos penales que deben considerarse Delito Informático, lo que sin duda hace necesario que lo analicemos en los siguientes apartados del presente trabajo, estos grupos son los siguientes:

I. *Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos*. Engloba las conductas de acceso ilícito, interceptación ilícita, interferencia de datos, interferencia de sistemas y el abuso de dispositivos (arts. 2 al 6 del Convenio).
II. *Delitos informáticos*. Dos tipos penales, la falsificación informática y el fraude informático (arts. 7 y 8)
III. *Delitos relacionados con el contenido*. Comprende las conductas relacionadas con la pornografía infantil en la Red (art.9). Además, se incluyeron las conductas de apología del racismo y xenofobia a través de la Red, mediante el *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos* de 2003.
IV. *Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines*. (Art 10).

También podemos fijarnos en la Instrucción 2/2011dictada por la Fiscalía General del Estado por la que se crea la figura del Fiscal de Sala de Criminalidad Informática y en la que además se trata de concretar el catálogo inicial de delitos a los que se extiende el marco competencial de esta área. El catálogo se ha estructurado en tres categorías, "*delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs, delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs y delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia*"[14].

09000016802fa41c> [Consulta: 14 marzo 2017].

[14]FISCALIA GENERAL DEL ESTADO. *Instrucción 2/2011 sobre el fiscal de sala de criminalidad informática y las secciones de criminalidad informática de las fiscalías*. [En línea]. Madrid, 2011. Págs. 7-8. <https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_instru_02.pdf?idFile=6311c525-d23a-45d7-9e50-458f6f8c3406> [Consulta: 23 marzo 2017].

2.2.-Convenio sobre Ciberdelincuencia

2.2.1.- Antecedentes.

Motivado por las amenazas que supone la evolución de las TIC, la globalidad, la posible desvinculación de los lugares de origen y resultado, la posibilidad de provocar daños supranacionales, surge el Convenio del Consejo de Europa sobre Ciberdelincuencia adoptado en Budapest el 23 de noviembre de 2001. Este Convenio pretende armonizar la legislación de los diversos países que lo ratifiquen, no sólo en materia de derecho penal sustantivo, sino también de derecho procesal para hacer frente a ese tipo de delincuencia.

Se constituye hasta el momento, como el primer y único Convenio en materia de ciberdelincuencia. Por ello, es relevante estudiar los orígenes y evolución del mismo.

Es evidente que la creación de este Convenio no fue fácil, autores como Rodríguez Bernal, sitúa el origen del Convenio en 1983, momento en el que un grupo de expertos formado por miembros de numerosos organismos internacionales como Interpol, la Organización de Naciones Unidas y la Unión Europea (UE) entre otros, advierte a la Organización para la Cooperación y Desarrollo Económico (OCDE) de la inminente necesidad de elaborar un sistema de cooperación internacional en el que se tratase la materia de delitos informáticos. Consecuentemente, se elaboró un informe en 1986 "*que recoge las normas penales existentes en diversos países, proponiendo reformas y recomendado un mínimo de ilícitos que debieran ser prohibidos y castigados por la ley penal*"[15], que sirvió para que el Consejo de Europa, como señala Díaz Gómez, tome la iniciativa, "*y ya en1989 publica la Recomendación nº 89(9), mostrando la clara tendencia que desembocará en Budapest*"[16]:

> *"De conformidad con el Artículo 15.b del Estatuto del Consejo de Europa y habida cuenta de que el objetivo del Consejo de Europa es lograr una mayor unidad entre sus miembros, el Comité de Ministros; reconociendo la importancia de dar rápidamente una respuesta adecuada al*

[15]RODRIGUEZ BERNAL, A. *Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia*. Revista de derecho informático nº 103. 2007, pág. 13. <http://www.egov.ufsc.br/portal/sites/default/files/los_cibercrimenes_en_el_espacio_de_libertad_seguridad_y_justicia.pdf>. [Consulta: 23 marzo 2017].

[16]DÍAZ GÓMEZ, Andrés. *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*, REDUR 8. [En línea]. Diciembre 2010, pág. 195. <http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf> [Consulta: 14 marzo 2017].

nuevo desafío que constituye el delito cibernético; considerando que el delito cibernético suele tener carácter transfronterizo; consciente de la necesidad concomitante de promover la armonización de la legislación y las prácticas, y de mejorar la cooperación internacional, recomienda a los Gobiernos de los Estados Miembros que:

1. *Tengan en cuenta, al revisar su legislación o iniciar la promulgación de nuevas leyes, el Informe sobre el delito cibernético preparado por el Comité Europeo para problemas criminales, y en especial las directrices destinadas a los parlamentos nacionales.*
2. *Informar al Secretario General del Consejo de Europa durante 1993 acerca de cualquier evolución de su legislación, práctica judicial o experiencia en materia de cooperación jurídica internacional en lo que concierne al delito cibernético."*[17]

En 1996, el Comité Europeo para los problemas criminales (CDPC) establece un Comité de expertos encargado de los delitos informáticos, teniendo su fundamento principalmente en la rápida evolución de las TIC y la creación del ciberespacio, con el peligro que acarrea la posibilidad de cometer delitos en el mismo con la dificultad de determinar a quién corresponde su investigación, debido a la transnacionalidad que tienen y por ello consideraban que el derecho penal no podía dar la espalda a dicha evolución.

Además, el CDPC también considero el informe elaborado, por el profesor H.W.K. Kaspersen, a petición suya, que llegaba a la conclusión de que "*habría que buscar otro instrumento jurídico más obligatorio que una recomendación, tal como un convenio. Dicho convenio no debería abordar tanto las cuestiones de derecho penal sustantivo como las cuestiones de derecho procesal penal, así como también los acuerdos y procedimientos del derecho penal internacional*"[18], conclusiones estás similares a la de la Recomendación R (89) 9.

[17] Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.[En línea]<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094>[Consulta: 23 marzo 2017].

[18]CONSEJO DE EUROPA. *Informe explicativo del Convenio sobre la Ciberdelincuencia.* Serie de Tratados Europeos nº 185. [En línea]. 2001. Pág. 3<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa403> [Consulta: 14 marzo 2017].

A la vista de esto, en abril de 1997 el Comité de Expertos en la Delincuencia del Ciberespacio (PC-CY) comienza a trabajar sobre el Convenio, hasta diciembre del 2000, se fueron realizando las actuaciones correspondientes, en este periodo de tiempo se redactaron muchas versiones del proyecto. Los ministros de Justicia europeos apoyaron en más de una ocasión (Praga, junio 1997 y Londres junio 2000, entre otros), la labor que estaba llevando a cabo el PC-CY, animándoles con el proyecto y la consecución de dos objetivos principalmente: solventar de rápida y eficientemente los problemas derivados de la ciberdelincuencia y conseguir que fuese firmado y ratificado por la mayoría de los Estados.

El 27 de abril de 2000 se alcanzó el consenso necesario para poder publicar el Proyecto de Convención sobre Delito Cibernético, no obstante, esta primera versión no prosperó, por lo que a continuación, se fueron realizando diversas versiones del Proyecto. Dando de esta forma la oportunidad a los Estados de poder realizar consultas y solventar todas aquellas cuestiones que pudiese suscitar, resultando de gran utilidad este proceso de consulta.

Finalmente, el Convenio sobre la Ciberdelincuencia fue aprobado por el Consejo de Ministros del Consejo de Europa el 8 de noviembre de 2001 y el día 23 de noviembre, abierto para su firma.

2.2.2.- El Convenio sobre Ciberdelincuencia

El objeto del Convenio es lograr **unificar la actuación de los países contra la ciberdelincuencia**, centrándose principalmente en la armonización normativa y en el reforzamiento de la cooperación internacional. El Convenio establecía, para todo aquel país que ratificara el mismo, la obligatoriedad de adoptar las medidas legislativas, y de otro tipo, que resultaran necesarias para alcanzar los objetivos en él marcados.

El Convenio, establece en su preámbulo unas premisas importantes, donde se reflejaban los objetivos[19] del mismo como es la necesidad de adoptar una legislación adecuada mejorando la cooperación internacional, asumiendo los poderes suficientes para garantizar la lucha eficaz contra la ciberdelincuencia que faciliten su detección, investigación y sanción, permitiendo la obtención de pruebas electrónicas para aportar más calidad en las investigaciones y procedimientos penales, destacando la importancia de la

[19] Ob. Cit. CONSEJO DE EUROPA. *Convenio sobre la Ciberdelincuencia.* Págs.1-2.

cooperación público-privada, señalando a su vez la importancia de que estas medidas se han de promover tanto a nivel nacional como internacional.

El Convenio se organiza en tres grandes bloques, distribuidos en cada uno en un capítulo, donde se abordan distintas cuestiones, y finaliza con un cuarto capítulo de Disposiciones finales.

En este Convenio, además de establecer una **terminología básica común**[20], se realiza una **armonización normativa en materia penal**[21], acotando los delitos informáticos en cuatro grupos y definiendo los tipos penales que han de considerarse como delito informático, como ya hemos señalado en el inicio del presente capítulo de este trabajo, y posteriormente se abordan las responsabilidades y sanciones conexas.

Además, el Convenio también establece procedimientos buscando una **armonización normativa común procesal y de investigación**, sobre los siguientes conceptos:

- Conservación rápida de datos informáticos almacenados.
- Conservación y Revelación parcial rápida de datos conservados.
- Órdenes emitidas a personas o proveedores de comunicación de datos.
- Registro, confiscación e interceptación de datos.
- Obtención en tiempo real de datos relativos al tráfico.
- Asistencia mutua en relación con el acceso a datos almacenados.
- Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público.
- Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico.
- Asistencia mutua en relación con la interceptación de datos relativos al contenido.

[20]En el capítulo 1 "*Terminología*" se recogen una serie de definiciones y conceptos considerados esenciales para la aplicación del convenio. Establece las definiciones de "sistemas informáticos", "datos informáticos", "proveedor de servicios" y "datos relativos al tráfico". Ver glosario.

[21]El capítulo 2 "*Medidas que deberán adoptarse a nivel nacional*", se encuentra a su vez dividido en varias secciones. Sección 1(*Derecho penal sustantivo*), sección 2 (*Derecho procesal*) y sección 3 que incluye disposiciones en materia de jurisdicción.

Por último, el Convenio realiza un **reforzamiento de Cooperación Internacional**, estableciendo unas herramientas para mejorar la cooperación de forma que se habilitan los siguientes procedimientos:

- **Extradición**.
- **Asistencia mutua,** en investigaciones o al objeto de obtención de prueba electrónica, respecto de conservación y acceso a datos informáticos.
- Traslado de **información espontánea**[22].
- **Comunicación directa entre autoridades judiciales** para solicitud de asistencia, en casos de urgencia.
- Creación de la **Red 24/7**, designando cada Parte un punto de contacto permanente, garantizando la inmediatez de la asistencia.

2.2.3.- Estado Actual del convenio

Actualmente el Convenio sobre la Ciberdelincuencia ha sido ratificado por 55 países, y firmado por cuatro países pero no ratificados hasta el momento, Irlanda (firmado 28/02/2002), San Marino (17/03/2017), Suecia (23/11/2001) y Sudáfrica (23/11/2001)[23].

Para observar la importancia de este Convenio también merece atención la evolución de los Estados no miembros realizada en los últimos años puesto que, desde la aprobación de éste, tan solo había sido ratificado por Estados Unidos en 2006. Sin embargo, a partir de 2012, fueron varios los Estados terceros que decidieron ratificarlo, Australia y Japón (2012), República Dominicana y Mauricio (2013), Panamá (2014), Sri Lanka y Canadá (2015), Israel y Senegal (2016), siendo los últimos países en ratificarlo Chile el 20 de abril de 2017 y Tonga el pasado 09 de mayo de 2017.

Actualmente hay cuatro países invitados a adherirse, Colombia, Ghana, Paraguay y Perú.

[22]Sin necesidad de solicitud previa, una Parte podrá comunicar a otra la información que resulte de sus propias investigaciones si considera que ésta pueda iniciar investigaciones o procedimientos en relación con delitos que se abordan en el Convenio, o cuando esta información provocare la petición de cooperación.

[23]*Firmas y ratificaciones del tratado nº 185. Convenio sobre Ciberdelincuencia.* [En línea]. <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures> [Consulta: 12 junio 2017].

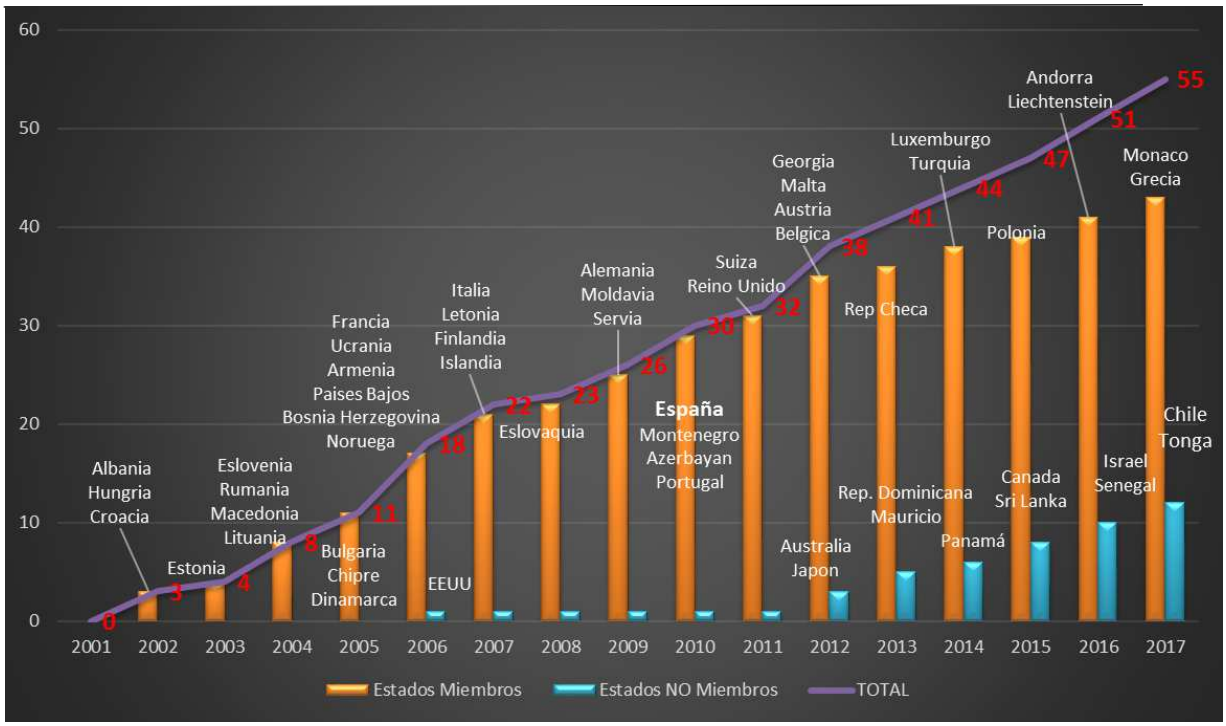

Figura 2.-*Países que han ratificado el Convenio sobre ciberdelincuencia. (Elaboración propia)*

España, que estuvo presente desde las negociaciones iniciales del Convenio, lo firmó el mismo 23 de noviembre de 2001 y sería el día 3 de junio de 2010 cuando decidió ratificarlo mediante el instrumento de ratificación[24],con periodo de efecto fechado para el día 1 de octubre de 2010 y con dos Declaraciones una en la que señala que las relaciones internacionales de Gibraltar, son responsabilidad de Reino Unido, al ser éste un territorio no autónomo y otra en las que comunica las Autoridades responsables que establecen el Convenio en lo referido a la Extradición (art. 24) y solicitudes de asistencia mutua (art.27), siendo ésta la Subdirección General de Cooperación Jurídica Internacional del Ministerio de Justicia, así como que sería la Comisaría General de Policía Judicial del Ministerio de Interior el punto de contacto de la Red 24/7 dispuesto en el art.35 del Convenio.

2.2.4.- El Protocolo adicional al Convenio sobre la Ciberdelincuencia

Para complementar al Convenio, en el año 2003, se redactó un instrumento importante, el Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la

[24]GOBIERNO DE ESPAÑA. *Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001*. Agencia Estatal Boletín Oficial del Estado. [En línea]. 2010. <https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf> [Consulta: 23 marzo 2017].

penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, entrando en vigor el 1 de marzo de 2006.

Aprovechando las herramientas de cooperación internacional que ofrece el Convenio sobre la Ciberdelincuencia y atendiendo a la necesidad de armonización en materia penal para afrontar la divulgación de tipo racista y xenófoba que se comenten mediante los sistemas informáticos, este documento vino a ampliar el catálogo de actos ilícitos que engrosaban los delitos relacionados con el contenido (*artículo 9: Delitos relacionados con la pornografía infantil*) regulados en el Titulo 3 del Convenio.

De este modo se viene a tipificar la difusión, amenazas e insultos de índole racista y xenófoba y la negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad, cuando estos actos se llevan a cabo por medio de un sistema informático.

El Protocolo adicional, fue firmado por España en 2013, ratificado en diciembre de 2014[25] haciendo una declaración sobre Gibraltar en los mismos términos a la realizada en la ratificación del Convenio sobre la Ciberdelincuencia y con entrada en vigor el 01 de abril de 2015.

2.3.- La ciberdelincuencia en España en datos.

Centrándonos en España, al objeto de observar cómo va evolucionando la ciberdelincuencia, podemos fijarnos en los datos estadísticos aportados tanto por el Ministerio del Interior como por el Ministerio de Justicia:

1º.- Si observamos el Estudio sobre Cibercriminalidad del Ministerio del Interior, siendo el último publicado del año 2017, correspondiente a datos del año 2016 en el que se recogen datos estadísticos sobre la cibercriminalidad, en el mismo se hace un análisis empleando las tipologías penales descritas en el Convenio sobre Ciberdelincuencia. En la siguiente figura se representa la actividad registrada por las Fuerzas y Cuerpos de Seguridad

[25] GOBIERNO DE ESPAÑA. *Instrumento de Ratificación del Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*. Agencia Estatal Boletín Oficial del Estado. [En línea]. 2013. <https://www.boe.es/boe/dias/2015/01/30/pdfs/BOE-A-2015-793.pdf> [Consulta: 23 marzo 2017].

del Estado (FCSE), la Policía Foral de Navarra, y algunas Policías Locales que facilitaron datos al Sistema Estadístico de Criminalidad durante el año 2016.

Grupos delictivos	2012	2013	2014	2015	2016
Acceso e interceptación ilícita	1.701	1.805	1.851	2.386	2.579
Interferencia en los datos y en el sistema	298	359	440	900	1.110
Falsificación informática	1.625	1.608	1.874	2.361	2.697
Fraude informático	27.231	26.664	32.842	40.864	45.894
Delitos sexuales	715	768	974	1.233	1.188
Contra la propiedad industrial/intelect.	144	172	183	167	121
Contra el honor	1.891	1.963	2.212	2.131	1.524
Amenazas y coacciones	9.207	9.064	9.559	10.112	11.473
Total	42.812	42.403	49.935	60.154	66.586

Figura 3.-*Evolución tipologías penales conocidas cometidas con TIC en España.(Fuente: Ministerio del Interior)*[26]

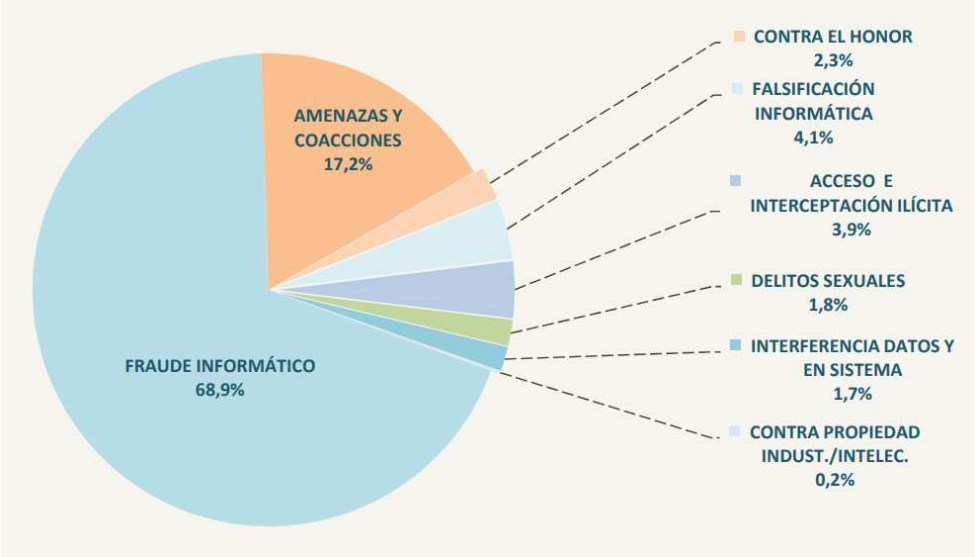

Figura 4.-*Tipologías penales conocidas cometidas con TIC España 2016 (%). (Fuente: Ministerio del Interior)*

2º.- Revisando las Memorias elaboradoras por la Fiscalía General de Estado, siendo en estos momentos la más actual la del año 2016, concretamente se debe analizar el

[26]GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR. *Estudio sobre la cibercriminalidad en España 2016*. [En línea]. Madrid, 2017. Pág. 33. http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf > [Consulta: 4 julio 2017].

contenido de su capítulo de criminalidad informática[27], para poder determinar en comparación con años anteriores cual ha sido la evolución de esta modalidad delictiva.

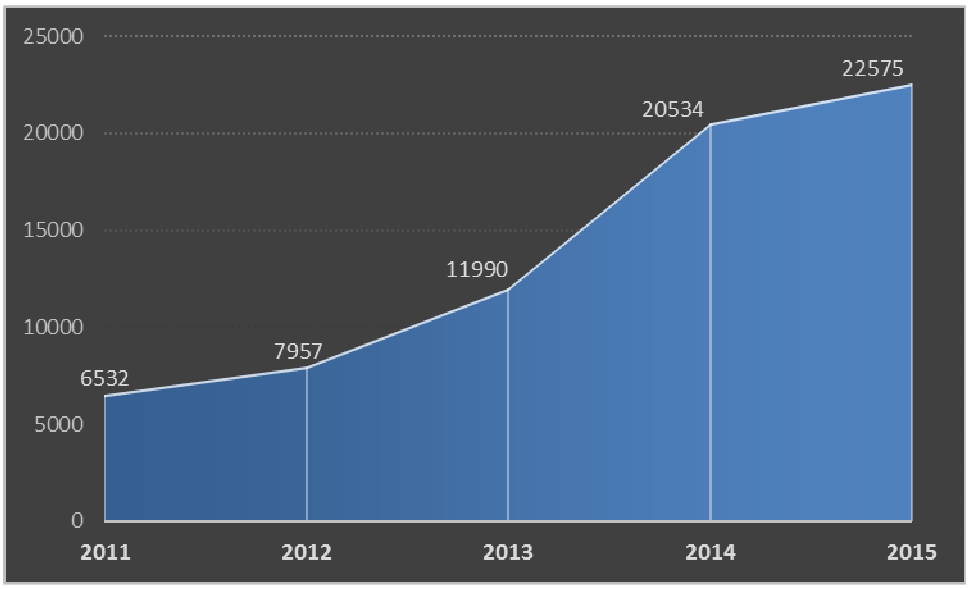

***Figura 5**.- Evolución procedimientos judiciales incoados referidos a criminalidad informática. (Elaboración propia)*

La evolución según observamos en las figuras 3 y 5 demuestra que este tipo de delitos han aumentado con el paso de los años, acorde a la misma evolución del uso de las TIC. Sin embargo, si analizamos los datos de la Fiscalía, a diferencia de los aportados por el Ministerio del Interior, parece que el incremento exponencial que se venía dando ha disminuido, encontrando la explicación a ello en la misma Memoria, de forma que justifican la ruptura de este ritmo de crecimiento al art. 248.2 de la LECrim, ya que tras la última reforma la Autoridades policiales no remiten sus diligencias a la Autoridad Judicial, cuando no existe autor conocido y no concurren las excepciones marcadas en el referido artículo.

[27] FISCALIA GENERAL DE ESTADO. *Memoria elevada al Gobierno de S.M. Capítulo III. Fiscales Coordinadores y Delegados para materias específicas- 8. Criminalidad Informática.* Centro de Estudios Jurídicos. Ministerio de Justicia. [En línea]. Madrid, 2016. <https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/recursos/pdf/capitulo_III/cap_III_8.pdf> [Consulta: 26 marzo 2017].

Delitos informáticos		Procedimientos judiciales	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.).	1.009	4,47
	Acoso a través de TICs (art. 172 ter).	96	0,43
Contra la integridad moral	Trato degradante a través de TICs (art. 173).	226	1,00
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189).	767	3,40
	Acoso menores a través de TICs (art. 183 ter).	98	0,43
	Otros delitos c/libertad sexual a través TIC.	77	0,34
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter).	220	0,97
	Descubrimiento/revelación secretos a través TIC (art. 197).	597	2,64
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215).	254	1,13
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (art. 248 y 249).	18.201	80,62
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss.).	276	1,22
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286).	27	0,12
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	295	1,31
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss.).	70	0,31
De falsedad	Falsificación a través de la TICs.	193	0,85
Contra Constitución	Discriminatoria a través TIC (art. 510).	40	0,18
Otros		129	0,57
Total		22.575	100

***Figura 6.**- Procedimientos judiciales incoados por hechos ilícitos en año 2015. (Fuente: Fiscalía General Estado)*

De la observancia de la estadística se hace necesario realizar algunas apreciaciones, en la memoria se analiza los procedimientos incoados en el año 2015 si observamos la figura 6, vemos que las estafas/fraudes informáticos representan un 80,6 % (18.201)[28]., constituyendo según el Ministerio del Interior el 68,9 % de los delitos conocidos por la Autoridades policiales, como consta en la figura 4.

La Fiscalía en la misma Memoria, al respecto indica que este tipo delictivo engloba acciones muy diferentes con modalidades específicas, lo que dificulta su investigación y determinación de responsabilidades, señalando la participación de delincuencia organizada, la transnacionalidad, la necesidad de cooperación internacional, la acreditación de intencionalidad dolosa o imprudente, etc.

[28] La estafa se presenta como el delito más conocido, siendo su evolución en años anteriores la siguiente; año 2011; 4204, año 2012: 5992, año 2013:9663 y en 2014: 17328 expedientes.

Realmente si nos damos cuenta al abordar la criminalidad informática, no es que conozcamos delitos nuevos, sino que lo que observamos es otra forma de cometer los delitos sirviéndose de las posibilidades de las TIC.

Está claro es para una mejor comprensión de la ciberdelincuencia, podríamos abordar en el presente trabajo aspecto como quienes son los autores y las víctimas de este tipo de delitos, ya que es importante ser conscientes de la existencia de diferentes tipos de autores[29] de la actividad ilícita, conocer las características de los distintos perfiles del delincuentes para poder diferenciarlos, conocer sus motivaciones e intereses, así como reconocer a las posibles víctimas de los delitos para poder prevenirlas ante futuras amenazas, sin duda alguna este conocimiento aportaría mayor calidad al trabajo en sí, pero no es menos cierto que ya de por sí solo, estos actores, podrían ser el objetivo de un trabajo por sí mismo y no es intención de incluirlos en el presente. Continuando en el conocimiento de la materia, resulta de interés mantenerse actualizado mediante los distintos informes oficiales[30] que se elaboran al respecto.

No obstante, debido a la gran importancia que adquieren el tipo delictivo de las estafas cometidas a través de las TIC (constituyen el 80,6 % de los delitos), se hace necesaria alguna mención al respecto sobre esta tipología. Nos podemos encontrar a modo de resumen dos tipos de actividad:

1º.-En la que el sujeto pasivo se dirige al delincuente de forma que involuntariamente le aporta los datos que este necesita, donde entraría el Phising, que se puede definir como "*un mecanismo que emplea tanto técnicas de ingeniería social y técnicas evasivas para robar la identidad, los datos personales y la información financiera de los consumidores*"[31], el Ramsomware, etc.[32]. Existen diferentes modalidades de *phishing*, como *pharming, smishing, vishing* o *spear phishing*. Al parecer en la actualidad, en lugar de intentar el envío de correos de forma indiscriminada a multitud de usuarios se tiende a la variedad "spear phishing", consistente en "*mandar mensajes estafa a objetivos concretos, bien sea un grupo de trabajadores de una*

[29] *Hackers, Crackers, Phreakers,* etc.

[30]Consultar informes en web: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html

[31]VELASCO SAN MARTÍN, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet.* Valencia: Tirant lo Blanch, 2012. Pág. 71.

[32] Ver glosario.

misma empresa, bien sea una única persona, consiguiendo tasas de éxito veces mayores: se estudian sus hábitos y se crea mensajes a medida"[33]. Es decir, seleccionando a los sujetos pasivos, entre los que se conocen sus hábitos y expectativas, es más fácil hacerlos caer en el engaño.

2.- En las que el delincuente se dirige hasta la víctima, accediendo a su ordenador, para "robar" sus datos, claves, etc. Es decir, el acceso a sistemas con archivos espía para obtener claves, que tiene lugar a través de diversos tipos de malware o software malicioso. Éstos, son "*programas de cómputo que son introducidos en los sistemas de información de los usuarios para causarles algún daño o simplemente para modificar su uso y obtener su control*"[34], por lo que, además de ser capaces de provocar daños en los sistemas informáticos, también pueden ser empleados para recoger datos personales del usuario y enviarlos a terceras personas sin que sean conscientes de ello.

2.4.- Tendencias de la Ciberdelincuencia

Continuando con lo referido a la evolución de la ciberdelincuencia, es necesario reseñar que en septiembre de 2016, se presentó por parte de Europol, la Evaluación de la Delincuencia Organizada de Internet[35] (Internet Organised Crime Threat Assessment 2016; IOCTA), donde señala que continúa incrementándose el coste de la ciberdelincuencia, siendo el objetivo de este documento facilitar la toma de decisiones a las Autoridades encargadas de la lucha contra la ciberdelincuencia.

El propio director de Europol, Rob Wainwright[36] , manifiesta que la expansión de la ciberdelincuencia es una amenaza a la seguridad europea, y muestra su preocupación por cómo estos delincuentes saben utilizar la dependencia de los usuarios de las TIC, por otro lado, señala también que en respuesta a ello las distintas Policías, están mejorando en lo que se refiere a cooperación policial cada vez más, ayudados por el EC3, pero a su vez advierte

[33]MEDINA LINÀS, Manel. *Cibercrimen: ¡protégete del "bit-bang"!, los ataques en el ciberespacio a tu ordenador, tu móvil, tu empresa: aprende de víctimas, expertos y cibervigilantes.* Barcelona: Tibidabo, 2015. Pág.33.

[34] Ob. Cit. VELASCO SAN MARTÍN, Pág. 73.

[35] EUROPEAN POLICE OFFICE. *Internet Organised Crime Threat Assessment (IOCTA) 2016*. [En línea]. 2016. <https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf> [Consulta: 14 marzo 2017].

[36]https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime

que, la utilización por los grupos criminales de servicios de cifrado legales, usados para la actividad delictiva, y los que le aportan anonimato, dificultan en gran medida las investigaciones policiales.

En el IOCTA se hace una detallada evaluación sobre los últimos ciberdelitos, su dimensión y sus víctimas, poniendo en duda la calidad de las medidas de seguridad que se ponen por parte de usuarios y empresas para minimizar estos riesgos. En este documento, se establecen resultados de investigaciones sobre *malware*, *hackeos* y *Darknets* y se incluyen acciones en tres áreas, los ciberataques, la explotación sexual infantil on line y los fraudes informáticos a la vez que se identifican las principales tendencias de la ciberdelincuencia:

1. **Ransomware**. El ramsomware, es actualmente la amenaza de malware más preocupante, por encima de *spyware* y troyanos bancarios, y se prevé que continúe así, lo que provocó que las fuerzas policiales y sectores de la industria se volcaran en minimizar sus riesgos, mediante campañas de concienciación y prevención. El uso de los teléfonos móviles está provocando que se desarrollen malware móvil para afectar a estos dispositivos. En el pasado, el ransomware existente estaba orientado a los usuarios individuales, pero ahora el objetivo ha cambiado y lo que se busca es bloquear la información, principalmente de entidades y empresas. *Véase por ejemplo en ciberataque de 'ransomware' que se extendió a escala mundial el pasado 13 de mayo, afectando a sistemas informáticos de decenas de países (equipos de la sede de Telefónica en Madrid, al sistema de salud británico o el ministerio del Interior ruso, entre muchos otros)*[37].
2. **Explotación sexual infantil *on line***. La utilización de la *Darknet*, el uso de plataformas de cifrado de extremo a extremo para establecer comunicaciones, P2P, los sistemas de pago anónimos, moneda virtual bitcoin ha facilitado un aumento de la existencia del abuso sexual infantil *on line*. Las redes sociales, mediante utilización de técnicas de ingeniería social, destacan como foco de primer orden para la captación de nuevas víctimas.
3. **Pago fraudulento**. Medidas de seguridad como EMV (chip y PIN), geo-bloqueo y otras medidas de la industria dificulta a los delincuentes el fraude con tarjeta en la UE, desplazando a los mismos a realizar sus actividades en otros países de Asia o América del Sur. pero los ataques de *malware* y directamente contra cajeros

[37] Noticias relativa al ataque de "ransomware" de mayo 2017. [En línea]. <http://elpais.com/tag/ataques_informaticos/a> [Consulta: 27 mayo 2017].

automáticos proliferan y siguen evolucionando, al igual que los ataques al uso de las tarjetas no presentes, enfocando las acciones a sectores como el transporte, las pequeñas empresas y la hostelería. Los grupos del crimen organizado están empezando a cometer fraude afectando a las tarjetas sin contacto (NFC). Por lo que se propone que, para luchar contra el fraude con tarjeta presente, hay que mitigar el malware utilizado, sobre todo para obtener datos o dinero en los cajeros automáticos, y transferencias no consentidas en regiones no compatibles con EMV

4. **El robo de datos**. Los datos siguen siendo un producto clave para los ciberdelincuentes, centran sus objetivos tanto en usuarios como empresas, destacando la hostelería, comercios minoristas y últimamente en los registros médicos (información registros sanitarios); mediante el robo de estos datos se obtienen beneficios económicos de forma directa en muchos casos, pero, cada vez más, también se adquieren para realizar fraudes más complejos, el ransomware o directamente para extorsionar.
5. **La ingeniería social**. Ha evolucionado mucho en lo referido al *phishing* orientado ya no solo a usuarios, sino que se tiene constancia que también se han dirigido contra empresas importantes del sector privado. Una variante muy precisa de *spear phishing*, fraude CEO, es la tendencia actual.
6. **Crime-as-a-Service.** Existe un crecimiento del *Crimen-as-a-Service* que interconecta los proveedores especializados de herramientas y servicios de ciberdelincuencia, con un número creciente de grupos del crimen organizado, donde los terroristas también tienen la posibilidad de acceder a este "servicio" en el futuro. Por lo tanto, se trata de delincuentes que ofrecen sus servicios a cambio dinero, utilizando mayormente la "*Deep Web*", para contactar y realizar las operaciones.
7. **Utilización de Darknet**[38]. La utilización de foros o canales encriptados o el uso de la *Darknet*, ha servido para que los ciberdelincuentes o grupos criminales establezcan sus comunicaciones; dificultando de este modo la actividad de las fuerzas de inteligencia policial y el acceso a pruebas esenciales en la investigación. En la *Darknet* se puede disponer de casi todo, como hemos señalado anteriormente

[38] Darknet es una red que forma una pequeña parte de la *deep web* donde todo es anónimo y está cifrado, de tal forma que no es posible entrar en ella con navegadores normales sino con el famoso Tor. Esta red permite que los cibercriminales puedan compartir fácilmente contenidos ilegales sin poder ser rastreados. Por tanto, es habitual que muchas de las prácticas citadas en este informe sean intercambiadas a través de esta red.

lo han utilizado para el intercambio de material de la explotación sexual infantil, además de ser utilizada para otros tipos de actividades ilícitas como el tráfico de drogas o armas. Los grupos criminales tenían técnicas para realizar ciberataques limitadas, pero la disponibilidad de herramientas y servicios para los delitos informáticos que se disponen en la *Darknet*, les ofrece posibilidades de cambio, teniendo que prestas mucha atención a los actores terroristas en este fenómeno. La *Darknet*, engloba un mundo paralelo delincuencial por ello, igual es necesario plantearse dar formación sobre la misma a investigadores de este tipo de delincuencia (drogas, armas, etc.) y no solo a los ciberinvestigadores.

8. **Monedas virtuales**. El *Bitcoin* sigue siendo la moneda de elección para el pago de productos y servicios criminales en la economía sumergida digital y la *Darknet*. *Bitcoin* se suele usar como medio de pago para rescates por ransomware o para los pagos de extorsión.

Recientemente se ha publicado por parte del Centro Criptológico Nacional el informe de "*Ciberamenazas y Tendencias. Edición 2017",* en el que se analizan en el ámbito nacional e internacional las ciberamenazas, por lo que debemos reseñar algunas cuestiones reflejadas en el mismo:

En **ciberdelincuencia**, al igual que el IOCTA destaca la organización de los ataques por ransomware los cuales han incrementado en número y han sido dirigidos posiblemente mediante el uso de "*spear-phising*", teniendo especial incidencia en sector de la energía, sanidad, de telecomunicaciones, entidades financieras o a nivel gubernamental. Afectando también a los dispositivos móviles. Referido a España, señala que "el CCN-CERT gestionó un total de 2.030 incidentes de distintos tipos de ransomware (un 375% más que en 2015)"[39].

El *malware* o código dañino se presenta como forma más habitual con la que se realizan los ciberataques, de forma que "*en 2016, de los 20.940 ciberincidentes gestionados por el CERT Gubernamental Nacional en el sector público y en empresas de interés estratégico, el 53,6% (11.237) correspondían con la tipología de código dañino y, dentro de esta, los troyanos (con el 86,64% de*

[39] CENTRO CRIPTOLÓGICO NACIONAL. "*Ciberamenazas y Tendencias Edición 2017 CCN-CERT IA-16/17".* [En línea]. Madrid,2017. Pág. 14< https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2224-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017/file.html >. [Consulta:03 julio 2017]

los casos) y el ransomware (9,2%) fueron los de mayor incidencia"[40]. Destacando como uno de los procedimientos más eficaces utilizados en las actividades de ilícitas el uso de herramientas de acceso remoto, aunque también contempla que la ingeniería social sigue como una de las técnicas más utilizadas con las que se inician los incidentes, dirigidas a usuarios concretos normalmente usando el *spear-phishing*.

Se aumenta el número de ataques DDoS seguidos de extorsión, englobándose en el conocido como *Crimen-as-a-Service,* aumentando también la afectación a los teléfonos móviles. La propagación de malware mediante publicidad engañosa en web famosas ha contribuido a la gran difusión de estos entre sus usuarios.

Destaca que las medidas preventivas como la **actualización del software** de los equipos y dispositivos sigue siendo tarea pendiente, lo que hace muy vulnerable a los sistemas, al igual que la escasez de medidas de seguridad que se detectan en la pequeña y mediana empresa.

Del mismo modo, el informe también viene a señalar como una de las amenazas más importantes el **ciberespionaje** tanto de carácter económico como político, afectando el primero la propiedad intelectual de empresas públicas y privadas, y el segundo detectado entre estados.

[40] Ibíd. Pág. 46

3. MARCO JURIDICO

Antes de comenzar, se debe centrar qué tipo de legislación afecta al universo de estudio, la ciberdelincuencia. Es importante dejar claro que, como se ha venido reseñando, el desarrollo de las TIC que ha experimentado la sociedad, ha supuesto una evolución en muchas facetas, de forma que este fenómeno provoca la discusión entre si nos encontramos ante una forma autónoma de delincuencia, por lo que se estaría hablando de la existencia de un "delito informático" independiente o, por otro lado, si simplemente nos encontramos con los mismos delitos, pero utilizando para su comisión las TIC. Lo que parece claro es que el concepto de delito informático suscita no pocos debates entre juristas, como quedó reflejado en epígrafes anteriores.

Pero antes de entrar en esa problemática, se debe hacer un análisis completo de la legislación que puede afectar a España. Para ello, hay que tener en cuenta tanto la legislación nacional, como los Convenios Internacionales y los Acuerdos establecidos en el marco de la Unión Europea y que vinculan el ordenamiento jurídico nacional. Con la intención de hacer el estudio lo más comprensible posible, se va a hacer un análisis inverso de la legislación internacional, para descender después a la legislación nacional.

3.1.- Ciberseguridad y ciberdelincuencia

Antes de comenzar con el análisis normativo, es importante hacer un pequeño paréntesis para explicar la diferencia entre ciberseguridad y ciberdelincuencia, puesto que, a pesar de hacer referencia a ambos términos tanto en la introducción como en el epígrafe anterior, a lo largo del presente capítulo se va a hablar en profundidad de ambas, y es necesario tener claro las diferencias entre éstas, a modo de resumen:

- La **ciberseguridad** tiene como objetivo mantener la disponibilidad e integridad de las redes y la confidencialidad de la información que contienen infraestructuras. Por tanto, abarca las salvaguardias y medidas que pueden utilizarse para proteger el ciberespacio, en los ámbitos tanto civil como militar, de las amenazas inherentes a sus redes interdependientes e infraestructuras de información, o que pueden dañarlas.
- La **ciberdelincuencia**, implica el desarrollo de una actividad delictiva, en la que los ordenadores y los sistemas de información se utilizan como principales herramientas para delinquir o son objeto principal del delito. La ciberdelincuencia,

por tanto comprende delitos tradicionales, delitos relacionados con los contenidos y delitos exclusivos de ordenadores y sistemas de información[41].

Por tanto, la ciberseguridad es un concepto mucho más amplio, y del que la ciberdelincuencia forma parte cuando es una de las causas de la vulneración de esa seguridad. De este modo, es necesario hablar de ella, ya que sienta bases y es referenciada como marco general en normativas que afectan de igual modo a la ciberdelincuencia.

3.2.- Marco normativo internacional

A nivel internacional la primera referencia que existe, la cual goza de mayor aceptación, ha sido la realizada por el Consejo de Europa a través del **Convenio sobre la Ciberdelincuencia**, el cual ha sido abordado por su importancia anteriormente.

Otra de las herramientas internacionales que se creó fue el **Convenio Europeo de Asistencia Judicial en Materia Penal**, es el número 030 del Consejo de Europa, hecho en Estrasburgo el 20 de abril de 1959.

En este Convenio se regula el compromiso, entre países firmantes, a prestarse la asistencia judicial en materia penal cuya infracción fruto de la represión, es competencia de la parte requirente. Este Convenio no es aplicable a infracciones de carácter militar, que no formen parte del Derecho Penal Común. Por tanto, este Convenio establece los procedimientos y requisitos de las **Comisiones Rogatorias Internacionales**.

3.3.- Marco Normativo de la Unión Europea.

La UE lleva trabajando muchos años en varias áreas para asegurar la seguridad en las redes y de la información, para asegurar la confianza de los usuarios, la prosperidad y el desarrollo económico de la misma. En el año 2010, con el objetivo de obtener un máximo rendimiento de las TIC, la Comisión Europea adoptó el 19 de mayo, la denominada **Agenda Digital para Europa**[42]. En ella, al abordar el tema de la confianza y seguridad,

[41]Como son los delitos de fraude, falsificación, usurpación de identidad, pornografía infantil, terrorismo, incitación al odio, ataques contra los sistemas de información, la denegación de servicio, programas maliciosos, etc.

[42] COMISIÓN EUROPEA. Comunicación dirigida al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM [2010] 245 final), "*Una Agenda*

muestra su preocupación por el incremento de la ciberdelincuencia. Por ello, pone especial énfasis en la necesidad de afrontar esta amenaza y reforzar la seguridad en la sociedad digital. De forma que en su desarrollo indica la necesidad de establecer un centro europeo de la ciberdelincuencia y una plataforma europea dentro de las acciones a realizar, proponiendo en las dos acciones clave 6 y 7, reforzar en 2010, la política de seguridad de las redes y de la información, mejorando ENISA (Agencia Europea de Seguridad de las Redes y de la Información) para dotarla de mayor capacidad de respuesta ante un ciberataque, además de incluir un CERT (equipo de respuesta a emergencias informáticas) para instituciones de la UE; en la misma línea y para combatir los ciberataques contra los sistemas de información establecer medidas, incluyendo las legislativas y poniendo como fecha tope el año 2013 para presentar una normativa sobre la jurisdicción en el ciberespacio a nivel europeo e internacional.

3.3.1.- Líneas estratégicas en la Unión Europea.

En el ámbito de la seguridad interior, la UE actúa a través de las políticas comunes, la legislación y la cooperación práctica en materia judicial y policial, la gestión de fronteras y la gestión de crisis, de manera que contar con la contribución de las políticas internas y de las políticas exteriores de la UE, es de vital importancia para la consecución de nuestros objetivos de seguridad.

En consecuencia, la Estrategia de Seguridad Interior de la UE en acción presenta una agenda común para los Estados miembros (EEMM), el Parlamento Europeo, la Comisión, el Consejo, las agencias y otros organismos, incluida la sociedad civil y las autoridades locales. Dicha Estrategia pretende ofrecer respuestas a los retos de seguridad de nuestro tiempo, al mismo tiempo que contribuye a reforzar y desarrollar el modelo europeo de economía social de mercado propuesto en la Estrategia de Europa 2020.

La vigente **Estrategia Europea de Seguridad Interior**, identifica los principales riesgos y amenazas para la seguridad de la UE en los próximos años, "*como el terrorismo, la delincuencia organizada grave, el tráfico de drogas, la ciberdelincuencia…, se adaptan muy rápidamente a la evolución científica y tecnológica, en su intento de aprovecharse ilegalmente y socavar los valores y la*

Digital para Europa" [En línea]. 2010. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245&from=ES > [Consulta: 11 abril 2017].

prosperidad de nuestras sociedades abiertas"[43]. Entre ellos, cabe destacar dos que afectan directamente al contenido del presente estudio como son la Ciberdelincuencia y en la parte que nos puede afectar el terrorismo y la delincuencia organizada y grave.

En esta Estrategia Europea de Seguridad Interior se hace un llamamiento a la Comisión para que proponga medidas de aplicación de la estrategia, de ahí que en noviembre de 2010 se adopta la Comunicación *"**La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura**"*, para proponer acciones que pusieran en práctica la Estrategia durante el período 2011-2014.

El citado documento establece cinco objetivos estratégicos y acciones específicas para contribuir a mejorar la seguridad de la UE. Dado que el objetivo del presente trabajo no es hacer un análisis exhaustivo de dicha Estrategia, nos centraremos en aquellos que más afectan a la Ciberseguridad y la Ciberdelincuencia.

Así pues, resulta destacable el OBJETIVO 3 señalado en dicha estrategia, referido a *"Aumentar los niveles de seguridad de los ciudadanos y las empresas en el ciberespacio"* [44]. En este objetivo se reitera, lo que venimos abordando a lo largo del presente trabajo, al igual que reconoce la Agenda Digital para Europa sobre la importancia de la seguridad en este ámbito por la influencia de las TIC en muchos ámbitos, la globalidad de la ciberdelincuencia, los conflictos jurisdiccionales del ciberespacio, etc. provoca la necesidad imperiosa de que los EEMM realizan esfuerzos de forma conjunta.

En búsqueda de lograr este objetivo la Comunicación, propone tres acciones:

- En primer lugar, identificándola como la primera línea de acción (LA1), el propio documento estratégico señala la necesidad de ***reforzar la acción represiva y el***

[43]SECRETARIA GENERAL DEL CONSEJO DE EUROPA. *Estrategia de Seguridad Interior de la Unión Europea: Hacia un modelo europeo de seguridad.* Oficina de Publicaciones de la Unión Europea [En línea]. Luxemburgo: ISBN 978-92-824-2680-7 doi:10.2860/881. 2010, Pág. 7. <https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ESC.pdf> [Consulta: 11 abril 2017].

[44]COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo y el Consejo. *La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura.* COM (2010) 673 final. [En línea]. Bruselas, 2010. Págs. 10-11.< http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0673&from=ES > [Consulta: 11 abril 2017].

poder judicial. Para ello, propone la creación de un centro de la ciberdelincuencia a más tardar en 2013[45], con el objetivo fundamental de aumentar las capacidades operativas y analíticas para la investigación y la cooperación, estableciendo entre sus misiones la mejora de las medidas preventivas y de investigación existentes, la formación y sensibilización sobre la acción represiva y la cooperación con ENISA y con la red de CERTs. Todo ello, para constituirse como referencia de la lucha contra la Ciberdelincuencia en Europa.

En este mismo orden de cosas, la propia UE obliga a los EEMM a garantizar unas normas comunes para la investigación y persecución de esta de delincuencia para los actores implicados en su lucha. Igualmente, instando a su vez a los EEMM a mejorar su formación sobre la misma apoyándose para ello en los otros sectores como la industria y los académicos.

- Como LA2, establece ***trabajar con la industria para capacitar y proteger a los ciudadanos***, en la que se propone crear un sistema que garantice la comunicación de incidentes relacionados con la ciberdelincuencia, acceso posterior a las medidas preventivas a adoptar y la elaboración de directrices sobre cooperación para tratar los contenidos ilegales de Internet.
- La LA3, consistente en ***mejorar la capacidad para tratar los ataques informáticos***. En este sentido, la UE señala necesidad de mejorar las medidas sobre la prevención, la detección y la reacción rápida de ciberataques o de interrupción informática, obligando al establecimiento de CERT,s a los EEMM e instituciones de la UE, de forma que cooperen en la prevención y reacción con las autoridades encargadas de la lucha contra la delincuencia, conectando conjuntamente los EEMM sus CERT nacionales en la red. Todo ello, con el objetivo último de desarrollar un sistema europeo de intercambio de información y alerta (EISAS) para el usuario, así como el establecimiento de una red de puntos de contacto entre los organismos competentes y los EEMM.

A la vista de estas premisas, se establece que la capacidad de la UE de enfrentarse a la ciberdelincuencia se verá reforzada con el establecimiento del Centro Europeo de Ciberdelincuencia (EC3) en EUROPOL y la adopción de la directiva relativa a los ataques

[45] En 2013 la UE creó el Centro Europeo de Ciberdelincuencia (EC3) en el marco de Europol, se abordará en epígrafes posteriores, junto con otros organismos e instituciones.

contra los sistemas de información. Estas propuestas formarán parte de la Estrategia Europea de Ciberseguridad.

3.3.2.- Estrategia de ciberseguridad de la Unión Europea.

Durante los siguientes años se llevaron a cabo la mayor parte de los objetivos marcados, habiéndose elaborado por parte de la Comisión Europea la *"**Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro**"*[46], desarrollada en Bruselas, el 7 de febrero de 2013.

La propia estrategia afirma que la UE y los EEMM para luchar contra la ciberdelincuencia necesitan una normativa eficaz y que el Convenio sobre la Ciberdelincuencia, de 2001 se constituye en el marco idóneo para su transposición a normativa interna.

En la Estrategia se proponen una serie de medidas para que los países de la UE y los sectores privados (*incluidos los proveedores de Internet*), lleven a cabo una cooperación efectiva.

Todos los Gobiernos de la UE podrían responsabilizarse de prevenir y responder a las amenazas a las redes digitales, tendrían que cumplir normas comunes sobre ciberseguridad y aumentar la cooperación en la lucha contra la ciberdelincuencia. Por ello, la Estrategia de ciberseguridad establece cinco prioridades estratégicas para resolver los problemas de ciberseguridad, siendo la segunda de ellas: *"**Reducir drásticamente la ciberdelincuencia**"*.

Para alcanzarla, la Estrategia analiza la situación y conoce de la necesidad de contar con los instrumentos necesarios para abordar el rápido perfeccionamiento de los ciberdelincuentes, que se aprovechan del anonimato y la carencia de fronteras, siendo imprescindible la cooperación internacional para las autoridades encargadas de su represión. Por ello, la UE afirma que se debe hacer lo siguiente:

[46]COMISIÓN EUROPEA. Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones. *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*. JOIN (2013) 1 final. [En línea]. Bruselas, 2013. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:ES:PDF.>
[Consulta: 13 abril 2017].

- Establecer una normativa estricta y eficaz. Se debe trasponer y aplicar las directivas relativas a la ciberdelincuencia, se insta a la ratificación y aplicación del Convenio sobre la ciberdelincuencia.
- Mayor capacidad operativa para luchar contra la ciberdelincuencia. Se insta a que todos los EEMM cuenten con unidades nacionales especializadas en la lucha contra la ciberdelincuencia, que sin duda mejorarán sus capacidades. Para ello, se colaborará estrechamente con **EUROJUST** y con el **EC3**.
- Mayor coordinación en la UE. Señalando la importancia de trabajar de forma coordinada y colaborativa por los EEMM, haciendo participes a las autoridades policiales y judiciales, así como a las partes interesadas de los sectores público y privado de la UE y del exterior.

  En cuanto a esa mayor coordinación dentro de la UE, la Comisión se marca una serie de objetivos que es necesario referenciar:

  - Apoyar al EC3 como centro de referencia en la lucha contra la ciberdelincuencia[47]. Pedir a EUROPOL (EC3) que elabore periódicamente informes estratégicos y operativos sobre tendencias y amenazas incipientes.
  - Aumentar la exigencia de responsabilidad y exactitud de información a los registradores de nombres de dominio y titulares de sitios web, conforma a la legislación y sobre todo en lo relativo a la protección de datos.
  - Solicitar a la **Escuela Europea de Policía** (**CEPOL**) que en cooperación con EUROPOL, se aporte una formación apropiada a las autoridades policiales.
  - Pedir a EUROJUST que investiga las dificultades en la cooperación judicial en este tipo de investigaciones, impulse la coordinación entre los EEMM y con terceros países.
  - Solicitar a EUROJUST y a EUROPOL (EC3) que en el ámbito de sus atribuciones exista entre ambos la cooperación y el intercambio de información necesario.

[47] El EC3 proporcionará análisis e información, respaldará las investigaciones, aportará conocimientos
forenses de alto nivel, facilitará la cooperación, creará canales de intercambio de información entre las autoridades competentes de los Estados miembros, el sector privado y otras partes interesadas, y se convertirá progresivamente en portavoz de la comunidad de cuerpos de seguridad.

Dentro de la Estrategia de ciberseguridad se establecen tres pilares: el de la Seguridad de las redes y la información, el de los Cuerpos de Seguridad (asociada a este pilar, normalmente, la ciberdelincuencia común) y la Defensa; tal y como muestra la siguiente figura, aquí existen diferentes marcos jurídicos, según el tipo de ciberincidente que tenga lugar (nacional, europea e internacional). Además, se debe tener en cuenta la necesaria colaboración con el mundo académico y el sector privado (industria), ya que a este último pertenece un grupo tan importante como son los proveedores de servicios.

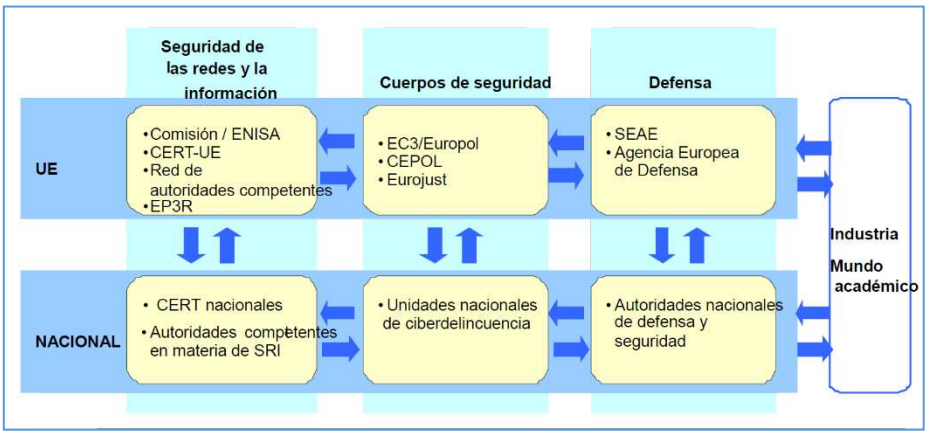

Figura 7.- *Pilares de la Estrategia de ciberseguridad de la UE. (Fuente: Comisión Europea)*

La vinculación que existe entre el pilar que es de interés para este trabajo (el de la ciberdelincuencia, por ende el de los Cuerpos de Seguridad) y el resto de pilares, radica en el hecho de que los ciberincidentes que tengan origen delictivo, deberán ser dirigido hacia a EUROPOL (EC3), para que junto con las autoridades policiales de los países afectados (las unidades nacionales especializadas en la ciberdelincuencia), puedan iniciar una investigación, conservar las pruebas, identificar a los autores y velar por que se castigue el delito. Para ello, también se debería lograr la coordinación con el sector privado, habida cuenta de la importancia de su colaboración.

Tal y como marcaba la Agenda Digital para Europa, durante el año 2013 se elaboró la **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**[48], la cual tiene como objetivos armonizar la norma penal de los EEMM en esta materia, a través de la

[48]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. [En línea]. < http://www.boe.es/doue/2013/218/L00008-00014.pdf >. [Consulta: 14 abril 2017].

determinación de infracciones penales y sanciones, e impulsar la cooperación entre los autoridades competentes, Cuerpos de Seguridad y otras autoridades de los EEMM que velen por el cumplimiento de la ley, y por parte de la UE aquellos organismo implicados como EUROJUST, EUROPOL (EC3) y ENISA. Asimismo, se remarca la necesidad de la cooperación público-privada y la participación de los propios usuarios, para la prevención y represión, además de la necesidad de impulsar la cooperación entre las autoridades policiales y judiciales con el sector Industria (proveedores de servicios, productores...)[49].

En dicha normativa, se vuelve a reiterar que debe ser prioritario el proceso de ratificación del Convenio sobre la Ciberdelincuencia de 2001 por todos los EEMM.

En base a las consideraciones señaladas, entre otras, la Directiva lleva acabo una armonización en la tipificación de ciertas conductas delictivas, estableciendo las siguientes infracciones penales (Arts. 3-8):

1. **Acceso ilegal a los sistemas de información**. Acceso sin autorización de forma intencionada y violentando alguna medida de seguridad.
2. **Interferencia ilegal en los sistemas de información**. Obstaculización o interrupción de forma intencionada y sin autorización.
3. **Interferencia ilegal en los datos**. Borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos de forma intencionada y sin autorización.
4. **Interceptación ilegal**, de forma intencionada y sin autorización, de transmisiones no públicas de datos informáticos, a través de medios técnicos.
5. **Uso instrumentos para comisión infracciones anteriores**. Se penan una serie de actividades (producción, venta o adquisición, importación, distribución…) que se realizan sin autorización y cuya finalidad es proporcionar instrumentos para su posterior uso en la comisión de las anteriores infracciones penales.
6. **Inducción**, **complicidad y tentativa**. Para todos los casos anteriores se podrá aplicar la inducción y la complicidad. En cuanto a la tentativa sólo será aplicable en las interferencias ilegales de sistemas de información y/o datos.

[49]Dicha cooperación podría incluir el apoyo prestado por los proveedores de servicios al contribuir a mantener posibles pruebas, a proporcionar elementos que ayuden a identificar a los infractores y, en última instancia, a cerrar, total o parcialmente, los sistemas de información o la supresión de las funciones que hayan creado una situación de peligro o se hayan utilizado con fines ilegales.

Asimismo, se establece una normalización procesal al establecer unos canales de **intercambio de información**, de aplicación a los seis tipos de infracciones penales anteriormente citados. Para ello, los EEMM deben contar con un punto de contacto nacional incluido en la **Red 24/7**, que estableció el Convenio sobre la Ciberdelincuencia.

3.3.3.- Agenda Europea de Seguridad.

En el año 2015, se establece la **Agenda Europea de Seguridad** que viene a sustituir o ampliar a la Estrategia adoptada en 2010 (*Estrategia de Seguridad Interior, donde se proponían acciones para 2011-2014).* En esta Agenda Europea de Seguridad, la Comisión Europea fija la estrategia con la que la Unión hará frente a las amenazas a la seguridad en la UE durante el período 2015-2020.

La Agenda aborda las amenazas del terrorismo, la delincuencia organizada[50] y la **ciberdelincuencia**, destacando la interconexión existente entre ellas y su carácter transnacional, constituyéndose como las tres prioridades para la seguridad europea. Por ello la Agenda pretende ayudar a los Cuerpos de Seguridad de los distintos EEMM a proceder con mayor eficacia al intercambio de datos y a mejorar su cooperación en la lucha contra la delincuencia transfronteriza, de forma que se insta a los EEMM a recabar el apoyo de las agencias de la UE, impulsando y proponiendo las siguientes medidas:

- Facilitar el intercambio de información entre las autoridades policiales y judiciales y las agencias de la UE.
- Mejorar la cooperación policial operativa: *Equipos conjuntos de investigación (ECI)*[51]*, agencias como EUROPOL, EUROJUST…*
- Impulsar la formación y la cofinanciación de la seguridad a nivel de la UE: *CEPOL.*

En lo referido a la lucha contra la Ciberdelincuencia la Agenda, deja claro que la prevención es muy importante en la lucha contra la ciberdelincuencia al considerar que "*la*

[50] Como señala la Agenda, se integra también en el terrorismo y la ciberdelincuencia a través de canales como el suministro de armas, la financiación mediante el tráfico de drogas, y la infiltración de los mercados financieros.

[51] Los ECI reúnen agentes de policía de varios EEMM durante un período determinado para investigar casos concretos de índole transfronteriza. La Comisión Europea fomentará un recurso más sistemático a los ECI por parte de los EEMM y se asegurará de que los terceros países participen en esos casos.

ciberseguridad *es la primera línea de defensa*"[52], por lo que hace referencia a la Estrategia de ciberseguridad de la UE de 2013 e insiste en la necesidad de la cooperación con el sector privado para subsanar deficiencias y mejorar la formación específica, señalando a su vez la importancia de la Directiva de 2013 sobre seguridad de las redes y de la información, con la mejora de capacidades en ciberseguridad de los EEMM y cooperación entre FCSE y autoridades de la ciberseguridad, así como la importancia de ENISA.

La Agenda reseña que es primordial **garantizar la plena aplicación de la legislación vigente de la UE.** La ciberdelincuencia, por sus características, exige que las FCSE sean ágiles y flexibles en sus acciones de prevención e investigación, de forma que impone que las autoridades judiciales reconsideren las formas de cooperación en su jurisdicción para buscar la rapidez en el intercambio de información y acceso a las pruebas. Del mismo modo que nos situamos en un marco en el que se exige una gran capacitación para enfrentarse a este tipo de delincuencia, mediante la formación y respuestas globales en las que además de las FCSE nacionales, puede ser necesario la participación del EC3, los CERT de los EEMM que puedan resultar afectados o el sector privado a través de los proveedores de servicios, que en última instancia pueden avisar y proteger a los usuarios.

La Agenda propone reforzar la capacidad de las autoridades judiciales y policiales, insistiendo en que el EC3 debe ser el núcleo de información central para las FCSE en este ámbito y pretende suprimir los obstáculos a las investigaciones penales en materia de ciberdelincuencia, especialmente en lo que se refiere al acceso a las pruebas, con la continuidad de las funciones de EUROJUST.

Las acciones que la Agenda propone en este ámbito, además de mejorar como siempre los instrumentos de cooperación internacional, son: impulsar las políticas de ciberseguridad y ciberataques, mejorar la legislación para luchar contra el fraude y falsificación informática y revisar las dificultades existentes en ámbito procesal sobre temas de jurisdicción y acceso a información y a las pruebas.

[52]COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo y al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. "*Agenda Europea de Seguridad*". COM (2015) 185 final. [En línea]. Estrasburgo, 2015. Pág. 22 < http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0185&from=EN .> [Consulta: 15 abril 2017].

3.3.4.- Directiva NIS

Como venimos reseñando, la UE va legislando con el objetivo de garantizar una mayor seguridad en el ciberespacio, Agenda Digital en 2010, Estrategia de Ciberseguridad en 2013… y como complemento a éstas la **Directiva (UE) 2016/1148** del Parlamento Europeo y del Consejo, de 6 de julio de 2016, **relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión**"[53].

Esta Directiva conocida como la Directiva NIS, tiene por objeto armonizar el nivel de seguridad de las redes y sistemas de información entre los EEMM de la UE, con la pretensión de que sea alto, para ello fija los requisitos mínimos comunes en seguridad y notificación que deben cumplir los operadores de servicios esenciales y los proveedores de servicios digitales, obliga a los EEMM a establecer una estrategia nacional, en lo referido a la cooperación, se establece un Grupo de cooperación y se crea una red de equipos de respuesta a incidentes de seguridad informática (CSIRT), además obliga a los EEMM a designar autoridades competentes, puntos de contactos y CSIRT. En definitiva, insta a lo siguiente:

- Identificación de los operadores de servicios esenciales[54] y los proveedores de servicios digitales[55] de los EEMM a los que también les exige unos requisitos en materia de seguridad y notificación de incidentes.
- Las autoridades competentes y/o CSIRT, deben recibir la notificación de incidentes con efecto perturbador significativo por parte de los operadores de servicios esenciales y de proveedores de servicios digitales, debiendo determinar si pueden tener efecto transfronterizo, y cuando éstos puedan tener como origen la acción

[53] DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016, *relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*. [En línea]. < http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES >. [Consulta: 15 abril 2017].

[54] Energía: (electricidad, petróleo, gas); Transporte: aéreo, marítimo, ferrocarriles y carreteras; Banca (entidades de crédito); Infraestructuras del mercado financiero; Sector sanitarios (incluyendo hospitales y clínicas privadas) Suministro y distribución de agua potable; Infraestructuras digitales (puntos neutros, proveedores de servicios de DNS y registros de nombres de dominios).

[55] Mercado en línea; Motor de búsqueda en línea; Servicios de computación en nube.

delictiva se instará a que operadores y proveedores notifiquen directamente a la autoridad policial.

- Adopción de una Estrategia nacional de seguridad de las redes y sistemas de información.
- Designación de una o más autoridades competentes y del punto de contacto único en materia de seguridad de las redes y sistemas de información, con la posibilidad de que los EEMM asignen estas funciones a autoridades ya existentes, de forma que los primeros se encarguen de las cuestiones de aplicación en ámbito nacional de la directiva y las circunstancias sobre la notificación de incidentes, y el punto de contacto ejercerá funciones de enlace con las Autoridades competentes de los EEMM, el Grupo de cooperación y la Red de CSIRT garantizando las cooperación transfronteriza.
- Designación de uno o varios Equipos de respuesta a incidentes de seguridad informática (CSIRT), que llevaran el peso de la gestión de incidentes.
- Garantizar la cooperación en ámbito nacional., de forma que si la autoridad competente, el punto de contacto único y los CSIRT son distintos, deberán cooperar para garantizar el cumplimiento de la Directiva, relativo a notificación incidentes, información a los puntos de contacto…
- Continuando en el capítulo de cooperación a escala internacional. Establecimiento del Grupo de Cooperación. Integrado por la Comisión, ENISA y representantes de los EEMM, el cuál asumirá funciones de cooperación estratégica, intercambio de información y buenas prácticas, etc. Establecimiento de una Red de CSIRT, formada por representante de los CSIRT de los EEMM En la cual los EEMM, con diversas funciones como el intercambio de información, respuesta coordinada a un incidente, etc.

3.3.5.- Ámbito judicial- procesal.

En el ámbito judicial-procesal existe el **Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea**[56], hecho en Bruselas

[56] CONSEJO DE EUROPA. Acto del Consejo por el que se celebra, de conformidad con el artículo 34 del Tratado de la Unión Europea, el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea. Bruselas, 29 mayo de 2000. (2000/C 197/01). [En línea]. Bruselas, 2000. < http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:C2000/197/01&from=ES .> [Consulta: 11 abril 2017].

el 29 de mayo de 2000. Este Convenio viene a complementar otros Convenios sobre este ámbito entre los que se encuentra el Convenio europeo de asistencia judicial en materia penal de 1959, regulando para los países de la UE herramientas tan importantes como los Equipos Conjuntos de Investigación o las Investigaciones encubiertas (donde actúan los agentes encubiertos).

Como última normativa a tener en cuenta en el ámbito de la UE, existe la **Directiva 2006/24/CE**, del Parlamento europeo y del Consejo, **sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones**[57], comporta un profundo cambio de los principios básicos de la protección de datos personales.

Como se viene reseñando una de las características de la ciberdelincuencia es el anonimato y la deslocalización, por lo que como es evidente los datos de tráfico y localización de las comunicaciones son de suma importancia para las investigaciones de esta actividad delictiva, por ello, mediante esta Directiva se pretende que los EEMM pongan en común las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, garantizando de esa forma su posterior explotación en caso de ser necesario por autoridades policiales o judiciales. Por ello, los proveedores de servicios de comunicaciones electrónicas deben conservar los datos que permitan identificar el origen, el destino, la fecha, hora y duración de una comunicación electrónica, el tipo de comunicación realizada, el equipo utilizado y la localización de dicho equipo.

Por tanta la Directiva se aplicará solo a los datos de tráfico y de localización sobre personas físicas y jurídicas, a efectos de identificación, no al contenido de las

[57]DIRECTIVA 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*. [En línea]. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF>. [Consulta: 15 abril 2017].

comunicaciones. Se concede a los Estados amplias facultades de control, garantizando así la disponibilidad de datos para investigación, detección y enjuiciamiento.

3.4. Marco normativo nacional

En el ordenamiento jurídico español existen una serie de normas que afectan directamente a la lucha contra la ciberdelincuencia. Se va a hacer un análisis de la normativa desde lo más general, donde se verán las directrices y el marco de actuación que existe, para luego descender a las normas que definen qué acciones son consideradas ilícitos penales y cómo se debe investigar los hechos, para poder obtener las pruebas contra los criminales que los llevan a cabo.

La primera referencia que se posee es el **Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia**, publicado en el BOE núm. 226, de17 de septiembre de 2010. Como ya se ha explicado, su importancia es fundamental para lograr una lucha eficaz a nivel internacional contra la ciberdelincuencia.

3.4.1.- Estrategia de Seguridad Nacional.

Si analizamos las líneas estratégicas nacionales, debemos referenciar la **Estrategia de Seguridad Nacional de 2013[58](ESN)**, que es un documento público elaborado por el Gobierno de España, en el que se actualiza la Estrategia del año 2011, y por el que se analiza la seguridad española en el marco internacional, de manera que tras la identificación de las debilidades, riesgos y amenazas, se establece el marco estratégico donde se marcan objetivos a conseguir mediante diversas líneas de acción que se consideran fundamentales para España.

En su desarrollo la ESN, señala entre los varios riesgos que afectan a España destacando, por su influencia para este trabajo el terrorismo, el crimen organizado y las ciberamenazas.

Sobre las ciberamenazas, en la ESN se muestra la preocupación del Gobierno de España muestra su preocupación en este ámbito, ya que es consciente de la evolución de las actividades que se desarrollan en el ciberespacio y de la dependencia que se tienen de

[58] GOBIERNO DE ESPAÑA. *Estrategia de Seguridad Nacional.* [En línea]. Madrid, 2013. <http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf> [Consulta: 6 marzo 2017].

éstas que además de otorgarnos beneficios y facilitar las cosas, nos expone sin duda a situaciones de riesgo.

Haciendo un repaso a esta amenaza, expone algunas de sus características, como su fácil acceso, deslocalización y ausencia de fronteras, anonimato, coste y riesgo bajo, así como las carencias en cuanto a legislación sobre ciberseguridad, señalando que estos ataques pueden afectar tanto a particulares como instituciones, siendo la amenaza variada englobando además del ciberdelito, el ciberespionaje o el ciberterrorismo. Entre los sujetos activos de esta amenaza se encuentran desde personas aisladas hasta Estados, pasando como no por grupos criminales o terroristas o las propias empresas, aunque no se puede descartar que los fenómenos naturales o motivos técnicos puedan afectar a la ciberseguridad.

Todo lo anterior y con el convencimiento de que este tipo de amenazas seguirán proliferando, consideran prioritario garantizar la seguridad de los sistemas que gestionan infraestructuras críticas o servicios muy utilizados.

Una vez situadas las amenazas, la ESN, establece cuáles serán los campos de actuación, marca el objetivo a conseguir en cada uno de ellos y establece las LA,s para lograrlos.

LUCHA CONTRA EL TERRORISMO	Neutralizar la amenaza que representa el terrorismo y reducir la vulnerabilidad de la sociedad ante sus ataques, haciendo frente a los procesos de radicalización que lo puedan preceder o sustentar.
CIBERSEGURIDAD	Garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques.
LUCHA CONTRA EL CRIMEN ORGANIZADO	Impedir el asentamiento de los grupos criminales organizados, poner a disposición de la justicia a los que ya operan dentro de nuestras fronteras e impedir la consolidación de sus formas de actuación delincuencial.

Figura 8.- *Objetivos principales de Terrorismo, Ciberseguridad y Crimen Organizado de la ESN. (Fuente: Gobierno España)*

En cuanto a las LA,s en ciberseguridad se establecen seis, buscando el incremento de seguridad especialmente en lo referido a infraestructuras críticas y servicios esenciales, aumentando las capacidades de prevención, detección, respuesta e investigación de ciberataques, implantar el Esquema Nacional de Seguridad, aumentar la colaboración entre el sector público y privado lo que sin duda provocara aumento de la seguridad y resiliencia de las TIC, alentar la formación especializada en materia de ciberseguridad, concienciar a

los usuarios de la importancia de las medidas preventivas y como no puede ser de otra forma, impulsar la cooperación internacional, buscando la armonización en esta materia.

En lo referido a la Delincuencia Organizada, por sus características, el carácter transfronterizo de éstos, se señala que las LA,s deben estar marcadas por la cooperación internacional tanto en ámbito público como en el privado, destacando la LA que busca que la lucha contra el crimen organizado sea de forma coordinada y con dirección centralizada, para aumentar la eficacia policial y reforzando la colaboración con la autoridad judicial y ministerio Fiscal.

En materia de la lucha contraterrorista, entre las distintas LA, remarca en el pilar de la prevención que se debe evitar que los grupos terroristas se aprovechen del ciberespacio para realizar actividades de proselitismo, radicalización o logro de objetivos.

3.4.2.- Estrategia de Ciberseguridad Nacional.

Dentro de la ESN se establece la promoción de otras estrategias que correspondan, de manera que la **Estrategia de Ciberseguridad Nacional** es el documento que viene a cumplimentar las acciones necesarias para cubrir el ámbito de las ciberamenazas.

El propósito de la Estrategia de Ciberseguridad Nacional, en coherencia con la ESN y con las iniciativas desarrolladas en el ámbito europeo, internacional y regional, que hemos comentado anteriormente, es fijar las directrices para el uso seguro del ciberespacio, impulsando una visión integradora, a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas entre ellas, con el sector privado y con los ciudadanos.

La Estrategia de Ciberseguridad Nacional, se sustenta e inspira en los Principios Rectores de "Liderazgo nacional y coordinación de esfuerzos, Responsabilidad compartida, proporcionalidad racionalidad y eficacia y cooperación internacional".

Esta estrategia comparte el objetivo global a lo señalado en la ESN sobre ciberseguridad, "*lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques*"[59], señalando además diversos objetivos parciales, de los que derivas las LA,s.

[59] Ob. Cit. GOBIERNO DE ESPAÑA. *Estrategia de ciberseguridad Nacional.* Pág. 21.

Para alcanzar este objetivo y la seguridad del ciberespacio, la Estrategia promueve el oportuno desarrollo normativo, así como que todos los agentes e instituciones responsables en la materia trabajen de forma coordinada bajo la cobertura de una estructura que beneficie a la mejora de las capacidades. Por supuesto la Política de Ciberseguridad Nacional se posicionará en la misma línea que la de nuestros semejantes, instituciones europeas e internacionales y concretamente, con la Estrategia de Ciberseguridad de la UE.

Como objetivos parciales se marca los reflejados en la figura siguiente.

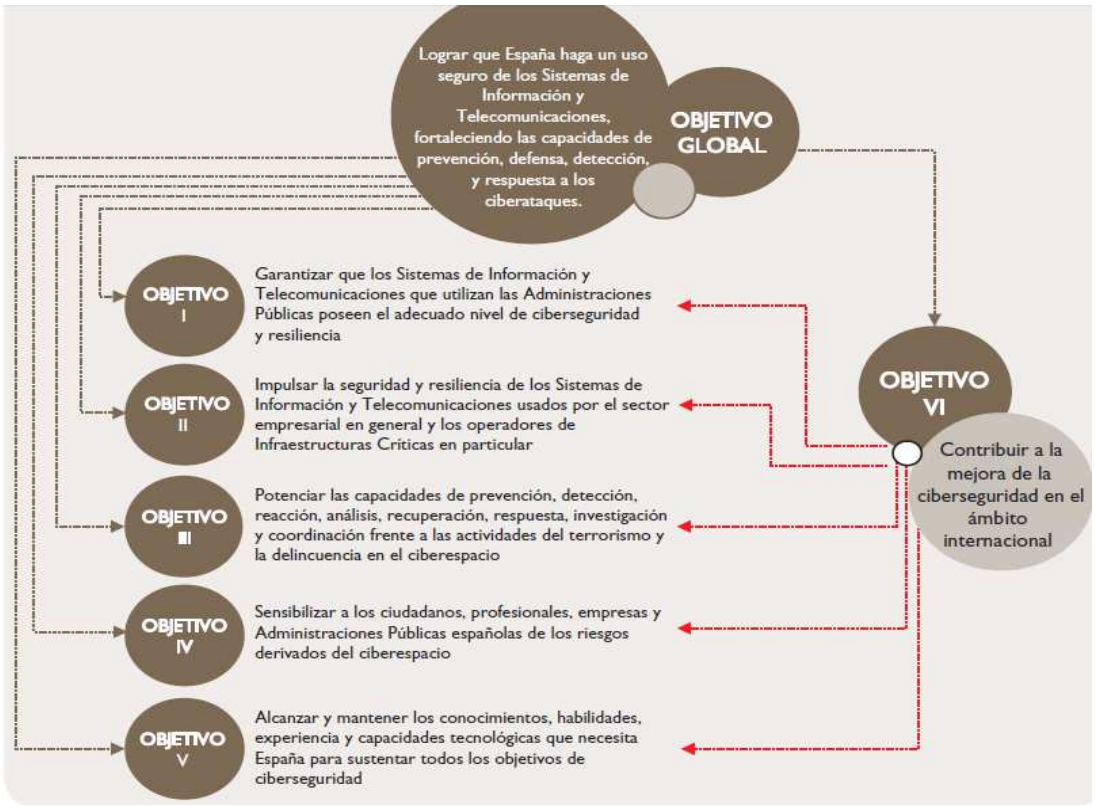

Figura 9.- *Objetivos de la Estrategia de Ciberseguridad Nacional. (Fuente: Gobierno España)*

Al igual que sucede con otros documentos estratégicos, una vez fijados los objetivos a alcanzar, se deben describir las **líneas de actuación** que conducirán a los mismos. Así pues, el propio documento estable cuales deben ser dichas líneas. En la siguiente figura se enumeran las LA, haciendo posteriormente hincapié en aquellas que impactan directamente en el tema de estudio, la Ciberdelincuencia.

	LINEA DE ACCCIÓN	CONTENIDO
1	**Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas**	Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las Ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
2	**Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas**	Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
3	**Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas**	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
4	**Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia**	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
5	**Seguridad y resiliencia de las TIC del sector privado**	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
6	**Conocimientos, Competencias e I+D+i**	Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de Ciberseguridad.
7	**Cultura de ciberseguridad**	Concienciar a los ciudadanos, profesionales y empresas de la importancia de la Ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
8	**Compromiso internacional**	Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

Figura 10.- *Líneas de Acción de la Estrategia de Ciberseguridad Nacional. (Fuente: Gobierno España)*

En las distintas LA se aborda el incremento de las capacidades preventivas, de detección y de resiliencia, así como de respuesta ante los incidentes, también la necesaria cooperación entre los organismos responsables en la materia tanto públicos como privado y con los órganos con capacidad de respuesta y las unidades especiales de las FCSE, la implantación del Esquena Nacional de Seguridad, revisar la normativa de protección de infraestructuras críticas para garantizar tanto la seguridad en el aspecto físico como en el tecnológico, el desarrollo de un Marco de conocimientos en ciberseguridad no solo en el aspecto técnico, sino también en el operativo y en el jurídico, y como no podía ser de otra forma la necesaria cooperación internacional que requiere esta materia, en los distintos ámbitos, tanto de armonización legislativa como en el policial, judicial y de intercambio de información.

A la vista de las líneas fijadas por la Estrategia, se observa como el número cuatro impacta directamente en el objeto de este trabajo, puesto que aborda la "*capacidad de*

investigación y persecución del ciberterrorismo y la ciberdelincuencia". Esta LA4 se concentra en las actividades delictivas que operan en el ciberespacio utilizando éste tanto como medio para alcanzar sus objetivos o como fin de los mismos.

En esta LA4, se plantean diversas medidas a adoptar, como es la integración en el marco jurídico de cuestiones de ciberseguridad sobre todo lo concerniente al ámbito penal y la labor de los órganos competentes, se tiene consciencia de la necesidad de que los organismos competentes en la investigación de los delitos en ciberespacio, aumenten sus capacidades y mejoren su coordinación con las propias del ámbito de la ciberseguridad, mediante la fluidez del intercambio de conocimientos entre ambos, en relación al ámbito internacional se insiste en reforzar la cooperación policial y también se pretenden hacer partícipes a los propios usuarios buscando la implicación de estos de forma que se plantean canales para que aporten información que pueda ser de utilidad para la actividad policial. Por último, se otorga importancia al conocimiento de esta materia para hacer frente a su lucha, de forma que se insta a facilitar la instrucción en materia de ciberseguridad en los ámbitos policiales y de la autoridad judicial y fiscalía, para poder aplicar los mismos en la parte operativa, legal y técnica.

En esta línea de acción se hace referencia a "*organismos con competencias en la investigación y persecución del Ciberterrorismo y la Ciberdelincuencia*", los cuales serán abordados en epígrafes posteriores, además de otros con competencias en Ciberseguridad.

3.4.3.- Código Penal.

Es fundamental nombrar la **Ley Orgánica 10/1995**, de 23 de noviembre, del **Código Penal**[60], el cual ha venido recibiendo varias reformas en cumplimiento a las obligaciones internacionales en esta materia por lo que debemos señalar:

1º.- **Reformas penales del año 2010**: siendo en este año cuando España ratificó el Convenio sobre Ciberdelincuencia.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal[61].

[60] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [En línea] < http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html > [Consulta: 17 abril 2017]

- Por esta Ley se incorpora al Derecho español, entre otras normas de la UE la Decisión Marco 2005/222/JAI[62], relativa a los ataques contra los sistemas de información. En su preámbulo apartado XIV señala que motivada por la Decisión Marco, en referencia a los delitos informáticos se deben incorporar varias conductas ilícitas tanto en lo referido a los daños como al descubrimiento y revelación de secretos.
- Se incluye dentro del artículo de descubrimiento y revelación de secretos (**artículo 197**), el denominado "***Hacking***" a través del apartado 3, de Sistemas, programas o datos informáticos; donde se castiga el intrusismo e interceptación de las comunicaciones a través de la red, por tanto, castiga a quien acceda y utilice un sistema informático ajeno de forma no autorizada.
- Se introduce el denominado "***Cracking***" a través del **artículo 264**; Daños a Sistemas, programas o datos informáticos. En definitiva, se castiga los daños graves que se causen a través de internet, agravando las penas en caso de que se trate de organizaciones criminales o sea una persona jurídica (una sociedad) la responsable del delito. Castigando con la reforma de este artículo el ciberterrorismo y el vandalismo digital.
- También se modifica el **artículo 248**, incluyendo entre las estafas la utilización de tarjetas bancarias o sus datos en perjuicio de otros, aumentando las ya existentes y en la que ya se referenciaba la "manipulación informática"
- Con la creación del artículo 183 bis, se regula el denominado internacionalmente "*child grooming*"[63], donde se castiga a la persona que desarrolla conductas mediante

[61]Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal. [En línea] < https://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf > [Consulta: 17 abril 2017]

[62]CONSEJO DE LA UNION EUROPEA. *Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.* [En línea]. 2005. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ES:PDF> [Consulta: 14 abril 2017].

[63] Childgrooming puede ser **definido** como una práctica por la cual "*un adulto (generalmente un depredador sexual) contacta con un menor a través de redes sociales o valiéndose de Internet para crear un vínculo afectivo, intentando ganarse la confianza del mismo, para concertar una cita con claros fines sexuales*"; en BIURRUN ABAN, Fernando J. Los riesgos de las nuevas tecnologías. *Actualidad jurídica Aranzadi.* 2016, Nº 921, pág.: 28.

internet, el teléfono u otra TIC para ganarse la confianza de menores de trece años buscando concertar encuentros para obtener concesiones de índole sexual.

2º.- **Reformas penales del año 2015**:

Ley Orgánica 1/2015, y **Ley Orgánica 2/2015**, ambas de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal[64].

- Por la Ley Orgánica 1/2015 se incorpora al Derecho español, entre otras normas de la UE, la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información, que sustituye a la Decisión Marco 2005/222/JAI[65].
- La reforma que se realiza es amplia y con mucha afectación a las TIC, como señala en su preámbulo apartado XIII, buscando alinearse al marco europeo y cubrir las reconocidas carencias penales en este ámbito. De este modo las principales reformas en nuestro objeto de estudio fueron:
- **Relativos a descubrimiento y revelación de secretos de sistemas, programas o datos informáticos, se producen las siguientes reformas:**
  - Se modifica el **artículo 197.** Se aborda el descubrimiento y revelación tanto de secretos o datos que vulneran la intimidad como los reservados de carácter personal. Se castiga la difusión, revelación o cesión de esos datos tanto al que participa activamente en su descubrimiento como al sujeto que, sin haber participado en éste, conozca de su origen ilícito y realiza esas actividades. En su último apartado, castiga las conductas en las que se difunden imágenes o grabaciones sin la oportuna autorización de la persona afectada, que menoscaben gravemente a la intimidad de esa persona, cuando éstas se obtuvieron previamente con el debido consentimiento en el círculo apropiado.
  - Se introduce el **artículo 197 bis.** Donde se tipifica el acceso o la facilitación para el acceso a datos del sistema de información o mantener en el mismo sin autorización; y en el párrafo 2 se castiga la interceptación no autorizada de transmisiones no públicas de datos de un Sistema de información.

[64] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [En línea] <https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf > [Consulta: 17 abril 2017]

[65] En esta Directiva se marcaba que los EEMM estaban obligados a incorporarla a su ordenamiento jurídico nacional a más tardar el 4 de septiembre de 2015.

- Se introduce el **artículo 197 ter.** Castiga la producción, adquisición, facilitación de programas informáticos, códigos o equipos diseñados para la intrusión en Sistemas

- **Relativos a daños informáticos:**
  - **Artículos 264 y 264 bis,** con la modificación del primero y la creación del segundo se regula de forma separada los supuestos de daños informáticos y las interferencias en los sistemas.
  - **Artículo 264 ter,** se castiga la facilitación/producción de programas informáticos o equipos diseñados o adaptados para la comisión de otros delitos informáticos.
- **Relativos a Propiedad Intelectual:**
  - **Artículo 270;** en su párrafo 2 se introduce la tipificación de las Páginas de enlace castigando a las que sin autorización de los titulares facilitan el acceso o localización de obras o prestaciones objeto de propiedad intelectual.
- **En relación al ejercicio de los derechos fundamentales y libertades públicas:**
  - **Artículo 510.** Se produce una agravación de conductas de Incitación al odio y a la violencia que, al poder obtener mayor publicidad, se realicen por medios de comunicación social, Internet u otras TIC.
- **Relativos a delitos contra la libertad sexual y protección de menores:**
  - Se introduce el **artículo 183 ter**, para proteger a los menores de dieciséis años de manera que castiga al que trate de contactar con éstos, mediante internet u otras TIC con la intención de realizar los actos que describen los arts. 183 y 189 y en el segundo apartado se castiga al que utilice esos mismos medios con objeto de engatusar al menor para que le proporcione imágenes o material porno gráfico relativo a menores.
  - Se modifica el **artículo 189**, se incluye en el apartado 1, la definición de pornografía infantil. Además de castigar la adquisición o tenencia de pornografía infantil y se incluye un apartado que sanciona al que accede por medio de las TIC con conocimiento, a este tipo de pornografía.

Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal[66].

[66]Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de

- A través de esta Ley Orgánica se adapta la legislación penal española, en virtud a la Resolución 2178 del Consejo de Seguridad de las Naciones Unidas[67].
- Esta reforma supone un paso muy importante para la prevención de la difusión del terrorismo yihadista a través de internet y otras TIC, puesto que en esas reformas que afectan a los delitos de terrorismo contenidos en los artículos 571 al 580, introducen el "delito informático" como delitos de terrorismo con en el **artículo 575** que tipifica como delito de terrorismo, adoctrinamiento/adiestramiento, el "acceso habitual" mediante internet o TIC a determinados contenidos que "*estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines"* o también el que con el mismo fin, posea documentos de ese tipo.
- En lo relativo a los delitos de enaltecimiento, justificación o actos de descrédito, menosprecio o humillación de las víctimas del terrorismo del **artículo 578**, así como la difusión de mensajes o consignas para incitar a otros a la comisión de delitos de terrorismo, se produce un agravamiento cuando estos actos se difundan mediante o por medio de internet, TIC, etc.

Como observamos en el Código Penal español no se halla un título específico que contenga los delitos que se puedan definir como "informáticos" o ciberdelitos sino que se hace referencia a aquellos delitos cuyo objeto son los sistemas informáticos o TIC, se sirven de éstos para su ejecución o por su complejidad exige la metodología de investigación informática[68].

Actualmente, los tipos penales del Código Penal español que más se aproximan a lo que refleja el Convenio sobre la Ciberdelincuencia, y a modo de organizarlos un poco, en virtud de la catalogación que se realiza en la Instrucción 2/2011 dictada por la Fiscalía General del Estado son:

noviembre, del Código Penal. [En línea]< https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3440.pdf > [Consulta: 17 abril 2017].

[67] NACIONES UNIDAS. Resolución 2178 del Consejo de Seguridad. 24 de septiembre de 2014 [En línea] <http://www.un.org/en/sc/ctc/docs/2015/N1454802_ES.pdf> [Consulta: 17 abril 2017].

[68] Tal es el caso de los delitos de terrorismo a través de las TIC, blanqueo de capitales, etc.

I. Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC.
    a. Descubrimiento y Revelación de Secretos. Artículo 197.
    b. Ataques/interceptación sistemas y datos. Artículo 197 bis y ter
    c. Daños informáticos (sabotaje, denegación…). Artículo 264, 264bis y 264 ter.
    d. Descubrimiento y Revelación Secretos Empresa. Artículo 278 y ss.
    e. Contra servicios de radiodifusión /interactivos. Artículo 286.

II. Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TIC.
    a. Abusos y agresiones sexuales a menores. "*Grooming*". Artículo 183ter.
    b. Corrupción de menores/Pornografía infantil. Artículo 189.
    c. Estafa. Artículo 248 y 249.
    d. Defraudaciones. Artículos 255 y 256.
    e. Propiedad Intelectual /Industrial. Artículo 270 y ss.

III. Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TIC, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia.
    a. Amenazas/coacciones. Artículo 169 y ss. y 172 y ss.
    b. Contra la Integridad Moral (*mobbing*, *bullyng*, acoso) Artículo 172 ter y 173.1.
    c. Injurias y calumnias. Artículo 211 y ss.
    d. Falsificación documental. Artículo 399 bis y 400.
    e. Apología/Incitación, delitos de Odio. Artículo 510 y ss.

3.4.4.- Otras Leyes.

A continuación, se van a enumerar una serie de Leyes que, si bien afectan a la investigación de esta tipología delictiva, no son fundamentales para la misma, por lo que simplemente se hará una breve referencia al objeto de creación de las mismas. Se ha de hacer constar que alguna de estas normas, surge como necesidad de transposición de normas europeas que deben regularse a nivel nacional.

- ✓ **Ley Orgánica 15/1999**, de 13 de diciembre, **de Protección de Datos de Carácter Personal**[69].

  Tiene como objetivo la regulación de lo referido al tratamiento de datos personales, para proteger y garantizar los derechos fundamentales de las personas físicas, especialmente su derecho al honor y a la intimidad personal y familiar.

  En esta regulación del tratamiento de datos de carácter personal, se disponen unas obligaciones y unos requisitos mínimos de seguridad a cumplir por parte aquellos que dispongan de este tipo de datos, ya sean personas físicas o jurídicas; así como los derechos de los titulares de estos datos.

- ✓ **Ley 34/2002**, de 11 de julio, **de servicios de la sociedad de la información y de comercio electrónico**[70].

  El desarrollo de la Sociedad de la información y el aumento del uso de las TIC para realizar comercio electrónico, hace necesario que en cierto modo se regule este tipo de actividades para que las mismas se puedan realizar de forma segura y con confianza por parte de los usuarios y empresas. Esta ley establece el marco jurídico para regular esta materia en cuanto a las obligaciones de los proveedores de servicios e intermediarios de estos en la transmisión de contenidos a través de la Red y en lo referido a la realización de un comercio electrónico seguro.

- ✓ **Ley 39/2015,** de 1 de octubre**, del Procedimiento Administrativo Común de las Administraciones Públicas**[71].

---

[69]Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. [En línea] <http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html. > [Consulta: 17 abril 2017].

[70] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [En línea]. < http://noticias.juridicas.com/base_datos/Admin/l34-2002.html. > [Consulta: 17 abril 2017].

[71] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [En línea] < http://noticias.juridicas.com/base_datos/Admin/559951-l-39-2015-de-1-oct-procedimiento-administrativo-comun-de-las-administraciones.html > [Consulta: 17 abril 2017].

En lo referido al uso de los medios electrónicos son de interés las previsiones relativas a los derechos de las personas en sus relaciones con las Administraciones Públicas, derecho y obligación de relacionarse electrónicamente con las mismas, asistencia en el uso de medios electrónicos a los interesados; la representación y los registros electrónicos de apoderamientos, etc. Esta Ley deroga la **Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos.**

- ✓ **Ley 40/2015,** de 1 de octubre**, de Régimen Jurídico del Sector Público**[72]

Se puede destacar lo establecido en relación con los principios generales, los órganos colegiados, su capítulo V "Funcionamiento electrónico del sector público", gestión compartida de servicios comunes, técnicas de colaboración, transmisiones de datos entre AA.PP., Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad, reutilización de sistemas y aplicaciones de propiedad de la Administración y transferencia de tecnología entre Administraciones.

- ✓ **Ley 25/2007**, de 18 de octubre, **de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**[73].

Esta Ley integra en el ordenamiento jurídico español la Directiva 2006/24/CE, del Parlamento europeo y del Consejo, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones*, con el mismo objeto que ya fue comentado anteriormente.

- ✓ **Real Decreto 3/2010**, de 8 de enero, **por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica**[74].

---

[72] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [En línea] <http://noticias.juridicas.com/base_datos/Admin/559952-l-40-2015-de-1-oct-regimen-juridico-del-sector-publico.html > [Consulta: 18 abril 2017]

[73] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. [En línea] < http://noticias.juridicas.com/base_datos/Admin/l25-2007.html. > [Consulta: 18 abril 2017]

[74] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el

La *Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos*, estableció el Esquema Nacional de Seguridad, (ENS) que, aprobado mediante el **Real Decreto 3/2010,** tiene por objeto garantizar la protección de la información fijando principios y requisitos de seguridad, que serán aplicados por las AA.PP. en la utilización de medios electrónicos que gestione dicha información. Posteriormente, la Ley 40/2015 *de Régimen Jurídico del Sector Público*, recoge el ENS en su artículo 156.2 en similares términos.

En 2015 se publicó la modificación del ENS a través del Real Decreto 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, en especial de la UE, de las TIC y de la experiencia de la implantación del ENS.

- ✓ **Real Decreto 4/2010**, de 8 de enero, **por el que se regula el Esquema Nacional de Interoperabilidad en el Ámbito de la Administración Electrónica**[75].

Ley 11/2007, estableció en el artículo 42.1 el Esquema Nacional de Interoperabilidad (ENI) regulado por este Real Decreto, posteriormente en la Ley 40/2015, lo recoge en su artículo 156.1.

El ENI, con el fin de garantizar el oportuno nivel de interoperabilidad en los datos, informaciones y servicios que gestionan la AA.PP., establece los criterios comunes relativos a seguridad, conservación de datos, aplicaciones y formatos que deben ser considerados por las mismas.

- ✓ **Ley 9/2014**, de 9 de mayo, **General de Telecomunicaciones**[76].

En la misma línea que la Agenda Digital para Europa, pretende que el marco jurídico aporte seguridad para el mejor desarrollo de las telecomunicaciones.

ámbito de la Administración Electrónica. [En línea] < http://noticias.juridicas.com/base_datos/Admin/rd3-2010.html > [Consulta: 18 abril 2017].

[75] Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el Ámbito de la Administración Electrónica. [En línea] < http://noticias.juridicas.com/base_datos/Admin/rd4-2010.html > [Consulta: 18 abril 2017].

[76]Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [En línea] < http://noticias.juridicas.com/base_datos/Admin/529091-l-9-2014-de-9-may-telecomunicaciones.html > [Consulta: 18 abril 2017]

Deroga la *Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones*, siendo su objeto la regulación de las telecomunicaciones, aborda cuestiones sobre la explotación, la prestación de servicios y recurso asociados, incluyendo cuestiones de interés como el secreto de las comunicaciones y protección de datos, la interceptación legal de las telecomunicaciones, en los referido a la conservación y cesión de datos en ocasiones remite a la Ley 25/2007, sobre la que también realiza modificaciones, o en su Título IV la evaluación de conformidad de equipos y aparatos.

Modifica la reseñada Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico, siendo relevante lo añadido en sus disposiciones adicionales, que hacen referencia:

- La cancelación o suspensión cautelar de los nombres de dominio mediante los que se cometan actividades delictivas, por parte de la autoridad de asignación, por requerimiento judicial o a requerimiento de las FCSE mediante diligencia de prevención en las 24 horas siguientes al conocimiento del delito.
- La colaboración de los registros de nombres de dominio establecidos en España, facilitando los datos a las autoridades competentes.
- Sobre gestión de incidentes de ciberseguridad se establece la obligación de colaboración con el CERT competente en la resolución de incidentes y se insta al intercambio eficaz de información sobre amenazas, incidentes y vulnerabilidades para la Protección de infraestructuras críticas entre la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y la Secretaría de Estado de Seguridad.

3.4.5.- Ámbito procesal.

Por último, se debe enumerar las normas que afectan al ámbito procesal de una investigación, puesto que son el marco en el que judicialmente se va a mover una unidad de investigación.

- ✓ **Real decreto** de 14 de septiembre de 1882 por el que se aprueba la **Ley de Enjuiciamiento Criminal** (**LECrim**)[77].

En este sentido se destacan las últimas modificaciones del año 2015, la **Ley Orgánica 13/2015**, de 5 de octubre, **de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica**[78], para alinearse con la normativa europea y disponer de nuevas técnicas de investigación.

Como mayores novedades y en relación al objeto de estudio de este trabajo, introduce la adaptación de la legislación a la delincuencia en los que juega un papel importante las tecnologías (modificación del artículo 579, incorporación del artículo 579 bis; la creación en el Título VIII del Libro II los nuevos capítulos IV al X o el agente encubierto informático). A continuación, enumeramos algunas, aunque se abordarán de forma más amplia en otro epígrafe:

- Se regula el registro de sistemas informáticos y dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos.
- Se aborda el tema de la intervención e interceptación de las comunicaciones telefónicas y telemáticas. La incorporación al proceso de datos electrónicos de tráfico o asociados. Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad (direcciones IP, identificación de terminales mediante captación de códigos de identificación del dispositivo o sus componentes, la titularidad o identificación de un dispositivo electrónico).
- Se prevé la extensión de la figura del agente encubierto, para adaptarse a las exigencias de las investigaciones on-line, regulándose la figura del agente encubierto informático.

[77]Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal. [En línea] < http://noticias.juridicas.com/base_datos/Penal/lecr.html > [Consulta: 20 abril 2017].

[78] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. [En línea] < http://noticias.juridicas.com/base_datos/Penal/560107-lo-13-2015-de-5-oct-modificacion-de-la-ley-de-enjuiciamiento-criminal-para.html > [Consulta: 20 abril marzo 2017].

- ✓ **Ley 11/2003**, de 21 de mayo, **reguladora de los Equipos Conjuntos de Investigación penal en el ámbito de la Unión Europea**[79].

Cuando se constituyen equipos conjuntos de investigación para desarrollar investigaciones penales, entre dos o más EEMM de la UE, y se da la circunstancia que la creación sea solicitada por alguno de éstos y en el mismo tenga participación la autoridad española competente o las actividades del referido equipo conjunto tengan lugar en territorio español, será esta ley la encargada de regular de esa constitución.

[79] Ley 11/2003, de 21 de mayo, reguladora de los Equipos Conjuntos de Investigación penal en el ámbito de la Unión Europea [En línea] <http://noticias.juridicas.com/base_datos/Admin/l11-2003.html> [Consulta: 20 abril 2017].

4.- ORGANISMOS, AGENCIAS Y UNIDADES IMPLICADAS EN LA LUCHA CONTRA LA CIBERDELINCUENCIA

Para continuar con nuestro trabajo, en el que venimos señalando que para hacer frente a la ciberdelincuencia son esenciales varias medidas como la cooperación operativa en ámbito policial, judicial y de fiscalía, el intercambio de información, operaciones internacionales, la cooperación entre sectores público y privado, etc. en el presente epígrafe vamos a reseñar algunos organismos con competencias en Ciberseguridad, así como organismos y unidades competentes en la investigación y persecución de la ciberdelincuencia.

4.1.- Interpol

La mayor organización policial que existe, es INTERPOL (Organización Internacional de Policía Criminal), fundada en 1923 con ámbito internacional y que actualmente la forman 190 países, intentado hacer frente a la delincuencia mediante la colaboración de sus miembros.

INTERPOL también colabora en la persecución de la ciberdelincuencia, colaborando con sus miembros mediante la formación en esta materia, apoyando investigaciones con el desarrollo de nuevas tecnologías, coordinación, análisis de evidencias digitales, etc. Colaborando también mediante la elaboración de documentos estratégicos o de inteligencia operativa sobre ciberdelincuencia.

Dispone de un centro de investigación, el **Complejo Mundial de INTERPOL para la Innovación**[80] (“*INTERPOL Global Complex for Innovation*”, en adelante IGCI), donde se encuentran las capacidades y herramientas que INTERPOL pone a disposición de sus miembros para la persecución de este tipo de delincuencia, su ámbito de trabajo se dirige mayormente a la seguridad digital (investigación, análisis de ciberataques, fomento de la ciberseguridad, etc.), la capacitación y formación, así como al apoyo operativo y ayuda a la investigación (coordinación de investigaciones, intercambio operativo de información, etc.).

[80] https://www.interpol.int/es/Internet/Acerca-de-INTERPOL/El-Complejo-Mundial-de-INTERPOL-para-la-Innovaci%C3%B3n [Consulta: 5 mayo 2017].

También cuenta con el *CyberFusion Centre* (CFC), que con la visión de expertos de varios ámbitos (Cuerpos de Seguridad, sector privado, industria), realiza trabajos de inteligencia mediante el análisis de información sobre la ciberdelincuencia, que posteriormente trasladan a las autoridades policiales para su oportuna explotación operativa.

4.2.- El Centro Europeo de Ciberdelincuencia (EC3)

El Centro Europeo de Ciberdelincuencia (EC3)[81], inició su actividad el 1 de enero de 2013[82], con el objetivo de luchar contra la ciberdelincuencia, reforzando de este modo la respuesta policial de los EEMM a este fenómeno en la UE.

Encuadrado en EUROPOL, el EC3 forma parte de una serie de medidas destinadas a protegernos de la ciberdelincuencia, complementando propuestas legislativas, como la Directiva 2005/222/JAI, relativa a los ataques contra los sistemas de información[83] y la **Directiva 2011/92/UE** relativa a la lucha contra la explotación sexual de la infancia en Internet y la pornografía infantil, adoptada en 2011[84].

Por encima de todo, el EC3 trata de ser integrador de los países de la UE, prestando apoyo en las investigaciones y poniendo en común la información y los conocimientos técnicos.

El Centro también tiene la misión de facilitar la investigación y el desarrollo, y garantiza el refuerzo de las capacidades de las autoridades responsables de la aplicación de la ley, jueces y fiscales; asimismo, lleva a cabo evaluaciones de las posibles amenazas, que

[81] Centro Europeo de Ciberdelincuencia https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [Consulta: 5 mayo 2017].

[82] COMISION EUROPEA. Comunicación de la Comisión al Consejo y al Parlamento Europeo. "*La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia*". COM (2012) 140 Final. [En línea] Bruselas, 2012. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0140&from=ES > [Consulta: 5 mayo 2017].

[83]Sustituida en agosto 2013 por Directiva 2013/40/UE, ya analizada en el capítulo anterior.

[84]DIRECTIVA 2011/92/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de diciembre de 2011 *relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo*. Diario Oficial de la Unión Europea n° L 335 de 17/12/2011. [En línea] <. http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011L0093&from=ES> [Consulta: 5 mayo 2017].

incluirán análisis, previsiones de tendencias y alertas tempranas; esto es la recopilación de información sobre ciberdelincuencia, procedente de diversos sectores, para elaborar inteligencia que pondrá a disposición de las FCSE de los países de la UE. Además, presta apoyo operativo a los países cuando se solicita y aporta conocimientos técnicos, analíticos y de peritaje forense de alto nivel, en el marco de investigaciones conjuntas.

Para estas funciones se organiza en tres pilares, el estratégico, la investigación forense y la parte de Operaciones. En el área de operaciones orienta su trabajo a la lucha de ciberdelitos de estas características:

- Ciberataques que afectan a infraestructuras críticas y servicios esenciales de la UE.
- Explotación sexual de los menores on line.
- Delincuencia organizada, con atención preferente al fraude informático.

Para estas tareas en el área de operaciones se cuenta con una Unidad de ciberinteligencia (, además del Grupo de Acción contra la Ciberdelincuencia (*Joint Cybercrime Action Task Force,* en adelante *J-CAT*)[85] que aborda las investigaciones de mayor relevancia.

4.3.- Agencia de la Unión Europea para la Formación Policial (CEPOL)

Por el **Reglamento (UE) 2015/2219,** del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, **sobre la Agencia de la Unión Europea para la formación policial (CEPOL) y por el que se sustituye y deroga la Decisión 2005/681/JAI del Consejo**[86], se cambia también la antigua denominación de "Escuela Europea de Policía" y creación de la escuela de la referida Decisión del 2005.

[85]En el J-CAT, participan oficiales de enlace de varios EEMM de la UE y socios de cooperación no comunitarios, complementados con personal de EC3. Los oficiales de enlace cibernético provienen de: Austria, Francia, Alemania, Italia, Países Bajos, España, Reino Unido y además Australia, Canadá, Colombia y Estados Unidos, que está representado por dos el FBI y el Servicio Secreto. Por parte de España se contribuye con un oficial de la Guardia Civil y un miembro de la Escala ejecutiva del Cuerpo Nacional de Policía. <https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce> [Consulta: 5 mayo 2017].

[86] PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. *Reglamento (UE) 2015/2219 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre la Agencia de la Unión Europea para la formación policial (CEPOL) y por el que se sustituye y deroga la Decisión 2005/681/JAI del Consejo*. [En línea]. Estrasburgo, 2015. < http://eur-lex.europa.eu/legal-

Desde el 1 de julio de 2016, la CEPOL ha pasado a denominarse oficialmente **"Agencia de la Unión Europea para la Formación Policial"**, teniendo su sede en Budapest (Hungría).

CEPOL es una agencia de la UE que se dedica a desarrollar, implementar y coordinar la formación dirigidas a agentes policiales, de forma que agrupa una red de centros de formación para estos agentes, aportando la formación de primera mano (instrumentos operativos policiales y judiciales de cooperación internacional, organismos y herramientas, intercambio de información, etc.). Del mismo modo contribuye a la puesta en común de conocimientos entre las FCSE de los EEMM de la UE, e incluso con terceros países sobre cuestiones relativas a las prioridades de la UE en el ámbito de la seguridad.

4.4.- Unidad de Cooperación Judicial (EUROJUST)

La unidad se creó a través de la **Decisión 2002/187/JAI** del Consejo[87], de 28 de febrero de 2002, por la que **se crea EUROJUST para reforzar la lucha contra las formas graves de delincuencia**.

EUROJUST[88] apoya en el marco de investigaciones que afectan a dos o más países de la UE, a la coordinación y cooperación judicial entre las autoridades competentes de los EEMM, cuando las investigaciones se refieren a actividad delictiva considerada grave entre las que se incluye la ciberdelincuencia.

El ámbito de competencia de EUROJUST cubre los tipos de delincuencia y las infracciones de los que es competente EUROPOL en todo momento. De este modo, EUROJUST puede solicitar a las autoridades de los EEMM afectados varias cuestiones como el inicio de una investigación o actuaciones judiciales, la creación de un equipo conjunto de investigación, facilitar información, etc.

content/ES/TXT/PDF/?uri=CELEX:32015R2219&from=ES.> [Consulta: 6 mayo 2017].

[87] CONSEJO DE LA UNIÓN EUROPEA. *Decisión del Consejo de 28 de febrero de 2002 por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.* (2002/187/JAI). [En línea]. Bruselas, 2002. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002D0187&from=ES.> [Consulta: 6 mayo 2017].

[88] http://europa.eu/european-union/about-eu/agencies/eurojust_es [Consulta: 6 mayo 2017].

Para el mejor desarrollo de sus funciones y objetivos Eurojust lleva a cabo numerosas reuniones tanto de coordinación[89], como las articuladas por sus relaciones funcionales[90].

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

ENISA, se crea en el año 2004 y se modifica en 2013[91], es una agencia para ayudar a mantener un elevado nivel de seguridad de las redes y la información, que apoya y refuerza las capacidades de los distintos EEMM y de la UE para prevenir, detectar y dar respuesta a los problemas de seguridad de las redes y la información, de forma que contribuya a la sensibilización y promoción de una cultura de ciberseguridad que garantice confianza a los usuarios, empresas y organismos de la UE.

Entre sus funciones ENISA, desarrolla las siguientes:

- Contribuir en la elaboración de la política y legislación de la UE, asesorando, analizando estrategias o publicando información sobre ciberseguridad, ayudando al establecimiento de normas para gestionar incidentes buscando la normalización, etc.
- Apoya y reforzar las capacidades de ciberseguridad, mediante su asistencia y aportación de conocimiento, impulsando la cooperación entre los distintos actores en la materia, desarrollando y aumentando las capacidades de los distintos CERT, organizando ciberejercicios a escala europea o asesorando a los EEMM que los quieran a nivel interno, etc.
- Buscar la cooperación entre los organismos públicos y aquellos otros actores de interés en la materia ya sean públicos o privados; promoviendo la cooperación entre todos los CERT y CSIRT, el intercambio de conocimientos y lecciones

[89] Se centran en casos concretos y en la que intervienen fiscales, jueces y agentes de policía.

[90] Engloba tanto autoridades nacionales como organismos de la Unión Europea, tales como la Red Judicial Europea, Europol, CEPOL, OLAF, Frontex o la Red Europea de Escuelas Judiciales.

[91] PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. *Reglamento (UE) 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) 460/2004*. [En línea]. Estrasburgo, 2013. Diario Oficial de la Unión Europea n° L 165 de 18/06/2013. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:ES:PDF> [Consulta: 7 mayo 2017].

aprendidas, desarrollo de campañas de concienciación y consejos en materia de ciberseguridad, etc.

Es evidente que ENISA colabora estrechamente con organismos e instituciones de la UE competentes en materia de ciberseguridad, y como no puede ser de otra manera con aquellos dedicados a la lucha contra la ciberdelincuencia, como es Europol y el EC3, con el que intercambia información y lecciones aprendidas, prestando también su asesoramiento cuando estos lo requieran.

Para ENISA, es muy importante la investigación en esta materia por los insta a los EEMM, que inviertan en investigación al ser consciente de la rápida evolución de este campo, para poder adaptarse al mismo ritmo de evolución e incluso poder desarrollar técnicas preventivas. Para poder desarrollar sus funciones, de asesoramiento, formación, etc. Es necesario que la Agencia mantenga una elevada formación y conocimiento de la actualidad referida a la ciberseguridad, debiendo conocer del mismo modo el estado en el que se encuentran nivel de ciberseguridad en la UE en cada momento, debiendo participar esta información los EEMM y las propias instituciones y organismos de la UE, según las oportunas disposiciones normativas.

En la estructura de ENISA, encontramos expertos tanto del sector público como privado, procedentes del sector industria, proveedores de redes o servicios, expertos en ciberseguridad, usuarios, los expertos designados por las respectivas autoridades nacionales, etc. lo que sin duda beneficia para potenciar la cooperación no solo entre EEMM, sino también con el sector privado, el conocimiento de estos expertos aporta la experiencia necesaria para desarrollas las oportunas políticas y legislación que pretende anticiparse a los problemas se ciberseguridad que irán surgiendo.

4.6.- Instituto Nacional de Ciberseguridad (INCIBE)

El Instituto Nacional de Ciberseguridad de España (INCIBE)[92], es el centro nacional de referencia en materia de ciberseguridad, desde finales de 2014 viene a denominarse así en sustitución del antiguo Instituto Nacional de Tecnologías de la Comunicación (INTECO) que venía funcionando desde el año 2006, está en el organigrama del Ministerio de energía, Turismo y Agenda Digital, bajo la dependencia de la Secretaría de Estado para la Sociedad de la Información y Agenda Digital (SESIAD).

[92] INCIBE. https://www.incibe.es/ [Consulta: 7 mayo 2017].

INCIBE, tiene como misión mejorar y reforzar los niveles de ciberseguridad de España a la vez que eleva la confianza digital, para ello realiza actividades de promoción de servicios en materia de ciberseguridad que garantice una mayor privacidad y seguridad en la explotación de las TIC, trata de promover capacidades para la prevención y reacción de incidentes a la vez que insiste en la cultura de la seguridad con campañas de formación y concienciación. En aras de la búsqueda de la mejora INCIBE tiene un gran potencial en lo referido a la investigación de manera que su trabajo posteriormente pueda ser aprovechado por los distintos servicios, y para ello es necesario encontrarse en los foros adecuados, por lo que el Instituto es consciente de la importancia de la coordinación en este ámbito, por lo cuenta con una amplia de redes de colaboradores con los que intercambiar información y experiencia.

Como muestra de la importancia que se otorga a la investigación y a la colaboración, se podría destacar que INCIBE, se adhirió a la Organización Europea de Ciberseguridad ECSO (European Cyber Security Organisation)[93], como punto de contacto oficial y también ha promovido la creación en España de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC)[94], siendo miembro ya de pleno derecho de la ECSO, apostando ambas asociaciones por el impulso del I+D+I de la ciberseguridad tanto en Europa como en España.

La actividad del Instituto se dirige a un público muy diverso por lo que intenta en cierto modo satisfacer las necesidades concretas de cada uno de ellos, a los usuarios le proporciona la Oficina de Seguridad del Internauta (OSI), a la Administración, la red académica y de investigación española (RedIRIS) y las empresas, en especial de servicios esenciales, que hacen uno de las TIC sector les apoya en sus capacidades de prevención, detección y reacción en materia de ciberseguridad, y en lo referido a los profesionales expertos en ciberseguridad trabaja en colaboración con estos cuando es necesario, atendiendo sus demandas.

[93]<https://www.incibe.es/sala-prensa/notas-prensa/el-instituto-nacional-ciberseguridad-representa-los-intereses-nacionales-el >. Más información sobre ECSO en: www.ecs-org.eu. [Consulta: 7 mayo 2017].

[94] RENIC es una asociación sectorial de ámbito estatal basada en membresía que engloba centros de investigación, universidades y otros agentes dedicados a la investigación en materia de ciberseguridad de España. http://www.renic.es/es/index.html [Consulta: 7 mayo 2017].

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

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)[95], con dependencia orgánica de la secretaría de Estado de Seguridad y creado en el año 2007, es el órgano del Ministerio del Interior que realiza el impulso, coordinación y supervisión de las actividades que la SES tiene encomendadas relativas a la Protección de las Infraestructuras Críticas.

Para desarrollar su labor[96], el CNPIC, busca que integración de todos los actores del sistema de Protección de Infraestructuras Críticas, impulsado la participación de éstos y fomentando la confianza, promoviendo a su vez la necesaria cooperación entre sectores públicos y privados para la consecución de sus objetivos.

Para el apoyo en la gestión de incidentes de seguridad TIC en Infraestructuras Críticas, INCIBE actúa como herramienta técnica de CNPIC.

4.7.1.- La Oficina de Coordinación Cibernética del Ministerio del Interior (OCC)

La Oficina de Coordinación Cibernética (OCC) se creó en el año 2014, mediante la Instrucción 15/2014, de la SES, dentro del CNPIC que se configuró desde ese instante como el órgano técnico de coordinación de la SES en materia de ciberseguridad. Su objetivo es conseguir una mayor eficiencia en la gestión de aquellos aspectos de la Estrategia de Ciberseguridad Nacional que se encuentran bajo la competencia del Ministerio del Interior, siendo además el punto natural de interlocución del Ministerio con el CERT de Seguridad e Industria en este ámbito.

Para ello, la OCC cuenta con los oportunos mecanismos de intercambio de información para comunicarse tanto con el CERTSI como con las distintas Unidades tecnológicas de las FCSE, agilizando la difusión de información que pueda ser de interés para cualquiera de las partes.

---

[95] http://www.cnpic.es/index.html [Consulta: 8 mayo 2017].

[96] Reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf [Consulta: 8 mayo 2017].

Las actuaciones que lleva a cabo la OCC se refieren normalmente al intercambio de información en materia de ciberdelincuencia y ciberterrorismo; a la coordinación de acciones de respuesta ante incidentes, integrando las capacidades de las Unidades tecnológicas de las FCSE cuando sea necesario; a la emisión de información de alerta temprana sobre ciberamenazas; a la supervisión en materia de ciberseguridad de los planes de seguridad que conforman el PNPIC y a la participación en proyectos de I+D.

El pasado año, la OCC se constituyó como punto de contacto del Estado Español en el marco de lo prescrito por la Directiva 2013/40/UE de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, en virtud de la Instrucción 2/2016, de 20 de mayo, de la SES[97].

4.8.- Equipo de respuesta a incidentes cibernéticos de seguridad e industria (CERTSI)

En el año 2012, en virtud a la colaboración en materia de ciberseguridad, mediante Acuerdo entre la SES y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (actualmente SESIAD) se constituyó el CERT de Seguridad e Industria (CERTSI). El CERT de Seguridad e Industria (CERTSI)[98], como centro de respuesta a incidentes de ciberseguridad de los Ministerios de ambas Secretarias, Ministerio del Interior y el de Energía, Turismo y Agenda Digital

El CERTSI está coordinado por el CNPIC e INCIBE y técnicamente es operado por INCIBE, por lo que sumando las capacidades de ambos organismos, se constituye como punto de referencia en la resolución técnica de incidentes de ciberseguridad, para los

[97] Sin perjuicio de lo establecido en la Instrucción 15/2014, desarrolla otras funciones específicas para la OCC: Además de constituirse como el punto de contacto nacional ya referido, dispondrá de capacidades de operación 24 horas-día, 7 días-semana; con enlace permanente con las unidades responsables de las FCSE; la OCC se responsabilizará del intercambio de información sobre ciberdelitos con terceros países, y órganos internacionales y de la UE, cuando así se requiera por las autoridades competentes. La Instrucción también establece los procedimientos de comunicación y el establecimiento de un punto único de contacto especializado en cada una de las FCSE.

[98] https://www.certsi.es/sobre-certsi/que-es-certsi [Consulta: 8 mayo 2017].

operadores de infraestructuras críticas, públicos o privados, designados en virtud de la aplicación de la Ley 8/2011, según establece la Resolución de 8 de septiembre de 2015[99].

En 2015 el Consejo Nacional de Ciberseguridad[100], designó al CERTSI, como CERT Nacional para la respuesta a ciberincidentes, por lo que el CERTSI orienta sus capacidades para dar servicio de prevención, detección y respuesta ante incidentes en materia de ciberseguridad de forma permanente, tanto a empresas y ciudadanos, como a la red académica y de investigación tecnológica (RedIRIS), como a operadores estratégicos y de infraestructuras críticas.

4.9.- Centro Criptológico Nacional (CCN)

En el año 2004, mediante el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional[101], se crea este Centro quedando integrado en el Centro Nacional de Inteligencia (CNI), de manera que en el referido RD se establece que comparte director con el CNI y se marcan el ámbito de actuación y funciones del CCN, además de señalar que le será de aplicación todas las disposiciones de la Ley 11/2002, de 6 de mayo, reguladora del CNI[102].

El CCN[103] , se encarga de la seguridad de las TIC de la Administración que incluyan medios de cifra o trabajen con información clasificada, en este sentido el CCN elabora

[99] Resolución de 8 de septiembre de 2015(publicada en el BOE de 18 de septiembre), de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos. http://www.boe.es/buscar/doc.php?id=BOE-A-2015-10060 [Consulta: 10 mayo 2017].

[100] En acuerdo a lo previsto por la ESN, el Consejo Nacional de Ciberseguridad (Comité especializado) es un órgano colegiado de apoyo al Consejo Nacional de Seguridad con la finalidad de informar y asesorar a aquel en el ámbito de la ciberseguridad.

[101] REAL DECRETO 421/2004, *de 12 de marzo, por el que se regula el Centro Criptológico Nacional.* https://www.ccn.cni.es/images/stories/normas/pdf/rd421-2004centrocriptologiconacional.pdf [Consulta: 10 mayo 2017].

[102] LEY 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia https://www.ccn.cni.es/images/stories/normas/pdf/ley_11_2002_reguladora_cni.pdf [Consulta: 10 mayo 2017].

[103]Centro Criptológico Nacional https://www.ccn.cni.es/index.php?option=com_content&view=article&id=1&Itemid=3&lang=es [Consulta: 10 mayo 2017].

normas para garantizar la seguridad TIC en la Administración, forma a especialistas en esta materia, participa en el Esquema Nacional de evaluación y certificación de la seguridad de las TIC, realiza la acreditación del material criptológico con el que se pretenda trabajar, su activación, etc.

4.9.1.- CCN-CERT

En el año 2006 se crea en el CCN un CERT, que viene a denominarse CCN-CERT, constituyendo como Capacidad de Respuesta a incidentes en materia de ciberseguridad de éste, por lo que sus funciones están desarrolladas en la normativa señalada anteriormente, por las que se regulan tanto el CNI, como el CCN así como en el Real Decreto 3/2010, regulador del Esquema Nacional de Seguridad (ENS)[104], modificado por el RD 951/2015 de 23 de octubre.

El CCN-CERT, se constituye como CERT Gubernamental Nacional, con especial implicación en la ciberseguridad de las AAPP, tal como se recogía en la Estrategia de ciberseguridad española, señalando su importancia para la implantación del ENS y donde ya se proponía el refuerzo de su capacidad de respuesta, así como de detección y alerta temprana. Si bien en un principio su ámbito era las AAPP, actualmente entre sus competencias también se encuentra la gestión de los ciberataques que afectan a empresas y organismos a afectan a intereses estratégicos para España.

Por tanto, se encarga de apoyar a éstos a elevar su nivel de ciberseguridad, poniendo a su disposición todas sus capacidades tales como la gestión de incidentes (detección, evaluación, respuesta, eliminación, etc..), sistema de alerta temprana (que busca la anticipación o detección rápida), colabora también en la formación de personal y usuarios en la materia, tratando de concienciarlos en la importancia de las oportunas medidas de seguridad, de forma que también elabora y difunde tanto recomendaciones y guías de seguridad, como informes de inteligencias para los oportunos destinatarios con competencia en la materia.

La capacidad del CCN-CERT de coordinar e intercambiar información con los organismos adecuados fortalecer las capacidades de respuesta a incidentes. Del mismo

[104]Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica http://noticias.juridicas.com/base_datos/Admin/rd3-2010.html#c1 [Consulta: 10 mayo 2017].

modo, se puede requerir el uso de herramientas que pueden no estar disponibles para un solo organismo, sobre todo si se trata de un organismo pequeño o mediano y sí del CERT Gubernamental Nacional.

Entre los incidentes que se consideran prioritarios[105] para el CCN-CERT, entre otros se encuentran los ciberdelitos, la interrupción de servicios, el ciberespionaje, etc.

4.10.- Mando Conjunto de Ciberdefensa (MCCD)

En el año 2013 se crea el Mando Conjunto de Ciberdefensa (MCCD)[106], mediante Orden Ministerial 10/2013, dentro del Estado Mayor de la Defensa de las Fuerzas Armadas.

El MCCD se responsabiliza de garantizar la ciberseguridad en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa, pero no se limita únicamente a la protección infraestructuras militares, sino que deja abierta la posibilidad de que su ámbito de actuación incluya otras redes o sistemas que se le encomiende puesto que, como se señala en la Estrategia de Ciberseguridad nacional, comentada anteriormente, contribuye a aumentar las capacidades ante las ciberamenazas sobre todo de los sistemas que puedan afectar a la Defensa Nacional, por ello es necesaria una elevada y fluida cooperación con el CCN-CERT y el CERTSI.

Por lo tanto si bien el MCCD se centra principalmente en asistir a las infraestructuras militares, dependiendo de si afectase o no a la Defensa Nacional podría tener algún papel en la ciberseguridad de otros ámbitos, no obstante no cabe duda que se trata de otro actor importante al cual habrá que coordinar con el resto de actores, de forma que en lo que al objeto de este trabajo respecta, también puede colaborar con las FCSE entre otros, desde el punto de vista técnico y de intercambio de información.

4.11.- Agencia Española de Protección de Datos (AEPD)

La Agencia Española de Protección de Datos (AEPD)[107] es un organismo público, que en su actividad actúa con independencia de las AAPP, relacionándose mediante el Ministerio de Justicia con el Gobierno.

[105] CCN-CERT https://www.ccn-cert.cni.es/sobre-nosotros/faq.html [Consulta: 10 mayo 2017].

[106] http://www.emad.mde.es/CIBERDEFENSA/ [Consulta: 13 mayo 2017].

La AEPD se creó en 1992 y comenzó a funcionar en 1994 y es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos, garantizando y tutelando el derecho fundamental a la protección de datos de carácter personal de los ciudadanos.

Entre las funciones que desarrolla la agencia y en relación con la materia del presenta trabajo, hay que reseñar el permanente esfuerzo que realiza en materia de proporcionar recursos y herramientas y desplegar iniciativas de sensibilización tendentes a facilitar la adecuada adopción de la normativa por parte de las empresas, poniendo de manifiesto que el cumplimiento de la normativa provoque una mayor seguridad para las mismas. Es decir, en beneficio de la ciberseguridad y por ende la prevención de la ciberdelincuencia, actúa como autoridad reguladora y de control, mediante el análisis y la sanción de los incidentes que puedan surgir.

4.12.- Guardia Civil. Grupo de Delitos Telemáticos

La Guardia Civil afronta la lucha contra los delitos tecnológicos desde dos perspectivas y en su caso como una, considerada "ciberamenazas", de forma que sus Unidades especializadas en investigación tecnológica se encuentran en dos Jefaturas Centrales, la de Información y la de Policía Judicial, motivado porque históricamente se ha dado tratamiento distinto a los fenómenos de delincuencia organizada y de terrorismo, de manera que la respectiva evolución tecnológica de éstos han dado lugar a la ciberdelincuencia y el ciberterrorismo.

En el ámbito del ciberespacio, la aproximación de ambas formas es más patente si cabe, en las que unas se sirven de otras para lograr sus objetivos, (blanqueo de capitales, financiación del terrorismo, etc.). Si bien la finalidad del ciberdelito y el ciberterrorismo es diferente, el medio para conseguirlo es idéntico.

Como se observa en la figura 11, los Órganos Centrales de investigación con los que cuenta la Guardia Civil en esta materia son dos, la Jefatura de Información, en la que se encuentra el Grupo de Ciberterrorismo, encargada de dar el apoyo técnico tan necesario hoy en día en la investigación a través de internet y redes sociales para la lucha contra el

[107] http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php [Consulta: 13 mayo 2017].

terrorismo nacional e internacional y por otro lado la Jefatura de Policía Judicial, que se encarga de la investigación entre otros de la ciberdelincuencia.

Figura 11.-*Organigrama de Unidades de investigación de delitos tecnológicos en la Guardia Civil* [108]

El Grupo de delitos telemáticos (GDT)[109] es la Unidad más especializada en ciberdelincuencia dentro dela Guardia Civil, siendo que su misión fundamental es el desarrollo de investigaciones relacionadas con la delincuencia informática, especialmente de aquellas que por su complejidad técnica, ámbito territorial o novedad en su modus operandi requieran un tratamiento especial en lo que respecta a capacitación técnica.

Dentro de la plantilla que conforma esta Unidad, no todo el personal posee la misma formación, ya que dentro de la Guardia Civil no existen unos cursos específicos, salvo el Curso Básico de Investigación Tecnológica (CBIT), para las distintas áreas específicas que tienen que afrontar los miembros del GDT y el Curso Básico de Policía Judicial, donde se da un mero baño sobre los delitos informáticos.

De este modo, el personal se va formando a través de cursos específicos (análisis forense, dispositivos de telefonía, etc.) que empresas de seguridad, consultoras externas o

[108] Imagen facilitada en la presentación de la Conferencia *"Riesgos de ciberseguridad en entornos corporativos"*, realizada por el Comandante D. Oscar de la Cruz Yagüe, del Grupo de Delitos Telemáticos de la Guardia Civil en la "*JORNADA: Riesgos de Seguridad de la Información en las empresas*" Zaragoza, 15 de diciembre de 2015, organizada por la Confederación de empresarios de Aragón. http://www.ceoearagon.es/docs/Jornada_GC.pdf [Consulta: 16 mayo 2017].

[109] https://www.gdt.guardiacivil.es/webgdt/home_alerta.php [Consulta: 16 mayo 2017].

universidades realizan; incluso se llegan a organizar cursos específicos, en colaboración con estas empresas u organismos, para que puedan ser formados los miembros del GDT.

Dentro del Grupo de Delitos Telemáticos se ha adoptado el esquema de trabajo que se puede derivar del Convenio sobre ciberdelincuencia del Consejo de Europa de 2001 y el protocolo adicional firmado dos años después para incluir los delitos de apología del racismo y la xenofobia. Por lo tanto, para categorizar y estructurar el tipo de delincuencia que investiga el GDT, se han establecido cuatro grandes áreas:

- Relacionados con el contenido y menores, como son la pornografía infantil, abusos sexuales a menores y *grooming, ciberbullying,* etc.
- Delitos de fraude y falsificación informática, en sus distintas versiones como fraudes bancarios y phishing, y fraudes en el comercio electrónico.
- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas, más conocidos como hacking.
- Delitos contra la propiedad intelectual y derechos afines.

Asimismo, el GDT tiene otra serie de cometidos específicos:

- Apoyo técnico del resto de investigaciones de la UCO, tanto en el volcado y clonado de equipos informáticos intervenidos, como cualquier otro apoyo de carácter técnico que se pueda requerir en el desarrollo del resto de operaciones de la Unidad o del resto de Unidades Orgánicas de Policía Judicial (UOPJ).
- Ciberpatrullaje por la red pública.
- Formación del personal especialista de las distintas Comandancias, a través del curso básico de investigación tecnológica, CBIT.
- Dirección técnica de sus Unidades periféricas, en cuanto a las investigaciones que lleven y soliciten su apoyo al GDT.
- Es el punto de contacto de la Guardia Civil para la cooperación internacional en el ámbito de la ciberdelincuencia, por lo que tendrá el contacto directo con EUROPOL, y más concretamente con el EC3. También es punto de contacto con INTERPOL.
- Es miembro de Grupos de trabajo de INTERPOL, tanto en Europa como en Latinoamérica, en el Foro internacional del G-8 para el cibercrimen (siendo punto de contacto 24/7 para apoyos internacionales) y en el de EUROPOL.

- Organización del Foro Iberoamericano de Encuentro de Ciberpolicías (FIEC), referente de la colaboración internacional entre las unidades contra la ciberdelincuencia a nivel latinoamericano.
- Implicaciones en materia de ciberseguridad, tanto a nivel interno de la propia Unidad, como con colaboraciones con otros organismos competentes en la materia (INCIBE, CCN, CNPIC, etc.) además de la participación de diversos grupos y foros.

Esas unidades periféricas de que se han nombrado, los Equipos de Investigación Tecnológica (EDITE), se encuentran ubicadas en las Unidades Orgánicas de Policía Judicial (UOPJ) de las distintas Comandancias de la Guardia Civil, ubicadas en las distintas provincias españolas.

Los EDITE son unidades operativas que tienen por objetivo la lucha contra los delitos informáticos, pero sin embargo los medios y personal que poseen no les permite afrontar todo el abanico de tipología delictiva que se incluye entre estos delitos, así como aquellos casos que presenten altos conocimientos técnicos (ya que sus componentes reciben cursos "básicos" deformación).De este modo, aquellos delitos informáticos que poseen una complicación extra en su investigación, tienen que solicitar el apoyo del GDT.

Para realizar la correcta coordinación de estos Especialistas, realizar tareas de elaboración de inteligencia y posterior difusión a las Unidades afectadas, homogeneización de procedimientos e impulso de actividades de formación, así como canalizar comunicaciones con otros organismos nacionales e internacionales, la Unidad Técnica de Policía Judicial (UTPJ) dispone de su sección de Delitos Tecnológicos.

En el Servicio de Criminalística se encuentre el Departamento de Ingeniería que se encarga de apoyar las investigaciones que realizan el resto de Unidades de la Guardia Civil, realizando los análisis forenses de los equipos informáticos y dispositivos que les sean requeridos, ya se trate de discos duros, *tablets, smartphones*, *pendrives*, etc. El estudio forense de dichos dispositivos se plasmará en un informe pericial, con validez plena para el proceso penal, debido a la cualificación como peritos que tienen los miembros del Servicio de Criminalística.

4.13.- Cuerpo Nacional de Policía. Brigada de Investigación Tecnológica

Aunque ya se venía trabajando en este ámbito delictivo, en el año 2013, mediante la Orden INT/28/2013, de 18 de enero[110], crea una nueva Unidad denominada ***Unidad de Investigación Tecnológica***, dentro de la Comisaría General de Policía Judicial del Cuerpo Nacional de Policía, con los cometidos relacionados a la lucha contra los delitos que se valgan del uso de las TIC, es decir de la ciberdelincuencia, tanto en el marco nacional como internacional, incluyendo aquellos que afectan a la libertad, la intimidad, el patrimonio, la falsedad o la seguridad lógica.

Esta Unidad está compuesta a su vez por otras dos unidades:

- La Brigada Central de Seguridad Informática, que investiga actividades que incidan en la seguridad lógica.
- La Brigada Central de Investigación Tecnológica (BIT)[111], a la que corresponde la investigación de los delitos tecnológicos, realizan investigaciones que puedan resultar complejas, apoyan investigaciones de otras unidades, coordina investigaciones que afectan a varias unidades, así como las que tengan vinculaciones de carácter internacional, etc.

La estructura central de investigación tecnológica, al igual que el resto de unidades de Policía Judicial específica, acorde a un mejor despliegue y atendiendo a necesidades específicas, cuenta también con pequeñas unidades en diversas provincias que completan su estructura periférica.

Al ser conscientes que, para la investigación de este tipo de delincuencia, se requiere una formación específica, los miembros de la BIT se encuentran en continua formación, recibiendo para ello al apoyo de expertos tanto del sector público como privado, así como estando presente en diversos foros internacionales. De esta forma, la BIT también se

[110] En la Orden INT/28/2013, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía, se desarrolla dentro de esta Dirección General, en su artículo 7 la Comisaría General de Policía Judicial. https://www.boe.es/boe/dias/2013/01/24/pdfs/BOE-A-2013-662.pdf [Consulta: 16-05-2017].

[111] https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html [Consulta: 16-05-2017].

encargan de proporcionar la oportuna formación a otros agentes del Cuerpo Nacional de Policía u otras policías extranjeras.

Es necesario reseñar que esta Unidad, al igual que el GDT de Guardia Civil, no solo se dedican a la investigación, sino que también buscan la colaboración ciudadana en esta materia por lo facilita por diversos medios, página web, redes sociales, tanto el canal oportuno por el que notificar información que pueda tener interés policial o denunciar hechos de carácter delictivo, así como también aprovechan estas Unidades esos mismos canales para lanzar a los usuarios, mensajes de recomendaciones de seguridad, alertas, campañas de concienciación, etc.

4.14.- Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO)

A finales del año 2014, se constituye el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), bajo dependencia directa del Secretario de Estado de Seguridad, como consecuencia de la unificación de los dos servicios que se dedicaban a coordinar la lucha contra el terrorismo y el crimen organizado[112] en el Ministerio del Interior; el Centro Nacional de Coordinación Antiterrorista (CNCA) y el Centro de Inteligencia Contra el Crimen Organizado (CICO).

Tanto el CNCA como el CICO realizaban similares tareas cada uno en las amenazas de su objeto, y se tiene claro que las vinculaciones existentes entre terrorismo y delincuencia organizada son evidentes, por lo que parece lógico que en aras de mejorar el intercambio de información entre organismos especializados encargados de analizar la amenaza terrorista y la relacionada con el crimen organizado, y el extremismo violento, se constituya un órgano como el CITCO, que asuma las funciones de ambos Centros.

Por este motivo se crea el CITCO que, en el ámbito de delincuencia organizada y terrorismo entre otras funciones, recibe y analiza información operativa, elabora inteligencia estratégica, establece los criterios de coordinación en caso de coincidencia de investigaciones de varias unidades, elabora informes de situación, propone estrategias nacionales, etc.

[112] Real Decreto 873/2014, de 10 de octubre, por el que se modifica el Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. https://www.boe.es/boe/dias/2014/10/14/pdfs/BOE-A-2014-10398.pdf [Consulta: 19 mayo 2017].

4.15.- Fiscalía de Criminalidad Informática

En el año 2011, mediante la Instrucción 2/2011[113], de 11 de octubre, la Fiscalía General del Estado crea la figura del Fiscal de Sala de Criminalidad Informática, de esta forma se pretende coordinar y potenciar la armonización de las actuaciones en esta materia mediante la difusión de las oportunas Instrucciones buscando la "unidad de actuación especializada" en todas las jurisdicciones territoriales del Ministerio Público, al considerar que la delincuencia relacionada con las TIC está en constante aumento y la investigación y enjuiciamiento de las mismas no son tarea fácil, lo que hace necesario reforzar la unidad de actuación del Ministerio Fiscal también en esta materia completando la especialización del Ministerio Público.

La Instrucción 2/2011 concreta el catálogo inicial de delitos a los que se extiende el marco competencial del área de criminalidad informática, categorizándolos en tres, que ya fueron abordados en epígrafes anteriores del presente trabajo, pensando ya en esos momentos que este tipo de delincuencia evoluciona de forma rápida por lo que el catalogo inicial no puede ser cerrado, ya que sin duda alguna irán sucediéndose nuevos tipos delictivos.

4.16.-Otros organismos públicos y privados.

Con la asunción de mayores competencias en materia de Policía Judicial por parte de las policías autonómicas, los Mossos d´Esquadra o la Ertzaintza han ido creando sus propios grupos encargado de la investigación de delitos relacionados con las TICs.

Existen otros CERTs tanto de carácter público como privados, que ofrecen servicios a distintos sectores como los existentes en algunas Comunidades autonómicas como pueden ser Andalucía (AndalucíaCERT), Cataluña (CESICAT-CERT) o la Comunidad Valenciana (CESIRTCV). También podemos mencionar otros como como pueden ser: IRIS-CERT (RedIRIS), e-la Caixa-CSIRT, es-CERT (Universidad Politécnica de Cataluña), Mapfre CCG-CERT, S21Sec-CERT, TB-Security-CERT, Telefónica-CSIRT, etc.

[113] Ob. Cit. FISCALIA GENERAL DEL ESTADO. *Instrucción 2/2011.*

Con funciones equivalentes a las de la AEPD en sus respectivos territorios, no encontramos autoridades de protección de datos en comunidades autónomas (Madrid, Cataluña y País Vasco).

5.- HERRAMIENTAS PARA LA INVESTIGACION TECNOLÓGICA DE DELITOS.

Como ha quedado reflejado a lo largo del trabajo, el uso de las TIC implica la ausencia de fronteras a la hora delinquir, la nula regulación de Internet, carencia de armonización total sobre legislación penal, por lo que según el país que se tome como referencia se podrá contar con herramientas legales para investigar o no, que dificulta la cooperación internacional, etc. En definitiva, la ciberdelincuencia presenta unas características específicas que debemos conocer para su eficaz investigación y que podemos resumir en las siguientes:

- **Transnacionalidad**. No existen fronteras para este tipo de amenaza.
- **La comisión del delito es relativamente fácil y rápida**. Aunque se requiere cierto conocimiento sobre tecnologías, éstos no son muy elevados, a lo que se suma que el material necesario para la comisión (acceso a internet, malware, etc.) también son de fácil adquisición. Añadiendo a esto la rapidez de la comisión y la relatividad de la presencia física.
- **Amplitud y coste de los daños que provoca.** Los ciberincidentes y los ciberdelitos pueden afectar a usuarios a escala mundial, con costes económicos muy importantes. Se estima que en el año 2015 supuso unas pérdidas de unos 400.000 millones de dólares[114].
- **Dificultad de investigación y sensación de impunidad**. Las dificultades en la investigación de este tipo de delitos, la rapidez con la que evolucionan los mismos, y el anonimato que se les presupone aporta la sensación de impunidad entre los delincuentes.
- **Colaboración público-privada**. Puesto que en la incidencia de las TIC cohabitan tanto el sector público como privado, para la investigación de la actividad delictiva se requiere la colaboración de ambos, no solo por las imposiciones legales de colaboración que tienen algunos, como pueden ser los operadores o proveedores de servicio, sino que también es necesario el intercambio de información, apoyo técnico, formación, etc.

[114] Ob. Cit. CENTRO CRIPTOLÓGICO NACIONAL. *Ciberamenazas y Tendencias*. Pág. 24

Las investigaciones tecnológicas no tienen otro fin que, el de cualquier investigación criminal, como es la identificación del delincuente y la obtención de evidencias. Las características que hemos reseñado anteriormente nos muestran que, para hacer frente a este tipo de delincuencia, las técnicas tradicionales por si solas son ineficaces, por lo que también debemos hacer uso de las herramientas informáticas y tecnológicas que permitan un aprovechamiento de las capacidades de las TIC. Como consecuencia de esta necesidad el ordenamiento jurídico viene introduciendo nuevas técnicas de investigación, como la reforma operada por la LO 13/2015, que vino a modificar la LECrim, para reforzar este tipo de investigaciones. Por lo que en el presente epígrafe vamos a abordar principalmente algunas de estas nuevas medidas de investigación tecnológicas introducidas por la referida reforma.

5.1.- El agente encubierto informático.

La figura del agente encubierto viene regulada en el art. 282 bis de la LECrim, que por la reforma operada por la LO 13/2015, en el referido artículo se añaden los apartados 6 y 7, para introducir el agente encubierto informático. La utilización del agente encubierto informático en la actualidad, supone la adopción de unas características propias que lo diferencian del tradicional.

El art. 282 bis en su apartado primero contempla que "*Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez"* pueden autorizar a los funcionarios de Policía Judicial a actuar bajo identidad supuesta en investigaciones sobre delincuencia organizada, definida en el apartado cuarto[115], que tenían como fin la comisión de un catálogo de delitos previstos en el Código Penal. Es decir, para la figura del agente encubierto tradicional eran necesarios los requisitos de actividades de delincuencia organizada y que las mismas se refieran al catálogo cerrado de delitos contenidos en el art 282 bis apartado 4.

En el apartado 6 del art. 282 bis LECrim, se introduce la figura del agente encubierto al disponer que "*el juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados"* en la

[115] Se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada.

investigación de los delitos referidos en el art. 282 bis 4 o los contenidos en el art. 588 ter a[116], quedando incluida de esta forma la ciberdelincuencia.

Debemos fijarnos que, en el caso del agente encubierto informático, únicamente es la juez de instrucción quien puede autorizar esta medida a diferencia del agente encubierto tradicional, que además de la Autoridad judicial también lo podía autorizar el Fiscal dando cuenta inmediata al Juez, no teniendo muy claro cuál es la intención de esta distinción, siendo opinión del autor que, motivado por la inclusión de los delitos del art.588 ter a, deba ser exclusivamente el Juez el que deba medir la proporcionalidad y otros criterios, entre el hecho delictivo y la medida investigativa a emplear, debido a que supondría una clara afectación a los derechos fundamentales del individuo su uso para cualquier delito cometido a través de instrumentos informáticos.

Otra peculiaridad del agente encubierto informático es que su ámbito se limita a los "*canales cerrados de comunicación*" mediante autorización judicial, señalando sobre esto en el preámbulo de la LO 13/2015 que, en los canales abiertos no era necesaria esta figura por su propia naturaleza. Para entender cuando nos encontramos en un canal cerrado en el que tenemos que realizar acciones investigativas, debemos considerar como "*aquel espacio virtual en el cual para acceder debemos ocultar nuestra condición de agente de la ley, de forma que actuamos de forma engañosa, para acceder a los espacios o foros cerrados que nos interesan en los que, de no haber utilizado el engaño y la supuesta identidad falsa, el agente no hubiese tenido acceso. Hemos de entender que, al ser cerrado la información que se expone, el intercambio de archivos, opiniones, etc. que realizan los componentes del mismo lo hacen en un clima de confianza, de forma que si utilizamos el engaño sin la oportuna autorización judicial estaríamos vulnerando el secreto de las comunicaciones por ejemplo*"[117].

Otra cuestión es la posibilidad del intercambio o envió de archivos ilícitos, por parte del agente encubierto con autorización judicial, así como el posterior análisis de los resultados mediante los algoritmos identificativos de los referidos archivos. Debiendo en este caso de tener en consideración que el envío de estos archivos no constituya por sí

[116] "*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***". Art. 579.1 refiere "*Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión. Delitos cometidos en el seno de un grupo u organización criminal y Delitos de terrorismo*".

[117] Obtenido mediante entrevista con el Comandante D. César Lorenzana González, destinado en el GDT de la Guardia Civil.

mismo una provocación al delito, debiendo a su vez guardar el envío la proporcionalidad debía con el bien jurídico que se pretende proteger.

5.2.- Las Ciberpatrullas

Otra técnica utilizada por las FCSE, aunque ya se utilizaba previamente a la reforma operada por la LO 13/2015, relacionada con la figura del agente encubierto son, las denominadas ciberpatrullas, que son actuaciones de carácter prospectivos mediante la navegación por los espacios públicos de la red, de forma que aunque los agentes utilicen identidades supuestas para la detección temprana de posibles actividades ilícitas, las mismas al realizarse en canales públicos y abiertos, están amparadas por lo recogido en virtud de sus actuaciones y funciones de prevención de los delitos, en al art.11 de las LO 2/1986 de Fuerzas y Cuerpos de Seguridad, y en el en art. 282 de la LECrim.

Técnica también combinada con la investigación de fuentes abiertas o la investigación OSINT (*Open Source Intelligence*), de forma que mediante la utilización de buscadores o metabuscadores de la Red, las redes sociales u otras herramientas específicas se puede conseguir una gran cantidad de información importantes para una investigación y que en algún momento dado fue aportada de forma voluntaria en la red (correos electrónicos, Nick, archivos, etc.).

5.3.- Interceptación de telecomunicaciones.

Diligencia contenida en el art. 588 ter, en el que señala que la autorización se realiza cuando el ámbito de la investigación sean los delitos recogidos en al art. 579.1 LECrim o *"delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación"*, que ya tratamos en lo referido a la ampliación que conlleva el ámbito del agente encubierto informático.

Siendo los terminales o medios de comunicación que se pueden intervenir, los que utilice el investigado (*habitual u ocasionalmente*) sea titular o usuario, con la posibilidad de que también se establezca la medida en aquellos medios utilizados por terceros, como la victima (*ante la previsibilidad de grave riesgo para la vida o integridad*) u otra persona cuando se tenga constancia que el investigado lo utiliza o el titular colabore con éste; manera que la medida afecta al contenido de las comunicaciones y a los datos de tráfico o asociados[118].

[118] Según art. 588 ter b, *todos aquellos que se generan como consecuencia de la conducción de la comunicación a*

En la solicitud de la autorización se debe hacer constar las disposiciones comunes del art 588 bis b, la identificación del nº de abonado, del terminal o de la etiqueta técnica, así como la identificación de la conexión a intervenir, de forma que el objeto de la solicitud no es otra que el registro y grabación del contenido de las comunicaciones, conocer el origen y destino de estas y la localización geográfica, así como conocer otros datos de tráfico asociados o no a la comunicación.

También se encuentra regulado, el deber de colaboración de los operadores de comunicaciones, prestadores de servicios de telecomunicaciones y de toda persona que facilite comunicaciones, así como el oportuno sigilo para las actuaciones para las que son requeridos judicialmente. Además, otras técnicas de acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, como son la identificación mediante la dirección IP, la obtención por medios técnicos de la Policía Judicial del código IMSI o IMEI de terminales, para su posterior solicitud de intervención o datos sobre titularidad, la cesión de datos desvinculados de los procesos de comunicación relativos a la titularidad o identificación de un dispositivo electrónico, etc.

Se debe conocer aquellos casos de urgencias en los que no precisa en primera instancia la autorización judicial, pero si de una autorización especial, estos son en aquellos casos en los que existiendo urgencia por razones fundadas de que la intervención es imprescindible, en la investigación de delitos de banda armada o terrorismo, pudiendo otorgar la autorización el Ministro del Interior o, el Secretario de Estado de Seguridad en su defecto, debiendo comunicar al Juez la medida a la mayor brevedad posible dentro de las primeras 24 horas, quien resolverá como estime oportuno.

5.4.- Grabación de comunicaciones orales mediante dispositivos electrónicos.

En el art. 588 quarter se regula la "*colocación y utilización*" de dispositivos electrónicos para captación y grabación conversaciones, mediante la oportuna autorización judicial, del investigado, tanto en un espacio público abierto, como en un lugar cerrado, ya sea su domicilio u otro debiendo quedar constancia en la pertinente resolución judicial todo lo relativo al acceso al lugar cerrado (uso de la fuerza, etc.), del mismo modo que se deja

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.

abierta la posibilidad de complementar la medida con obtención de imágenes si lo acuerda el Juez.

Esta medida requiere un uso específico para reuniones, lugares concretos o previsibles, por lo que no se pueden realizar de forma indiscriminada, contemplando la posibilidad de desactivación del dispositivo una vez finalizada la comunicación, su ámbito en este caso se centra en delitos específicos (*delitos dolosos castigados con pena de prisión de tres o más años, delincuencia organizada o terrorismo*) sobre los que se estime que la medida pueda aportar datos esenciales y de relevancia en la investigación probatoria.

5.5.- Captación de imágenes y balizas de posicionamiento.

Diligencia regulada en al art. 588 quinquies, de manera con faculta a la Policía Judicial a obtener y grabar imágenes de la persona investigada en los lugares públicos, para lograr entre otros, información necesaria a efectos de identificación, localización de efectos del delito u otros datos que permita el esclarecimiento de los hechos investigados; esta medida puesto que solo concierne a espacios públicos no requiere autorización judicial, por lo que la misma se podrá realizar aunque afecte a otras personas, cuando sea necesario para no perjudicar al desarrollo de la investigación o tengan relación con el investigado.

Este articulo también regula el uso de las balizas (*medios técnicos de seguimiento y localización*), siendo imprescindible la autorización judicial para su uso de manera que, al concurrir razones de necesidad, así como no exista otro medio menos gravoso (*excepcionalidad y proporcionalidad*), se determinara el medio técnico a emplear en la autorización, la cual por razones de urgencia[119] puede ser obviada por los agentes.

5.6.- Registros de sistemas y dispositivos informáticos.

En este apartado se aborda el registro, es decir el acceso a los sistemas y dispositivos electrónicos, tanto de forma física o la novedosa medida regulada del acceso remoto, a los efectos de obtención de datos o información útiles para la investigación.

[119] Cuando existan razones que puedan frustrar la investigación, en caso de no actuar, la Policía Judicial está habilitada a la colocación debiendo comunicárselo a la Autoridad Judicial a la mayor brevedad y en plazo máximo de 24 horas, siendo ésta quien la ratificará o denegará, teniendo en este último caso nulidad a efectos procesales.

En primer lugar, debemos señalar que en las investigaciones penales durante el desarrollo de las mismas podemos practicar entre otras, un registro domiciliario, en el cual seguramente se proceda a la aprehensión de efectos procedentes del delito o de pruebas e indicios, pues bien si en este caso se procede a la aprehensión de un ordenador u otros dispositivos de almacenamiento masivo de información, esta diligencia no habilita al acceso al contenido de los mismos, siendo necesario la autorización expresa en el mandamiento de Registro por parte de la Autoridad Judicial, como viene recogido en el art. 588 sexies LECrim.

Siendo igualmente necesaria la oportuna autorización judicial, cuando se pretende acceder a la información de dispositivos que se hayan incautado fuera del domicilio del investigado.

Sobre los registros remotos de equipos informáticos, es decir sin necesidad de su presencia física, no incautados, en el art. 588 septies LECrim se regula que con Autorización judicial se puede practicar esta diligencia, mediante la utilización de dos técnicas de investigación:

- la utilización de datos de identificación y códigos, como puedan ser los que habiliten su acceso a los servicios en la nube (*iCloud de Apple, Google Drive, etc.*)
- la instalación de un software que permita el acceso y análisis sin darse cuenta el usuario o titular. Como puede la utilización de archivos espía, troyanos, en definitiva la utilización de *las técnicas de malware, más controladas por los investigadores*"[120].

Esta medida por su carácter excepcional, solo se contempla para una seria de delitos, como son los *"delitos cometidos en el seno de organizaciones criminales, delitos de terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la constitución, de traición y relativos a la defensa nacional y los delitos cometidos a través de instrumentos*

[120] CAMPANER MUÑOZ, Jaime. ¿*Remore Forensic Software* en España? Acerca de la utilización de virus con fines de investigación en el proceso penal. En: BUENO DE MATA, Federico. *Fodertics II: hacia una justicia 2.0.* Salamanca: Ratio Legis, D.L. 2014. Págs. 107-112. ISBN: 978-84-9045-274-5. Pág.108.

informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación" [121]

En la resolución habilitante del Juez para este tipo de registro acceso se especifican, los términos y el alcance del registro (*a qué tipo de información se puede acceder por los principios de excepcionalidad y necesidad*), así como la posible autorización para la realización de copias estableciendo las condiciones que aseguren la integridad de los datos y su preservación para el previsible informe pericial futuro, detalles coincidentes con el registro físico de los sistemas informáticos[122]; además para el caso del registro remoto se concreta el ordenador, dispositivo o medio concreto sobre el que se realiza la diligencia, los agentes habilitados para su práctica, el procedimiento para el acceso e incautación de los datos, así como el software que se utilizará para ello.

En casos de urgencia, la Policía Judicial, podrá actuar de forma directa mediante la ampliación el registro inicialmente autorizado, cuando considere por razones fundadas que los datos que están buscando están almacenados en otro sistema informático o en una parte de él, siempre que sean lícitamente accesibles desde el sistema inicial, medida que afecta tanto al registro físico como el remoto[123], o directamente cuando consideren esta diligencia como imprescindible al apreciar un interés constitucional legítimo, solo contemplado en el registro físico ya que en el remoto por cuestiones técnicas no es posible el procedimiento urgente. En ambos casos se debe informar inmediatamente al juez, como máximo en 24 horas sobre las razones por las que se adoptó la medida, qué y cómo se hizo y el resultado de la misma.

Para el registro remoto se contempla en las mismas condiciones que lo ya comentado sobre la interceptación de las comunicaciones el deber de colaboración y de secreto, para los prestadores de servicios y personas señaladas en al art 588 ter a, así como a los responsables o titulares del objetivo sobre el que se práctica el registro.

Referidos a ambos registros, a requerimiento de los agentes que practiquen esta diligencia, se podrá recabar la ayuda necesaria a personas que faciliten la práctica de la misma, informándole que en caso de negativa de colaboración pueden incurrir en delito de

[121] Art. 588 septies a.

[122] Según los artículos 588 sexies c y 588 septies a apartado 2 letras b), d) y e)

[123] Artículos 588 sexies c apartado 3 y 588 septies a apartado 3

desobediencia. Quedan excluidos de este deber de colaboración el investigado o encausado, las personas que están dispensadas de la obligación de declarar por razón de parentesco o en virtud de secreto profesional.

5.7.- Conservación rápida de los datos

Mediante el art 588 octies, se pretende establecer unas medidas que permitan la preservación de los datos o informaciones, para garantizar su conservación, evitar su alteración o desaparición hasta que se obtiene la pertinente autorización judicial, acorde a lo que se señalaba en el art. 16 del Convenio sobre la Ciberdelincuencia de 2001.

En este artículo se faculta al Ministerio Fiscal o la Policía Judicial a adoptar estas medidas de aseguramiento, mediante el requerimiento a todo aquel que tenga a "su disposición" el sistema objeto de la medida, hasta que resuelva la autoridad judicial. Quedando estos sujetos sometidos al deber colaboración y secreto que venimos comentando en epígrafes anteriores. El periodo máximo de esta medida son 90 días que se podrán prorrogar hasta un total de 180.

5.8.- Otras consideraciones

Para la investigación de la ciberdelincuencia, se debe combinar la investigación tecnológica y la tradicional, un ejemplo claro es que la identificación de una dirección IP, la identificación de un equipo o su titular, no tiene por qué coincidir con la identidad del autor de los hechos, por lo que es necesario utilizar técnicas de investigación tradicional (vigilancia y control de actividades, investigación patrimonial, etc.).

Para ser investigador de este tipo de delincuencia se requiere experiencia policial y unos conocimientos técnicos, *"respecto a los conocimientos técnicos, hay que decir que el nivel de exigencia no es tan alto como el de las habilidades investigativas. El investigador ha de conocer los conceptos básicos de la informática y de las redes, la estructura de los equipos informáticos, sus funcionalidades, las distintas arquitecturas de las redes, entender los sistemas operativos y la información que generan, el funcionamiento de los distintos servicios de Internet, y las capacidades de investigación que ofrecen. Las investigaciones permitirán conocer al detalle las distintas aplicaciones y servicios, e irán enriqueciendo los conocimientos básicos. Son éstos, en resumen, los conocimientos necesarios para saber dónde podemos encontrar rastros de las comunicaciones electrónicas, desde el ordenador en que se generan hasta el de destino.*

Aunque no cabe duda que mientras más conocimientos técnicos tenga el investigador, sobre ámbito ciber mejor resultado se obtendrá en explotación de recursos y por tanto en la investigación"[124].

Tal vez por esta necesidad de conocimientos en la materia cuando a amenazas que provienen del ciberespacio se refiere, el gobierno español está estudiando la posibilidad de reclutar a expertos civiles, para constituir una especie de nueva reserva de las Fuerzas Armadas, considerados como "ciberreservistas", en un principio bajo la responsabilidad del Mando Conjunto de Ciberdefensa.

Este grupo estaría formado por expertos de distintas áreas (ciberseguridad, redes sociales, sociólogos, ingenieros de telecomunicaciones, etc…) los cuales desarrollarían funciones diversas, considerándose necesarios "*perfiles analistas de malware, pentesting (investigación de fisuras en sistemas) y colaboración de los denominados hackers éticos (aquellos que descubren debilidades; no las atacan, sino que informan de los riesgos que comportan)*"[125].

Lo que sin duda reforzaría a las capacidades con la que cuenta el Estado, ya reseñadas en apartados anteriores, aprovechando de este modo a los ciudadanos que tengan una serie de conocimientos técnicos que aporten un plus a nuestra Defensa Nacional.

[124] Obtenido mediante entrevista con el Comandante D. César Lorenzana González, destinado en el GDT de la Guardia Civil.

[125] EL MUNDO: El PP quiere fichar "hackers" civiles contra ciberataques. http://elmundo.es/espana/2017/05/15/5918926322601d0a778b4669.html. [Consulta: 04 julio 2017].

6.- CONCLUSIONES.

Para concluir el presente trabajo, en este epígrafe se expondrán unas reflexiones sobre el mismo y para comenzar, es necesario indicar que en la actualidad Internet está muy presente en el día a día de la mayoría de las personas, de forma que nos aporta muchos beneficios pero que a su vez nos expone a ciertos riesgos que no deberíamos desconocer.

La ciberdelincuencia se aprovecha de esos beneficios que aporta la Red, para conseguir sus propósitos ilícitos vulnerando distintos bienes jurídicos de mediante nuevas formas, de manera que como características principales de las ciberdelincuencia podríamos señalar, la amplitud de posibilidades, puesto que cualquier usuario se convierte en victima potencial, la transnacionalidad, al quedar las fronteras desdibujadas, la rapidez de comisión del delito sin importar la ubicación geográfica, la facilidad de comisión y de eliminación de las evidencias, el anonimato y la sensación de impunidad sobre el delincuente al conocer estas características y la dificultad de su investigación, entre otros motivos la territorialidad o la rapidez con la que evolucionan las técnicas delictivas acorde al desarrollo y evolución de las TIC.

Debemos ser conscientes que cualquiera puede ser víctima de un delito de esta tipología, y debemos conocer que el perfil de los delincuentes es muy variado pudiendo tratarse de individuos, organizaciones criminales o en ocasiones de los propios estados.

A la vista de las estadísticas sobre cibercriminalidad, la misma se encuentra en constante aumento a pesar de que la regulación al respecto ha ido evolucionando a un ritmo considerable, siendo el principal delito por lo que se refiera a España, el fraude informático, viene a señalar en opinión del autor que, además de la respuesta represiva del Estado a este fenómeno mediante la tipificación de los nuevos delitos que van surgiendo en definitiva, la aplicación del Derecho Penal, es necesario incidir en campañas de sensibilización tratando de concienciar a la población, como usuarios, de la importancia de adoptar medidas de seguridad de la información, tanto preventivas, como algo tan simple como la actualización del software o uso de antivirus, como aquellas otras que les lleva a no caer tan fácilmente en las técnicas de ingeniería social utilizada por los por delincuentes o no exponer su vida en las distintas redes sociales, ya que de forma inconsciente se está aportando información que puede ser posteriormente utilizada para actividades ilícitas.

Del mismo modo según las mismas estadísticas es evidente que la incidencia de la cibercriminalidad cada vez será mayor en éstas desplazando a las otras tipologías delictivas. Parece lógico que la ciberdelincuencia se mueva buscando el beneficio económico, por ello entre las tendencias futuras se encuentra al ransomware, para pedir el posterior rescate, el uso criminal de los datos, etc. Además, cada vez prolifera más la moneda virtual, Bitcoin, sobre todo por la Deep Web, donde se garantiza aún más el anonimato.

De la globalización provocada por el ciberespacio, son conscientes los distintos Estados, por lo que han pretendido establecer un marco jurídico apropiado a sus aspiraciones en cuando a Seguridad, de este forma a nivel internacional contamos con una herramienta muy importante y que es consciente del alcance global del fenómeno, siendo el Convenio sobre la Ciberdelincuencia, un texto que apuesta claramente por la actuación conjunta de los países frente a la ciberdelincuencia, mediante la armonización de la legislación apropiada y en aras de mejorar la cooperación internacional, estableciendo la homogeneización de terminología, delitos, aspectos procesales y de investigación, facilitando de este modo la cooperación judicial y policial (*comunicación directa de autoridades, extradición, asistencia mutua, Red 24/7, etc.*).

Aunque el Convenio es un referente y deja claro la necesidad del establecimiento de acuerdos internacionales para luchar contra la ciberdelincuencia, es cierto que el mismo debe ser revisado puesto que se deben ir incluyendo nuevas tipologías delictivas fruto de la evolución y además el mismo tan solo ha sido ratificado por 55 países. España lo ratificó en el año 2010, dando de esta forma un paso importante al objeto de afrontar la ciberdelincuencia.

En el marco europeo en relación a las distintas Estrategias de Seguridad, también se es consciente de la globalidad necesaria para afrontar este fenómeno, así como reforzar la acción represiva y el poder judicial para aumentar la seguridad en el ciberespacio, debiendo aliarse los sectores públicos y privados para mejorar la capacidad de respuesta a los ciberataques.

Además de pretender potenciar las capacidades policiales e investigativas, tratan de mejorar las capacidades prevención y reacción rápida ante ciberataque, a la vez que quieren desarrollar el intercambio de información y alerta. Otro pilar muy importante en las Estrategias es el referido a la formación y concienciación, que afecta a ciudadanos como al

sector público o privado, por lo que impulsa también el I+D en este campo implicando al mundo Académico y centros de investigación.

Con estas mismas premisas de globalidad, en España en el año 2013, se elabora la Estrategia de Seguridad Nacional y la Estrategia de Ciberseguridad, donde se establecen objetivos y líneas de acción coincidentes con las del ámbito europeo, de ahí que, aunque el Gobierno lidere la Estrategia de Ciberseguridad en la misma participan todas las Administraciones, ciudadanos y el sector privado para formar una estructura donde se reúnan todas las capacidades en materia de ciberseguridad.

Referido a la Ciberdelincuencia y con implicación directa sobre las FCSE entre otros, se contempla en la misma estrategia entre sus líneas de acción el *"potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz"* y a su vez compartir inteligencia e información para coordinar sus capacidades con las de Ciberseguridad.

A nivel europeo, es importante también en 2013, la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información, que busca la armonización de la normativa penal en este aspecto y la mejora de la cooperación entre las autoridades competentes de los países, así como entre la parte pública, privada y ciudadanos de éstos, estableciendo además la obligación de los EEMM de ratificar el Convenio sobre la Ciberdelincuencia. De esta forma, se tipifican conductas delictivas y se establecen canales de intercambio de información, a través de la Red 24/7.

En el ámbito nacional, observamos que el marco jurídico que afecta a la ciberdelincuencia es amplio y en continua evolución, sucediéndose la transposición de la normativa comunitaria a nuestro propio ordenamiento, siendo una muestra de ellas las reformas operadas en nuestro Código Penal, por la se han ido introduciendo nuevos tipos penales por la evolución del fenómeno y siguiendo los pasos o recomendaciones de la UE y países de nuestro entorno. En el año 2010 por la reforma operada se introduce en nuestro ordenamiento la Decisión Marco 2005/22/JAI, que posteriormente fue sustituida por la comentada Directiva 2013/40/UE y se incorporan nuevos delitos que afectan a bienes jurídicos diversos, como la intimidad (*Hacking*) el patrimonio (*Cracking*) o la libertad sexual (*Child Grooming*). En el año 2015, se produce una modificación amplia, incidiendo especialmente en la ciberdelincuencia, por la LO 1/2015 se transpone la Directiva

2013/40/UE, volviendo a introducir o complementas tipos delictivos, que igualmente afecta a diversos bienes revelación secretos, daños, propiedad intelectual, libertades públicas, libertad sexual, etc. La LO 2/2015 viene a reformar los delitos de terrorismo introduciendo algunos tipos penales para luchar contra la difusión y adoctrinamiento de este a través de Internet y otras TIC.

Se podría decir que el ordenamiento jurídico español en lo referido a ciberdelincuencia es bastante completo, complementando la norma penal con otras leyes que también tratan de poner orden en la materia y por los que se exige unos requisitos mínimos para poder garantizar la seguridad. En el ámbito procesal y judicial también se cuenta con herramientas para garantizar una cooperación y colaboración policial y judicial eficaces con las que hacer frente a la ciberdelincuencia. En este sentido es de reseñar que nuevamente en el año 2015, con el conocimiento de que las técnicas de investigación criminal tradicionales no eran suficiente, la LO 13/2015, modifica la LECrim y viene a reforzar las posibilidades de las investigaciones tecnológicas.

El fenómeno de la ciberdelincuencia es difícil de combatir, por eso las distintas Estrategias vienen a señalar que la Ciberseguridad se constituye como la primera línea de defensa. Para ello en España se cuenta con varios organismos especializados en diferentes áreas que, en cierta forma vienen a aglutinarse y constituir la "estructura" que permite la mejor explotación de nuestras capacidades. Además, se dispone también de organismos internacionales que colaboran en esta materia con los que España está vinculada por distinta normativa y convenios al respecto.

En el aspecto policial- judicial, de investigación y persecución de los delitos, existen tanto a nivel internacional (INTERPOL), como a nivel europeo (EUROJUST – EC3, CEPOL y EUROJUST) y a nivel nacional (GDT, BIT), organismos dedicados a la lucha contra la ciberdelincuencia, si bien es cierto que se encuentran en ocasiones el problema de la falta de armonización normativa entre países para poder desarrollar efectivamente su trabajo[126].

Para afrontar este fenómeno también es necesaria la colaboración de organismos o instituciones competentes en materia de Ciberseguridad, ya que uno de las mejores medidas

[126] Un ejemplo de ello es INTERPOL que, aunque está formado 190 países y posee herramientas, como el punto de contacto 24/7, la carencia de normativa común dificulta un rendimiento eficaz.

para luchar contra la delincuencia es la prevención de ésta. En esta tarea, estos organismos tienen y adquieren grandes capacidades preventivas y de respuesta al objeto de minimizar los incidentes, por lo que día a día van adquiriendo información e inteligencia del devenir de mal uso de las tecnologías, las vulnerabilidades, etc. De ahí la importancia que tiene que, este tipo de organismos están colaborando con los organismos policiales en lo referido al intercambio de conocimientos, de lecciones aprendidas, etc.

Los dos organismos referentes de las FCSE (GDT y BIT), son conscientes de la aportación que consiguen desde el campo de la ciberseguridad, para su posterior utilización en sus tareas propias, de ahí que estén presentes en distintos foros con actores de este ámbito, compartan experiencias, obtengan formación y en caso necesario se prestan los apoyos técnicos oportunos. Tal es la importancia que se da por parte de las FCSE del Estado a la ciberseguridad, que los mismos también desarrollan tareas en ese campo y en el caso del cuerpo Nacional de Policía dentro de la BIT se dispone de una Unidad exclusiva a tales cometidos.

Se observa que los organismos con competencia en ciberseguridad y por aportan a la lucha contra la Ciberdelincuencia, pueden provenir de distintos sectores ya sean públicos o privados y con atención preferente a objetivos diversos, aunque todos como hemos reseñado anteriormente con la convicción de que la seguridad en el ciberespacio requiere de la implicación de todos.

Al igual que la ciberdelincuencia o las amenazas van evolucionando los organismos que pretenden combatirla también, de forma que han ido surgiendo en distintas épocas y se han ido reformando acorde a las necesidades específicas, de este modo observamos que para el Ministerio Fiscal no pasó de largo la importancia de este fenómeno, de ahí la importancia de la creación de la Fiscalía de Criminalidad Informática.

Por último, es necesario hacer mención a las medidas de investigación tecnológicas que se regulan por la modificación de la LECrim operada por la LO 13/2015, mediante la cual se da mayor cobertura a alguna de las técnicas que ya se venían utilizando como la interceptación de las telecomunicaciones, la grabación de comunicaciones orales mediante dispositivos electrónicos, la captación de imágenes o la utilización de balizas, medidas que fueron surgiendo en la práctica de las investigaciones y que eran avaladas por la Jurisprudencia existente.

Como diligencias más novedosas nos encontramos, la práctica de los registros de sistemas y dispositivos informáticos de forma remota, que debido a las características puede resultar una medida muy beneficiosa en las investigaciones puesto que ya no se requiere la incautación del objeto de registro, además al no ser conocido por el delincuente la práctica de la diligencia el mismo continuará utilizando el sistema o dispositivo, lo que aportará mayor información a los investigadores para su posterior explotación realizando sus actividades, de este modo también se minimizan las posibilidades de que la información objeto de investigación desaparezca tan fácilmente. La cuestión de la territorialidad también es importante, de manera que de forma remota podremos acceder sin importar la ubicación física del objeto de registro o si este se encuentra en el entorno virtual (Nube), pero si debemos de ser conscientes que en caso de que la ubicación física del sistema se encuentre fuera de España debemos a los mecanismos de cooperación que tengamos con ese país para practicar la diligencia.

También son importantes las medidas de aseguramiento incorporadas mediante la conservación rápida de los datos, para garantizar que la información seguirá disponible cuando se obtenga la autorización judicial, mediante medidas que eviten su alteración o desaparición.

Sobre la figura del agente encubierto informático, debemos comentar varios aspectos, primero que era una medida muy demandada porque suponía una necesidad operativa en la investigación de determinados delitos, aunque mediante entrevista con un experto en la materia de las FCSE[127], se tuvo conocimiento que por parte de la Guardia Civil en investigaciones del ámbito de competencias del GDT, no ven que la nueva la figura del agente encubierto informático esté cumpliendo las expectativas que sobre ésta se pusieron sin embargo si se ha utilizado en investigaciones de otras Unidades en el marco del terrorismo yihadista. Por lo que un principio parece que la medida es apropiada al menos para la obtención de información, en evitación de que se realicen determinadas conductas.

En la misma entrevista al abordar el tema del intercambio de archivos ilícitos, el experto venía a considerar que la medida estaba muy encaminada a solventar la problemática existente en el ámbito de la pornografía infantil, y que la regulación actual

[127] Obtenido mediante entrevista con el Comandante D. César Lorenzana González, destinado en el GDT de la Guardia Civil.

presenta muchas carencias a nivel operativo, como que no asegura el control y posterior recuperación en el intercambio de archivos que la puedan considerar como una especie de entrega vigilada informática.

En la utilización de esta figura por parte de las FCSE, se podrían plantear tres niveles de actuación; en un primer plano, el ciberpatrullaje, con el consiguiente descubrimiento y prevención de los delitos que se puedan cometer por la red, en un segundo nivel ase podría avanzar en el ciberpatrullaje para realizar contactos iniciales con los supuestos autores y recopilar indicios, con el fin de comprobar la veracidad de hechos delictivos, de forma que en caso de ser necesario, como último paso se encontraría la solicitud para actuar como agente encubierto informático.

La aparición de esta figura no viene a sustituir la del agente encubierto tradicional, pero atendiendo a la dinámica del tipo de investigación que requieren estos delitos donde se debe conjugar la investigación tecnológica con técnicas de la investigación tradicional, se debería considerar que la solicitud para actuar como agente encubierto informático vaya acompañada, a su vez, de la solicitud para actuar como agente encubierto tradicional.

Finalmente, debemos concluir que muchos Estados y en concreto España, está afrontando el fenómeno de la Ciberdelincuencia, de forma oportuna regulando su ordenamiento jurídico constantemente mediante sucesivas normas, convenios y estrategias, con el conocimiento de la solución global que se debe dar, al objeto de prevenirlo. Aunque todavía se tiene mucho por recorrer, cada vez nos encontramos con mayor armonización penal y de herramientas de cooperación internacional, procesales y de investigación, que permitan subsanar la desaparición de fronteras para esta tipología delictiva.

Otra cuestión en la que España está haciendo esfuerzos acertados es en la adopción de medidas preventivas y reactivas en materia de ciberseguridad consiguiendo implicar tanto al sector público como el privado, con la oportuna sinergia positiva que la misma supone, siendo esta suma de capacidades la que posiblemente haya llevado a pensar que cualquier ayuda es necesaria, ya provenga de instituciones, organismos o de individuos concretos, y sea éste uno de los motivos por lo que el Gobierno de España, este pensando en el reclutamiento de expertos en la materia que pueda ayudar a aumentar las capacidades. En España también se es consciente de la necesidad de formación especializada en este ámbito, por lo que promueve la colaboración con el sector Académico y centros de

investigación para que compartan sus conocimientos, así como apostando por I+D en este campo.

Por último y partiendo de la premisa que, el delito que mejor se resuelve es aquel que no llega a cometerse, debemos señalar la importancia de la concienciación y sensibilización a los usuarios, empresas y demás sobre la necesidad de la adopción de medidas de seguridad sobre los sistemas de información y el uso de éstos con el fin de minimizar posibles riesgos.

BIBLIOGRAFÍA

- ANARTE BORRALLO, Enrique. "Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información". *Derecho y Conocimiento, Anuario Jurídico sobre la Sociedad de la Información*, Volumen 1, Universidad de Huelva: Facultad de Derecho, 2001, Págs. 191 y ss.
- ACURIO DEL PINO, Santiago. *Delitos Informáticos: Generalidades*. [En Línea]. Págs. 10-11. Disponible en:<http://oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf> [Fecha de Consulta: 22 marzo 2017]
- BIURRUN ABAN, Fernando J. Los riesgos de las nuevas tecnologías. *Actualidad jurídica Aranzadi*. 2016, Nº 921. ISSN 1132-0257.
- CAMPANER MUÑOZ, Jaime. ¿*Remore Forensic Software* en España? Acerca de la utilización de virus con fines de investigación en el proceso penal. En: BUENO DE MATA, Federico. *Fodertics II: hacia una justicia 2.0*. Salamanca: Ratio Legis, D.L. 2014. Págs. 107-112. ISBN: 978-84-9045-274-5.
- COMISIÓN EUROPEA. Comunicación dirigida al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM [2010] 245 final), "*Una Agenda Digital para Europa*" [En línea]. 2010. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245&from=ES> [Consulta: 11 abril 2017].
- COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo y el Consejo. *La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura*. COM (2010) 673 final.[En línea]. Bruselas, 2010. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0673&from=ES> [Consulta: 11 abril 2017].
- COMISION EUROPEA. Comunicación de la Comisión al Consejo y al Parlamento Europeo. "*La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia*". COM (2012) 140 Final. [En línea] Bruselas, 2012.<http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0140&from=ES > [Consulta: 5 mayo 2017].
- COMISIÓN EUROPEA. Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones. *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*. JOIN (2013) 1 final. [En línea]. Bruselas, 2013. <http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:ES:PDF.> [Consulta: 13 abril 2017].

- COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo y al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. "*Agenda Europea de Seguridad*", 28.4.2015 COM (2015) 185 final. [En línea]. Estrasburgo, 2015. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0185&from=EN.> [Consulta: 15 abril 2017].
- CONSEJO DE EUROPA. Acto del Consejo por el que se celebra, de conformidad con el artículo 34 del Tratado de la Unión Europea, el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea. Bruselas, 29 mayo de 2000. (2000/C 197/01). [En línea]. Bruselas, 2000. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:C2000/197/01&from=ES.> [Consulta: 11 abril 2017].
- CONSEJO DE EUROPA. *Convenio sobre la Ciberdelincuencia*. Serie de Tratados Europeos nº 185. [En línea]. Budapest, 2001. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c> [Consulta: 14 marzo 2017].
- CONSEJO DE EUROPA. *Informe explicativo del Convenio sobre la Ciberdelincuencia.* Serie de Tratados Europeos nº 185. [En línea]. 2001.
- <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa403> [Consulta: 14 marzo 2017].
- CONSEJO DE LA UNIÓN EUROPEA. *Decisión del Consejo de 28 de febrero de 2002 por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.* (2002/187/JAI). [En línea]. Bruselas, 2002. < http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002D0187&from=ES.> [Consulta: 6 mayo 2017].
- CONSEJO DE LA UNION EUROPEA. *Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.* [En línea]. 2005. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ES:PDF> [Consulta: 14abril 2017].
- CONSEJO DE LA UNION EUROPEA. *Decisión 2005/681/JAI del Consejo de 20 de septiembre de 2005, por la que se crea la Escuela Europea de Policía (CEPOL) y por la que se deroga*

la Decisión 2000/820/JAI [En línea]. Bruselas 2005. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005D0681:ES:NOT.> [Consulta: 6 mayo 2017].

- DÍAZ GÓMEZ, Andrés. *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*, REDUR 8. [En línea]. Diciembre 2010, págs. 169-203. ISSN 1695-078X. <http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf> [Consulta: 14 marzo 2017].
- EUROPEAN POLICE OFFICE.*Internet Organised Crime Threat Assessment (IOCTA) 2016*[Enlínea]2016<https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf> [Consulta: 27 marzo 2017].
- FISCALIA GENERAL DEL ESTADO. *Instrucción 2/2011 sobre el fiscal de sala de criminalidad informática y las secciones de criminalidad informática de las fiscalías*. [En línea]. Madrid, 2011. <https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_instru_02.pdf?idFile=6311c525-d23a-45d7-9e50-458f6f8c3406> [Consulta: 23 marzo 2017].
- FISCALIA GENERAL DE ESTADO. *Memoria elevada al Gobierno de S.M.Capítulo III. Fiscales Coordinadores y Delegados para materias específicas- 8.Criminalidad Informática.* Centro de Estudios Jurídicos. Ministerio de Justicia. [En línea]. Madrid, 2016. <https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/recursos/pdf/capitulo_III/cap_III_8.pdf> [Consulta: 26 marzo 2017].
- GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR .*Anuario Estadístico del Ministerio del Interior.* [En línea]. Madrid, 2016. <http://www.interior.gob.es/documents/642317/1204854/Anuario_estadistico_2015_126150729.pdf/da61515a-9cd8-4cb4-bdd9-a17f3d3d7b20> [Consulta: 23 marzo 2017].
- GOBIERNO DE ESPAÑA. *Estrategia de Ciberseguridad Nacional.* [En línea]. Madrid, 2013. <http://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20ciberseguridad%20nacional.pdf> [Consulta: 6 marzo 2017].
- GOBIERNO DE ESPAÑA. *Estrategia de Seguridad Nacional.* [En línea]. Madrid, 2013. <http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf> [Consulta: 6 marzo 2017].

- GOBIERNO DE ESPAÑA. *Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001*. Agencia Estatal Boletín Oficial del Estado. [En línea]. 2010. <https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf> [Consulta: 14 marzo 2017].
- GOBIERNO DE ESPAÑA. *Instrumento de Ratificación del Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*. Agencia Estatal Boletín Oficial del Estado. [En línea]. 2013. <https://www.boe.es/boe/dias/2015/01/30/pdfs/BOE-A-2015-793.pdf> [Consulta: 23 marzo 2017].
- INSTITUTO NACIONAL DE CIBERSEGURIDAD. *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario.*[En línea]. 2017. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf> [Consulta: 30 marzo 2017].
- INSTITUTO NACIONAL DE ESTADISTICA. *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares. Año 2016*. [En línea]. Madrid, 2016. <http://www.ine.es/dyngs/INEbase/es/operacion.htm?c=estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608> [Consulta: 11 marzo 2017].
- INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. *BITCOIN: Una moneda criptográfica.* [En línea]. 2014. <https://www.certsi.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf> [Consulta: 30 marzo 2017].
- MEDINA LINÀS, Manel. *Cibercrimen: ¡protégete del "bit-bang"!, los ataques en el ciberespacio a tu ordenador, tu móvil, tu empresa: aprende de víctimas, expertos y cibervigilantes*. Barcelona: Tibidabo, 2015. ISBN: 978-84-16204-82-3.
- MIRÓ LLINARES, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, 2012. ISBN: 978-84-15664-18-5.
- NACIONES UNIDAS. Resolución 2178 del Consejo de Seguridad. 24 de septiembre de 2014. [En línea].<http://www.un.org/en/sc/ctc/docs/2015/N1454802_ES.pdf> [Consulta: 17 abril 2017].
- OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN. "*Estudio sobre la ciberseguridad y confianza en los hogares españoles"*. [En línea]. Madrid, 2017.<

http://www.ontsi.red.es/ontsi/es/Ciberseguridad-y-confianza-en-los-hogares-españoles-abril-2017 >. [Consulta: 28 abril 2017].

- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. *Reglamento (CE) 460/2004 del Parlamento Europeo y del Consejo de 10 de marzo de 2004 por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información*. [En línea]. Estrasburgo, 2004. < http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32004R0460&from=ES .> [Consulta: 7 mayo 2017].
- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. *Reglamento (UE) 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) 460/2004*. [En línea]. Estrasburgo, 2013. Diario Oficial de la Unión Europea n° L 165 de 18/06/2013. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:ES:PDF> [Consulta: 7 mayo 2017].
- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. *Reglamento (UE) 2015/2219 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre la Agencia de la Unión Europea para la formación policial (CEPOL) y por el que se sustituye y deroga la Decisión 2005/681/JAI del Consejo*. [En línea]. Estrasburgo, 2015. < http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015R2219&from=ES.> [Consulta: 6 mayo 2017].
- PAVÓN PÉREZ, Juan Antonio. Derecho Internacional Público. La labor del Consejo de Europa en la lucha contra la cibercriminalidad: El protocolo Adicional al Convenio Nº 185 sobre cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos. *Anuario de la Facultad de Derecho*. [En línea]. ISSN 0213-988-X Vol. XXI (2003) págs. 187-204.<https://dialnet.unirioja.es/descarga/articulo/854132.pdf> [Consulta: 14 marzo 2017].
- RAYÓN BALLESTEROS, María Concepción y GÓMEZ HERNÁNDEZ, José Antonio. Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*. [En línea]. XLVII (2014) págs. 209-234. ISSN: 1133-3677. <https://dialnet.unirioja.es/servlet/articulo?codigo=4639646> [Consulta: 14 marzo 2017].

- RODRIGUEZ BERNAL, A. *Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia.* Revista de derecho informático nº 103.[En línea]. 2007, Pág. 13. <http://www.egov.ufsc.br/portal/sites/default/files/los_cibercrimenes_en_el_espacio_de_libertad_seguridad_y_justicia.pdf>. [Consulta: 23 marzo 2017].
- SECRETARIA GENERAL DEL CONSEJO DE EUROPA. *Estrategia de Seguridad Interior de la Unión Europea: Hacia un modelo europeo de seguridad.* Oficina de Publicaciones de la Unión Europea [En línea].Luxemburgo: ISBN 978-92-824-2680-7 doi:10.2860/881. 2010. <https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ESC.pdf> [Consulta: 11 abril 2017].
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). *Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación Resolución 181 (Nueva).* [En línea]. 2010.<https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf> . [Consulta: 15 marzo 2017].
- VELASCO SAN MARTÍN, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet.* Valencia: Tirant lo Blanch, 2012.

LEGISLACION

- 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. [En línea]. <http://www.boe.es/doue/2013/218/L00008-00014.pdf>. [Consulta: 14 abril 2017].
- DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016, *relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.* [En línea]. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES>. [Consulta: 15 abril 2017].
- DIRECTIVA 2006/24/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de marzo de 2006 *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.* [En línea]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF>. [Consulta: 15 abril 2017].

- DIRECTIVA 2011/92/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de diciembre de 2011 *relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo*. Diario Oficial de la Unión Europea n° L 335 de 17/12/2011. [En línea] <. http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011L0093&from=ES> [Consulta: 5 mayo 2017].
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [En línea] <http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html> [Consulta: 17 abril 2017]
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. [En línea] <http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html. > [Consulta: 17 abril 2017].
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [En línea]. <http://noticias.juridicas.com/base_datos/Admin/l34-2002.html. > [Consulta: 17 abril 2017].
- Ley 11/2003, de 21 de mayo, reguladora de los Equipos Conjuntos de Investigación penal en el ámbito de la Unión Europea [En línea] <http://noticias.juridicas.com/base_datos/Admin/l11-2003.html> [Consulta: 20 abril 2017].
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. [En línea] <http://noticias.juridicas.com/base_datos/Admin/l25-2007.html. > [Consulta: 18 abril 2017].
- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [En línea] <https://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf> [Consulta: 17 abril 2017]
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.[En línea] <http://noticias.juridicas.com/base_datos/Admin/529091-l-9-2014-de-9-may-telecomunicaciones.html> [Consulta: 18 abril 2017]
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [En línea]

<https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf> [Consulta: 17 abril 2017]

- Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [En línea] <https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3440.pdf> [Consulta: 17 abril 2017].
- Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. [En línea] <http://noticias.juridicas.com/base_datos/Penal/560107-lo-13-2015-de-5-oct-modificacion-de-la-ley-de-enjuiciamiento-criminal-para.html> [Consulta: 20 abril marzo 2017].
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [En línea] <http://noticias.juridicas.com/base_datos/Admin/559951-l-39-2015-de-1-oct-procedimiento-administrativo-comun-de-las-administraciones.html> [Consulta: 17 abril 2017].
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [En línea] <http://noticias.juridicas.com/base_datos/Admin/559952-l-40-2015-de-1-oct-regimen-juridico-del-sector-publico.html> [Consulta: 18 abril 2017]
- Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal.[En línea] <http://noticias.juridicas.com/base_datos/Penal/lecr.html> [Consulta: 20 abril 2017].
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. [En línea] <http://noticias.juridicas.com/base_datos/Admin/rd3-2010.html> [Consulta: 18 abril 2017].
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el Ámbito de la Administración Electrónica. [En línea] <http://noticias.juridicas.com/base_datos/Admin/rd4-2010.html> [Consulta: 18 abril 2017].
- REAL DECRETO 421/2004, *de 12 de marzo, por el que se regula el Centro Criptológico Nacional.* https://www.ccn.cni.es/images/stories/normas/pdf/rd421-2004centrocriptologiconacional.pdf [Consulta: 10 mayo 2017].

- Resolución de 8 de septiembre de 2015(publicada en el BOE de 18 de septiembre), de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos. http://www.boe.es/buscar/doc.php?id=BOE-A-2015-10060 [Consulta: 10 mayo 2017].
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia https://www.ccn.cni.es/images/stories/normas/pdf/ley_11_2002_reguladora_cni.pdf [Consulta: 10 mayo 2017].
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica http://noticias.juridicas.com/base_datos/Admin/rd3-2010.html#c1 [Consulta: 10 mayo 2017].
- En la Orden INT/28/2013, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía, se desarrolla dentro de esta Dirección General, en su artículo 7 la Comisaría General de Policía Judicial. https://www.boe.es/boe/dias/2013/01/24/pdfs/BOE-A-2013-662.pdf [Consulta: 16 mayo 2017].
- Real Decreto 873/2014, de 10 de octubre, por el que se modifica el Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. https://www.boe.es/boe/dias/2014/10/14/pdfs/BOE-A-2014-10398.pdf [Consulta: 19 mayo 2017].

INTERNET:

- <http://www.internetworldstats.com/stats.htm>. [Consulta: 3 julio 2017].
- CNN-CERT.-https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html
- <https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce>[Consulta: 5 mayo 2017].
- http://europa.eu/european-union/about-eu/agencies/eurojust_es [Consulta: 6 mayo 2017].
- https://www.enisa.europa.eu/about-enisa/mission-and-objectives [Consulta: 7 mayo 2017].
- INCIBE. https://www.incibe.es/que-es-incibe [Consulta: 7 mayo 2017].

- http://www.cnpic.es/index.html [Consulta: 8 mayo 2017].
- https://www.certsi.es/sobre-certsi/que-es-certsi [Consulta: 8 mayo 2017].
- Centro Criptológico Nacional https://www.ccn.cni.es/index.php?option=com_content&view=article&id=1&Itemid=3&lang=es [Consulta: 10 mayo 2017].
- CCN-CERT https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html [Consulta: 10 mayo 2017].
- http://www.emad.mde.es/CIBERDEFENSA/ [Consulta: 13 mayo 2017].
- http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php [Consulta: 13 mayo 2017].
- https://www.gdt.guardiacivil.es/webgdt/home_alerta.php [Consulta: 16 mayo 2017].
- https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html [Consulta: 16 mayo 2017].

ACRÓNIMOS

AAPP: Administraciones Públicas

AEPD: Agencia Española de Protección de Datos

BIT: Brigada de Investigación Tecnológica

CBIT: Curso Básico de Investigación Tecnológica

CCN: Centro Criptológico Nacional

CDPC: Comité Europeo para los problemas criminales

CEPOL: *European Police College* (Agencia de la Unión Europea para la Formación Policial)

CERT: *Computer Emergency Response Team* (Equipo de respuesta a emergencias informáticas)

CERTSI: Equipo de respuesta a incidentes cibernéticos de seguridad e industria

CICO: Centro de Inteligencia Contra el Crimen Organizado

CITCO: Centro de Inteligencia contra el Terrorismo y el Crimen Organizado

CNCA: Centro Nacional de Coordinación Antiterrorista

CNI: Centro Nacional de Inteligencia

CNPIC Centro Nacional para la Protección de las Infraestructuras Críticas

CSIRT: *Computer Security Incident Response Team* (Equipo de respuesta a incidentes de seguridad informática)

EC3: *European Cybercrime Centre* (Centro Europeo de Ciberdelincuencia)

ECI: Equipo Conjunto de Investigación

ECSO: *European Cyber Security Organisation* (Organización Europea de Ciberseguridad)

EDITE: Equipos de Investigación Tecnológica

EEMM: Estados Miembros

EMV: *Europay MasterCard Visa* (Tarjeta con circuito integrado)

ENISA: *European Network and Information Security Agency* (Agencia Europea de Seguridad de las Redes y de la Información)

ENI: Esquema Nacional de Interoperabilidad

ENS: Esquema Nacional de Seguridad.

ESN: Estrategia de Seguridad Nacional

EUROJUST: Unidad Europea de Cooperación Judicial

EUROPOL: Oficina Europa de Policía

FCSE: Fuerzas y Cuerpos de Seguridad del Estado

GDT: Grupo de delitos telemáticos.

IGCI: *INTERPOL Global Complex for Innovation* (Complejo Mundial de INTERPOL para la Innovación)

INCIBE: Instituto Nacional de Ciberseguridad.

INTERPOL: Organización Internacional de Policía Criminal

IOCTA: *Internet Organised Crime Threat Assessment* (Evaluación de la Delincuencia Organizada de Internet)

IP: *Internet Protocol* (Protocolo de Internet)

LA: Línea de acción.

LECrim:	Ley de Enjuiciamiento Criminal
LO:	Ley Orgánica
MCCD:	Mando Conjunto de Ciberdefensa
OCC:	Oficina de Coordinación Cibernética.
OCDE:	Organización para la Cooperación y Desarrollo Económico
OSI:	Oficina de Seguridad del Internauta
PC-CY:	Comité de Expertos en la Delincuencia del Ciberespacio
RD:	Real Decreto
RENIC:	Red de Excelencia Nacional de Investigación en Ciberseguridad
SES:	Secretaria de Estado de Seguridad.
SESIAD:	Secretaría de Estado para la Sociedad de la Información y Agenda Digital
TIC:	Tecnologías de la Información y la Comunicación
UCO:	Unidad Central Operativa
UE:	Unión Europea
UOPJ:	Unidades Orgánicas de Policía Judicial
UTPJ:	Unidad Técnica de Policía Judicial

GLOSARIO[128]:

Abuso de los dispositivos: En dicho aparatado, se hace referencia a la venta, obtención para su utilización, importación, difusión o cualquier forma de poner a disposición de dispositivos o programas informáticos, que puedan ser utilizados o concebidos para la comisión de los delitos contemplados anteriormente, así como claves de acceso o programas que faciliten dichos códigos de acceso de forma ilegítima hacia sistemas informáticos.

Acceso Ilícito: Entendiendo como tal, el acceso deliberado e ilegitimo a una parte o a la totalidad de un sistema informático vulnerando las medidas de seguridad, con la intención de obtener información o datos informáticos de dichos sistemas, o de los sistemas conectados al mismo.

Bitcoin: es una moneda electrónica, un protocolo y un software. La conjunción de estos componentes permite la realización de transacciones casi instantáneas entre pares (*peer-to-peer* o P2P) y, por consiguiente, pagos en todo el mundo con unos bajos costos, o incluso nulos, de procesado de dichas transacciones.

Bitcoin opera bajo tecnología peer-to-peer para así evitar depender de una autoridad monetaria central que se encargue de la emisión y el control de dinero. Así, no es posible manipular el valor de las *bitcoins* o crear inflación produciendo más moneda. La propia red es la que gestiona las transacciones y la emisión de *bitcoins*, que se generan a través de la llamada minería, de forma controlada y descentralizada. La utilización de criptografía garantiza la seguridad de las transacciones. Por ejemplo, se puede controlar que sólo el dueño de las monedas pueda gastarlas, y que sólo las pueda utilizar en una única

[128] Definiciones obtenidas del Convenio sobre la Ciberdelincuencia, Budapest 2001.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario.* [En línea]. 2017. < https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf> [Consulta: 30 marzo 2017].

INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. *BITCOIN: Una moneda criptográfica.* [En línea]. 2014.

< https://www.certsi.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf > [Consulta: 30 marzo 2017].

transacción. Las figuras de control y supervisión presentes en los sistemas monetarios de los mercados actuales no existen en *bitcoin*.

Botnet: Una *botnet* es un conjunto de ordenadores (denominados *bots*) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de *spam*, ataques de *DDoS*, etc.

Las *botnets* se caracterizan por tener un servidor central (*C&C*, de sus siglas en inglés *Command* & *Control*) al que se conectan los *bots* para enviar información y recibir comandos.

Existen también las llamadas *botnets P2P* que se caracterizan por carecer de un servidor *C&C* único.

Ciberseguridad[129]: Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

1) disponibilidad
2) integridad, que puede incluir la autenticidad y el no repudio
3) confidencialidad

Datos informáticos: Se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

[129] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). *Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación Resolución 181 (Nueva).* [En línea]. 2010. <https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf >. [Consulta: 15 marzo 2017].

Datos sobre el tráfico: Se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

Denegación de servicio: *(También DoS, Ataque de Denegación de Servicio, DDoS)***.** Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él.

El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

Un método más sofisticado es el ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas, de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legítimos dueños (por ejemplo, a través de una botnet).

Esto puede ser así mediante el uso de programas *malware* que permitan la toma de control del equipo de forma remota, como puede ser en los casos de ciertos tipos de gusano o bien porque el atacante se ha encargado de entrar directamente en el equipo de la víctima.

Dirección IP: Las direcciones IP (del acrónimo inglés IP para *Internet Protocol*) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

Podríamos compararlo con una matrícula en un coche. Así, una dirección IP (o simplemente IP) en su versión v4 es un conjunto de cuatro números del 0 al 255 separados por puntos. Por ejemplo: 192.168.121.40

En su versión v6, las direcciones IP son mucho más complejas, siendo hasta 4 veces más largas, más seguras y permitiendo un gran número de sistemas conectados a Internet. Un ejemplo es el siguiente: 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

Las direcciones IP pueden ser «públicas», si son accesibles directamente desde cualquier sistema conectado a Internet o «privadas», si son internas a una red LAN y solo accesibles desde los equipos conectados a esa red privada.

Falsificación Informática: La cual no viene recogida en este punto como la creación de programas que pudieran plagiar a otros, sino refiriéndose a la introducción de programas o

archivos informáticos, que modifiquen datos propios del sistema, generando datos no auténticos, con la finalidad última de que los mismos sean considerados como verdaderos.

Fraude Informático: Se hace referencia al perjuicio patrimonial de la persona por sufrir actos ilegítimos mediante la alteración, introducción o borrado de datos informáticos o cualquier interferencia en el normal funcionamiento del sistema informático.

IMEI[130]: El IMEI (del inglés *International Mobile Station Equipment Identity*, identidad internacional de equipo móvil) es un código USSD pregrabado en los teléfonos móviles GSM. Este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta.

Esto quiere decir, entre otras cosas, que la operadora que usemos no solo conoce quién y desde dónde hace la llamada (SIM), sino también desde qué terminal telefónico la hizo. La empresa operadora puede usar el IMEI para verificar el estado del aparato mediante una base de datos denominada EIR (*Equipment Identity Register*). El IMEI permite funciones como el bloqueo de terminales móviles en caso de robo, para lo cual simplemente tendremos que notificar el IMEI del móvil a nuestra operadora de telefonía para que proceda su bloqueo y así pueda impedirse la comunicación desde ese dispositivo mediante el bloqueo de llamadas. También es posible liberar un teléfono móvil bloqueado para su uso con una nueva operadora móvil a partir del código IMEI, independientemente de la marca o modelo.

IMSI[131]: es el acrónimo de *International Mobile Subscriber Identity* (Identidad Internacional del Abonado a un Móvil). Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

Ingeniería social: Las técnicas de ingeniería social son tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.

[130] https://es.wikipedia.org/wiki/IMEI

[131] https://es.wikipedia.org/wiki/IMSI

Interferencia en el Sistema: Dicho apartado se refiere a la obstaculización grave de un sistema informático mediante la introducción, trasmisión, daño, borrado, deterioro o alteración y supresión de datos informáticos.

Interferencia en los Datos: Significando que están contenidos en dicho apartado la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

Interceptación Ilícita: Considerando la interceptación ilícita, ilegitima y deliberada por medios técnicos de datos informáticos en trasmisiones no públicas y dirigidas hacia un sistema informático, originadas en un sistema informático, o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas.

Malware: Es un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de *software* malintencionado: *malicious software*. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, *backdoors*, *spyware*, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

P2P: (del inglés *Peer-to-Peer*) es un modelo de comunicaciones entre sistemas o servicios en el cual todos los nodos/extremos son iguales, tienen las mismas capacidades y cualquiera de ellas puede iniciar la comunicación.

Se trata de un modelo opuesto al cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. El modelo P2P se basa en que todos los nodos actúan como servidores y clientes a la vez.

Una red P2P es por tanto una red de sistemas o servicios que utiliza un modelo P2P. Todos los sistemas/servicios conectados entre sí y que se comportan como iguales con un objetivo en común.

Por ejemplo, las *botnets P2P* utilizan este modelo para evitar que haya un servidor central único fácilmente detectable.

Proveedor de servicios: se entenderá: a) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y b) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio.

Pharming: Ataque informático que aprovecha una vulnerabilidad del software de los servidores DNS y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

Phishing: Es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

El estafador o phisher suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.

Existen diferentes modalidades de phishing. Cuando éste se realiza vía SMS el nombre técnico es Smishing y cuando se realiza utilizando Voz sobre IP, se denomina vishing. Otra variedad es el spear phishing, en la que los atacantes intentan mediante un correo electrónico, que aparenta ser de un amigo o de empresa conocida, conseguir que les facilitemos: información financiera, números de tarjeta de crédito, cuentas bancarias o contraseñas.

Ransomware. El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos. La seguridad del sistema está basada en la dificultad de factorización de grandes números. Su funcionamiento se basa en el envío de un mensaje cifrado mediante la clave pública del destinatario, y una vez que el mensaje cifrado llega, éste se encarga de descifrarlo con su clave privada.

Sistema informático: Se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa.