Universidad Internacional de La Rioja

Máster Universitario en Derecho Penal Económico

Cuestiones actuales de la criminalidad cibereconómica

Trabajo de fin de máster presentado por: **Samuel Alfonso Acuña Lara**

Titulación: Master Universitario en Derecho Penal Económico

Área jurídica: Derecho Penal

Director/a: Dr. Francisco Javier Hernández Suárez-Llanos

Ciudad: Bogotá, Colombia

16 de julio de 2020

Firmado por: Samuel Alfonso Acuña Lara

Índice

I. Introducción……7

II. Consideraciones generales……10

2.1. Vínculos entre cibercriminalidad y delitos económicos……10

2.2. Breves anotaciones sobre las nuevas tecnologías con relevancia jurídico penal ……14

III. La criminalidad cibereconómica como forma de delincuencia organizada transnacional……20

3.1.Rasgos definitorios……20

3.2. Marco regulatorio de la cooperación internacional……23

3.3.Participación de la Europol en la lucha contra la cibercriminalidad…… 27

IV. Intervención de las nuevas tecnologías en el derecho penal económico……31

4.1. Principales reformas del Código Penal vinculadas con la criminalidad cibereconómica……31

4.2. Delito de blanqueo de capitales y el aumento exponencial del uso de los criptoactivos ……36

V. Prevención y persecución de la criminalidad cibereconómica……40

5.1. Medios tecnológicos de investigación en la Ley de Enjuiciamiento Criminal……40

5.1.1. La intervención de las comunicaciones telefónicas y telemáticas……..40

5.1.2 Captación o grabación de comunicaciones orales, con la utilización de dispositivos electrónicos……..44

5.1.3. El registro de dispositivos de almacenamiento masivo……45

5.1.4. La técnica de investigación de observación, análisis y extracción de información de un ordenador e instrumento de almacenamiento masivo, dispositivo electrónico o sistema de base de datos……..46

5.2. Prevención, detección y respuesta ante la cibercriminalidad como política de Estado ……47

VI. Conclusiones……52

VII. Bibliografía……55

VIII. Fuentes jurídicas utilizadas……59

IX. Otras fuentes……64

Listado de abreviaturas

(CE) Constitución Española

(CP) Código Penal

(CSA) Cloud Security Alliance

(CSC) Convenio sobre la Ciberdelincuencia

(DOT) Delincuencia Organizada Transnacional

(DPE) Derecho Penal Económico

(DAM) Dispositivos de almacenamiento masivo

(EC3) Centro Europeo de Ciberdelincuencia

(Europol) Agencia de la Unión Europea en materia policial

(FTTH) Fiber to the home

(GAFI) Grupo de Acción Financiera Internacional

(Interpol) Organización Internacional de Policía Criminal

(IoT) Internet de las cosas

(LECrim) Ley de Enjuiciamiento Criminal

(MIT) Massachusetts Institute of Technology

(NT) Nuevas tecnologías

(OCDE) Organización para la Cooperación y el Desarrollo Económico y los Estados

(OEA) Organización de Estados Americanos

(RFID) Radiofrecuencia en red

(TIC) Tecnologías de la Información y Comunicación

(UE) Unión Europea

(UNODC) Oficina de las Naciones Unidas Contra la Droga y el Delito

(UNTOC) Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

Resumen

El crimen cibereconómico es el resultado del uso de las tecnologías de la información y comunicación, y de las nuevas tecnologías para la comisión de delitos con sustrato económico. Las características propias del cibercrimen -silencioso, invisible, desterritorializado y no denunciado- generan dificultades para los Estados, en la prevención, represión y persecución de estas conductas. La normativa internacional que regula el cibercrimen se circunscribe el Convenio Sobre la Ciberdelincuencia, suscrito en Budapest el 23 de noviembre de 2001 siendo pertinente la catalogación como delito de delincuencia organizada transnacional con base a sus características propias, con el fin de ampliar los instrumentos de cooperación entre los Estados. En el Derecho interno español se han actualizado los cuerpos normativos (Código Penal y Ley de Enjuiciamiento Criminal) para estar en sintonía con el deber de protección a la sociedad dispuesta por la Unión Europea en la lucha contra estos ilícitos penales.

Palabras claves

Nuevas tecnologías. Blanqueo de capitales. Cibercrimen. Medios tecnológicos de investigación.

Abstract

Cyber-economic crime is the result of the use of information and communication technologies, as well as new technologies for the commission of crimes with an economic background. The characteristics of cybercrime -silent, invisible, that does not respect borders, and not denounced- generate difficulties for Governments in the prevention, repression and prosecution of these behaviors. The international legislation that regulates cybercrime is limited to the Convention on Cybercrime, Budapest November 23, 2001, with the classification as a transnational organized crime based on its own characteristics, in order to expand the instruments of cooperation between Governments. In Spain, internal laws, regulatory bodies (Penal Code and Criminal Procedure Law) have been updated to be aligned with the

duty to protect society provided by the European Union in the fight against these criminal offenses.

KEYWORDS

New technologies. Money laundering. Cybercrime. Technological means of investigation.

I. Introducción

Los delincuentes económicos basaban su *modus operandi* en medios e instrumentos de comisión tradicionales (tales como cheques, documentos falsificados, estructuras piramidales, utilización de interpuestas personas) viendo modificado su actuar al valerse de instrumentos técnicos más sofisticados que se han desarrollado con el advenimiento de la tecnología de información y comunicación (en lo sucesivo TIC) y en la actualidad con las nuevas tecnologías (en lo sucesivo NT).

Si bien es cierto que no debemos olvidar el nivel de lesividad de las conductas tradicionales que han atentado contra los bienes jurídicos de carácter socio económico, el presente y futuro de la ciencia jurídica penal debe analizar muy acuciosamente las nuevas conductas que afloren con el desarrollo de las NT y su utilización para cometer hechos punibles.

Por tanto, el propósito de este Trabajo de Fin de Master es determinar la evolución legislativa de cara a la adecuación de nuevas conductas que se han presentado con el uso de las NT, destinadas a la protección de los bienes jurídicos y examinar si las mismas han llenado las expectativas ante el crecimiento desmesurado de la criminalidad cibereconómica. De igual forma, se analizará cuál ha sido la respuesta del derecho penal en el ámbito de la política criminal desarrollada por el Estado, ante este flagelo.

En este orden de ideas, la presente investigación es de tipo documental, con carácter analítico y con un diseño bibliográfico basándose en una amplia y profunda revisión bibliográfica - doctrina y jurisprudencia -, teórico legal -instrumentos legales, nacionales e internacionales-, recolectando información de fuentes documentales y medios digitales como Internet, para analizarlas e interpretarlas con el fin de responder los objetivos trazados.

Producto de la evolución propia de las sociedades modernas, las conductas delictivas han mutado ante dos factores: el primero, la necesidad de salir airoso e impune después de cometer un hecho delictivo -consumado o no-, visto que las técnicas de investigación y medios utilizados para lograr reconstruir los hechos

empleados por los cuerpos policiales están más evolucionadas, tal como se verá en el desarrollo del presente trabajo.

El segundo factor, el uso de nuevas tecnologías genera a los delincuentes menos riesgos frente a la utilización de medios, instrumentos o *modus operandis* tradicionales. El nuevo delincuente suele tener en su haber conocimientos científicos, técnicos, formación académica superior a la media, suele vivir integrado en la sociedad e inclusive asirse de aportes financieros de terceros, y con su conducta lesiona bienes jurídicos sin contacto físico con su víctima.

En España las investigaciones arrojan que la edad de los ciberdelincuentes oscila entre los 18 y 60 años, quienes siempre van un paso delante de los órganos investigadores, en virtud de lo cual, el Estado en ejercicio de su función protectora de bienes jurídicos, debe hacer uso de una política criminal correcta que le permita prevenir, detectar y reprimir dichas conductas.

El sistema jurídico penal español se vio fortalecido en la lucha contra la delincuencia y la protección de los bienes jurídicos más importantes para la sociedad -entiéndase vida, integridad física, indemnidad sexual, seguridad nacional, patrimonio público y privado, protección del mercado, hacienda pública, entre otros- con la puesta en vigencia el 23 de noviembre de 1995 del Código Penal 1 (en lo sucesivo CP), que se estuvo gestando desde 1980.

Una de las principales características de este nuevo cuerpo normativo, es la de agrupar -o al menos intentarlo-, en una forma sistemática de acuerdo al bien jurídico tutelado todos los delitos contra el patrimonio y el orden socio económico en un solo Título y tiene el mérito reconocido e imitado por legislaciones latinoamericanas, de haber logrado este importante avance hacia la unificación.

Este CP ha sufrido diversas reformas entre las que resaltan la de los años 2010, 2015 y la más reciente del 23 de noviembre de 2019, con las cuales se han estado incorporando a la legislación las Directivas de la Unión Europea y agotando con soluciones plausibles las diversas controversias planteadas en la doctrina y jurisprudencia, respecto a instituciones penales como la responsabilidad penal

[1]Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado.* 24 de noviembre de 1995, núm 281, disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1995-25444

corporativa, la administración desleal, el blanqueo de capitales, los delitos de corrupción deportiva y transnacional, entre otros.

Después del año 2000 y a la par de las reformas legislativas se ha ido desarrollando en el campo de la tecnología de la información, una evolución desmesurada de nuevas tecnologías que tuvieron su soporte en la expansión y masificación del uso de Internet. Es innegable que por conducto de ese canal de comunicación digital se transmite y comparte información de la más amplia gama y a gran velocidad entre los diversos continentes, utilizando para ello la fibra óptica[2]. Si bien es cierto que en principio el ideal de los creadores de las nuevas tecnologías era ayudar, facilitar y mejorar la calidad de vida de las sociedades, la delincuencia también ha aprendido a usarlas y las ha destinado a trasgredir la ley con el fin de obtener beneficios económicos.

Para concluir esta introducción, agradezco a Dios por situarme en este camino educativo, así como el apoyo de mi cónyuge, Doris Alejandra -quien escuchaba mis disertaciones sobre la evolución y logros de este trabajo y del Master- mis hijos Diego, Samuel, Sebastián, Santiago y a mi madre Digna Mercedes, al ceder un tiempo del afecto para que pudiera concluir este proyecto con gran alegría y satisfacción personal.

[2] Los cables submarinos en el país ibérico se encuentran anclados al continente en el sur y resaltan el Columbus-III que data de diciembre de 1999 y une Hollywood, Fl, United States con Conil, Spain. https://www.submarinecablemap.com/#/submarine-cable/columbus-iii el Europe India Gateway (EIG) instalado en febrero de 2011 y el Flag Europe-Asia, de noviembre de 1997 con una longitud de 28000km.

II. Consideraciones Generales

2.1. Vínculos entre cibercriminalidad y delitos económicos

El uso de las nuevas tecnologías trae consigo un innegable beneficio para la sociedad moderna, ávida de conocimiento y con extrema necesidad por parte de sus miembros de relacionarse[3]. Sin embargo, proporcional a los beneficios obtenidos han emergido nuevos riesgos que preocupan a la sociedad organizada y a los Estados. Se ha evidenciado que los intereses patrimoniales y socio económicos, no quedan exentos de esta criminalidad, novedosa y cuyo *modus operandi* a evolucionado a la par de las nuevas tecnologías desarrolladas en las últimas dos décadas.

A manera de ejemplo, ante la implementación de controles y medidas anti lavado de activos por parte de los Estados, los criminales han recurrido a la utilización de criptoactivos para esconder las trazas de los procesos de incorporación de sus bienes de ilegal procedencia en los sistemas económicos. Esto es apenas un ápice del gran reto que tienen los Estados en esta nueva era que deben redefinir sus políticas de lucha contra la criminalidad y la resiliencia tecnológica a fin de mantener en un nivel aceptable el impacto de la criminalidad cibereconómica en la sociedad.

No se debe pasar por alto que los fraudes cometidos con medios informáticos fueron las primeras incursiones de la criminalidad cibereconómica, al lado de otras conductas ilícitas sin contenido económico que afectaban directamente a los sistemas de información. Ya SIEBER (1998, p. 3) en su estudio de vital importancia para esta materia, señalaba que los grupos activos del crimen organizado dedicados al espionaje corporativo, habían explotado estas nuevas características del *cibercrime*. Desde el punto de vista histórico el fenómeno de «*computer crime*» o «*computer-related crime»,* como era distinguido anteriormente, data de los años 1960 e incluía el sabotaje, manipulación de *hardware*, espionaje y uso ilegal de sistemas de computación. (SIEBER 1998, p. 18).

[3] Inclusive desde la óptica sociológica se ha incluido en la cohorte demográfica, la denominada generación Z - también conocida como generación posmilénica, *centennial o iGeneration* - sucedánea de la milénica (*millennnials*) como referentes de una carga genética proclive a la adaptación al campo tecnológico.

Paulatinamente, han ido apareciendo nuevas tendencias delincuenciales como el *hacking*, *virus y worms*, hasta llegar a nuestros días con estructuras organizadas dedicadas a cometer delitos cibereconómicos que usan como instrumentos las NT, tales como el espionaje corporativo, fraude, evasión de impuestos, alzamiento de bienes, entre otros.

En la actualidad los ataques a los sistemas de información sin interés ni contenido económico quedaron como un instrumento de acción de grupos políticos o religiosos -*hacktivismo*- o para cometer delitos de terrorismo. Se puede afirmar que existe un descenso del intrusismo y sabotaje informático y un aumento de la criminalidad cibereconómica, lo cual trae consigo una mayor amenaza hacia la estabilidad socio económica de los Estados, afectando la mayoría de las veces a los individuos que lo conforman. Tal como señala MESEGUER (2013, p. 7) hoy la mayor amenaza que se cierne sobre los ordenadores, son las denegaciones de servicio, el uso de dispositivos robados o malintencionados y el *software* malicioso, como, por ejemplo, *ramsonware y bot,* que son desarrollados con el propósito de obtener dinero de forma ilegal.

Resulta un gran desafío para el Derecho y especialmente para el Derecho Penal, estar en sintonía con el desarrollo de NT las cuales generan un ambiente criminógeno de primer orden. Varias iniciativas se han generado para crear conciencia y promover la cooperación internacional en la lucha contra los delitos relacionados con los ordenadores «*Computer-related crime*», entre las que se pueden citar las acciones del Consejo de Europa[4], el Grupo de los 8[5] y la Organización para la Cooperación y el Desarrollo Económico y los Estados (OCDE)[6], lo cual permite aseverar que es de vital importancia para los Estados crear en sus propias legislaciones una respuesta en el ámbito de la prevención y represión contra este tipo de conductas (SÁNCHEZ, 2008, p. 149).

[4] Que tuvo su concreción en el convenio sobre la ciberdelincuencia (2001).
[5] Recomendaciones y principios adoptados en 1996 y 1997 para la lucha contra la delincuencia de alta tecnología.
[6] La OCDE realizó en el año 1985 y 1992 varias recomendaciones para la tipificación de determinadas conductas producto del estudio de la criminalidad informática efectuada por el comité ad-hoc (Ad hoc committee on computer crime) y medidas dirigidas a la seguridad informática.

Como se ha percibido en el transcurrir de estos cuatro lustros, el *loci delicti commissi* o sitio de comisión del delito en el ámbito de los hechos punibles generados tanto por las TIC o por las NT se ha amplificado, extrapolando sus efectos a los territorios de diversos Estados -tanto la acción, desarrollo o resultado del *iter criminis*- en virtud de lo cual se ha concebido una doble o múltiple incriminación en la legislación de los Estados afectados, con el propósito final de cooperar en la investigación y persecución de los victimarios en forma activa y efectiva. El principio de la doble incriminación constituye la base fundamental para los Tratados de extradición y de asistencia jurídica mutua, instrumentos pertinentes para lograr la coordinación extraterritorial y avanzar en la lucha contra la criminalidad cibernética.

La afectación de los bienes jurídicos tradicionales -propiedad, intimidad, estabilidad financiera, administración de justicia- producto de los delitos cometidos con las NT deben ser objeto de un análisis jurídico penal constante, con apoyo criminológico, para identificar las formas de afectación y producir en el plano legislativo nuevas tipologías o la adecuación de las existentes con la inclusión de agravantes cualificadas en virtud del medio o instrumento usado para la comisión del delito.

Con la actualización en el sistema de justicia penal se genera una respuesta político criminal adecuada por parte del Estado con el fin de proteger de la delincuencia informática, los bienes jurídicos que son importantes para la sociedad, sin caer en el casuismo que atenta contra los principios de mínima intervención y subsidiariedad del derecho penal.

Sobre la base de una perspectiva criminológica, el concepto de delincuencia informática, expresión usada para identificar un objeto relativamente impreciso (ANARTE 2001, p. 8) se ha suplantado dicho término por el de ciberdelincuencia (MIRÓ 2011, p. 3), una traducción del anglicismo *cybercrime o cybercriminality*. Esta nueva expresión resulta más acertada para referirnos a los delitos cometidos en las redes informáticas (o a través de ellas) y engloba los delitos informáticos y los delitos cibernéticos.

El padre fundador de la cibercriminología, JAISHANKAR (2018, p. 2), la considera una sub disciplina de la Criminología que estudia las causas de los delitos que ocurren en el ciberespacio y su impacto en el espacio físico. Como producto del

uso de las TIC y de las NT que se han desarrollado en los últimos años, se ha observado un pujante incremento de la criminalidad cibereconómica que debe ser analizada constantemente para no perder de vista el escalamiento y desarrollo, y generar a partir de su observación, nuevas medidas de prevención en ciberseguridad.

No se puede pasar por alto que, a diferencia de la criminalidad tradicional, que se mantiene estática o con una mutación muy lenta en cuanto a la forma de cometer delitos, la criminalidad cibereconómica va evolucionando de la mano de las NT en las cuales invierte recursos y tiempo para adquirirlas, conocerlas y usarlas, esperando obtener un beneficio económico superior.

La participación de la criminología en apoyo a la ciencia jurídica es fundamental, ya que aborda desde su campo de acción entre otras cosas, las características especiales de los sistemas informáticos que los convierten en objetos o instrumentos cualificados del delito (MATA 2003, p. 35) y el estudio de la perfilación criminal del ciberdelincuente.

Desde el punto de vista estadal, el documento contentivo de la Estrategia Nacional de Ciberseguridad de 2019, definió la cibercriminalidad como:

«*el conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de Cyberdelito, o en su caso, de hacktivismo*».

Para controlar la cibercriminalidad el gobierno español ha dispuesto en dicho documento cinco objetivos específicos:

- Seguridad y resiliencia de las redes, sistemas de información y comunicaciones del sector público y de los servicios esenciales
- Uso seguro y fiable del ciberespacio frente al uso ilícito o malicioso
- Protección del ecosistema empresarial y social de los ciudadanos
- Difusión de la cultura de la ciberseguridad
- Potenciación de las capacidades humanas y tecnológicas.

Como corolario de lo antes expuesto, se puede afirmar que los factores criminógenos relevantes que traen los modernos ordenadores y las redes de comunicación -inexperiencia de algunos usuarios, posibilidad de interacciones

remotas, anonimato de los delincuentes, alcance mundial de Internet, encriptación de datos, desterritorialización, la rapidez del ciclo de innovación- permean en los delincuentes para avanzar en nuevas conductas delictivas.

EL uso de la TIC para cometer delitos ocasiona grandes problemas en el campo de la investigación penal, por la dificultad de reconstruir mediante pruebas tradicionales la forma en que acaecieron los hechos, con el fin de convencer a los juzgadores y a la comunidad, que se está persiguiendo en forma efectiva la criminalidad y generar en aquellos una sensación de seguridad. Hay que tomar en consideración, que los medios probatorios tradicionales y su naturaleza instrumental en el proceso penal deben ser adaptados a las exigencias de un mundo globalizado e interconectado.

2.2 Breves anotaciones sobre las nuevas tecnologías con relevancia jurídico penal

Existía una creencia en diferentes sociedades del mundo occidental que, con el arribo del siglo XXI, se producirían diversos cambios en los sistemas de la tecnología de la información que conducirían a la paralización de los sistemas de producción, comercio y todos aquellos que estuvieran ligados con un equipo informático. Esto quedó en una simple leyenda, al contrario, el uso de las tecnologías creció exponencialmente en los años subsiguientes.

Con base a la existencia y desarrollo de la aldea global[7] la ampliación de la conexión entre los países vía fibra óptica o *fiber to the home* (FTTH) fue el factor desencadenante de la aparición de nuevas tecnologías que utilizan la gran carretera de la información para comunicarse, transmitir información, ejecutar comandos a distancia, intercambiar servicios, entre otros. La ampliación de la banda de transmisión de datos mediante el uso de la fibra óptica a los nodos de los diversos países, sean privados o públicos, ha aminorado la brecha de la evolución entre naciones y ha permitido que sociedades que antes utilizaban internet de segunda

[7] El termino aldea global, fue acuñado por Marshall McLuhan y se refiere a que las personas gracias a la televisión, radio y los medios tecnológicos pueden enterarse qué pasa en cualquier lugar. La aldea global supone la desaparición de las distancias físicas para generar conocimientos.

generación evolucionaran a la recepción de contenido en *streaming*, video conferencias, publicación de imágenes en alta resolución, etc.

Conforme señala MATA MARTÍN «Internet ha supuesto un cambio tan espectacular en las posibilidades de comunicación e intercambio de información en el contexto global que, desde una perspectiva histórica ha sido comparado con la revolución industrial o con hitos históricos de semejante magnitud» (2003, p. 21).

Internet se basa en la posibilidad de que los usuarios (internautas) puedan acceder al contenido de páginas web que realizan personas jurídicas públicas y privadas, universidades y colegios, entre otros, a nivel mundial. Mediante ella pueden estar conectados en España y conocer o navegar a la página web de una empresa con sede en Australia, por ejemplo.

De acuerdo a los investigadores de Panda Security, el contenido que se puede accesar por este sistema es del 4% total del mundo web[8], es decir el noventa y seis por ciento (96%) de la *world wide web* son páginas que no están indexadas por los grandes buscadores, y son conocidos como *deepweb, dark web* o internet profunda.

Una de las características más representativas de la *deepweb* son los medios de pago utilizados para adquirir productos y servicios, en ella se aceptan *bitcoin* y otras criptomonedas, con la finalidad de preservar el anonimato en las transacciones. Las características de la deepweb ayudan para la comisión con regularidad de delitos como estafas o *scam*, por cuanto se paga por un producto que en muchas ocasiones no llega a la dirección del usuario, sin entrar a analizar los otros servicios ilícitos (drogas, sicariato, venta de datos, pornografía infantil) que son ofrecidas en este sub mundo digital.

La existencia de la *deepweb* ha ocupado al poder judicial, a tal punto que la sección segunda de la Audiencia Provincial de Tenerife, en sentencia No. 294/2018, de 3 de octubre declaró por probado que en la investigación realizada por la Guardia Civil se efectuó el control de los envíos de paquetes postales procedentes de Alemania, quedando oculta la identidad de los usuarios de los envíos al utilizar la red oscura o *Darknet*, mediante el uso de la red TOR acrónimo de "*The Onion Router*", que se ha desarrollado de forma superpuesta a Internet. Asimismo, quedó

[8] https://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/ visitado el 24 de abril de 2020.

demostrado que utilizaban para las compras de las sustancias estupefacientes la moneda virtual denominada *Bitcoin*, no dejando rastros ni identificación del sujeto que hacía el envío de las sustancias.

Otra de las NT que ha escalado en la última década, es el *cloud computing* definido como un modelo para hacer posible el acceso a red adecuado y bajo demanda a un conjunto de recursos de computación configurables y compartidos (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) cuyo aprovisionamiento y liberación puede realizarse con rapidez y con mínimo esfuerzo de gestión e interacción por parte del proveedor del *cloud*[9]. El desarrollo de los servicios empresariales y personales basados en la *cloud* ha avanzado en los últimos tiempos, por la versatilidad de poder accesar a los datos alojados en la nube desde cualquier localización, los bajos costos operativos que genera y la posibilidad de tener todos los documentos, data y aplicaciones en un solo sitio.

Se ha reportado a nivel mundial numerosos ataques a los sistemas de *cloud computing*, para ello, los ciberdelincuentes utilizan técnicas de inteligencia social para hacerse de las contraseñas, además de modalidades de *pishing* e inclusive técnicas de fuerza bruta. Una vez que ingresan a la nube suelen avanzar en posiciones dentro del sistema, desplazándose de forma lateral mediante el uso de mensajes internos de *pishing* para infectar a otros usuarios[10].

Dentro de la amplia gama de amenazas que ha sido señalada por la *Cloud Security Alliance* (CSA) ll y que tiene relevancia para el derecho penal económico, se encuentran las amenazas por la pérdida o fuga de información y el secuestro de sesión o servicio.

Los ataques de los delincuentes cibereconómicos en la época actual con la pandemia del Covid-19 han aumentado, al extremo de afectar los sistemas de instituciones hospitalarias. Tal es el caso del virus tipo *ransonware*[11], conocido como

[9] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf consultado el 24 de abril de 2020

[10] https://cuadernosdeseguridad.com/2019/03/los-ataques-a-aplicaciones-cloud-aumentan-un-65-en-el-primer-trimestre-de-2019/ consultado el 24 de abril de 2020

[11] Para Pandasecurity el ransonware es un software malicioso que al infectar el equipo informático, le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota, encriptar los archivos y pide el pago de un rescate para reintegrar el control de la información. https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/ consultado el 18 de Julio de 2020

"serpiente", que comprometió el sistema informático del hospital Fresenius, ubicado en Alemania considerado el más grande de Europa. Este virus ha atacado desde comienzo del año y busca el pago de un rescate por parte de las corporaciones afectadas. Es de resaltar como en estos ataques, se mezclan la TIC y las criptomonedas, esta última para obtener anonimato al recibir el beneficio económico.

En otro orden de ideas, la evolución de una NT, de uso constante y masivo, que ha sido considerada disruptiva por la sociedad del nuevo milenio es el conocido como Internet de las cosas (en lo sucesivo IoT), el cual se puede definir como una innovación tecnológica que tiene como objetivo conectar los ítems que usamos diariamente con Internet, con el objetivo de aproximar cada vez más el mundo físico a la digital [12].

El autor de este concepto, Kevin Aston, es un tecnólogo y experto en transformación digital que lo acuñó en su artículo «*That 'Internet of Things' Thing*»[13], elaborado cuando estudiaba en el *Massachusetts Institute of Technology* (MIT). Aston, laboraba en 1999 en *Procter & Gamble*, como Ejecutivo Junior. La empresa tenía un problema de gestión de negocios por cuanto uno de sus principales productos del área cosmética se agotaba en cuatro de diez tiendas, mientras que en el almacén de P&G había inventario suficiente[14]. Analizaron la problemática y con la instalación de un microchip de identificación por radiofrecuencia en red (RFID) lograron darle solución.

La evolución del esquema inicial de lograr que los ordenadores se comuniquen con los objetos ha llevado a la interconectividad bajo la plataforma de

---

[12] https://www.hostgator.mx/blog/Internet-de-las-cosas/?__cf_chl_captcha_tk__=ca4b47be6c3be26359d2ab3bb9164e1c65bbc140-1587901341-0-AaeAUL5blDmYDFMZ2wZdUGO-d9XnLK4QcS4TKqJ7ZJVwIGkDB2N2Suo-DDM5hCKVexNl1qPio_x2zflzDcS7uqZDSrrj-TcLI9n7HE9PeD3L_G4bBgadT0j8NW1SzhFcwZq0Nc2lwZsZu6HtDR_Vmm7CDvNhxPdgy8-KDEc_yGVBPEpiaiguVF4yhsUHPYASXgn8UzcUew2BhTwzTjSsLsnj4jltp4nfRXBtMwysuOX3fM_hLce8BeROf3p-p6nuaOo0L2ljj44X9e-k4_AcR1oJedzt-KwhFp2xGzv6B-6AIUT_k9rA7j7bHOaSdVmdxaPyTj5wEs2ISwUq-MN9bYSD6dISv5hRlGBTvO0XshzKygBuunH0VI775cegsZRGj5wW5rKfV0CzxuSsTr8XsVptjIMENY3aZ3DS8WfjaBeveBNRfGKt5rI5MEPFpG12VOo2JD2AhEdMUgQk9rvxlGheqiLYyPWAdtQc2ZfOe2megOuu7l94a-dDPlbJ4JcfsEKmVWhPZ1g2fxSVpYf7kLY consultado el 26 de abril de 2020.

[13] https://www.rfidjournal.com/articles/view?4986 consultado el 25 de abril de 2020

[14] http://www.eexcellence.es/index.php/expertos-en-gestion/kevin-ashton-un-tecnologo-visionario consultado el 26 de abril de 2020.

Internet. IoT está presente en nuestras vidas desde que nos levantamos, a tomar un café recién colado en la cafetera eléctrica inteligente, el reloj que mide las pulsaciones cardíacas y las calorías activadas diariamente, las cámaras *wi-fi* que permiten monitorear nuestro hogar u oficinas, en fin, se han hecho tan común la utilización de esta *technology* que muchas veces pasa desapercibida.

El creciente desarrollo de IoT, genera un desafío para el derecho penal cuantitativamente igual o superior al ocurrido con el advenimiento de Internet. Los millones de objetos de uso diario conectados a Internet avizora una fuente exponencial de posibles herramientas tecnológicas para cometer hechos punibles, que en nuestra área serían de carácter económico. Los nuevos retos que tienen los desarrolladores, se refieren no solamente a la evolución, calidad y usabilidad de los productos, sino a garantizar la seguridad para los usuarios finales de estas nuevas tecnologías. Los ciberdelincuentes exploran las brechas de como colarse entre los *firewall* y sistemas encriptados de transmisión de data de IoT para violar los mecanismos de seguridad y poder cometer delitos de mayor relevancia, delitos con contenido económico.

La amenaza que representa el uso indiscriminado y creciente de IoT por parte de los ciberdelincuentes ha llamado la atención al Parlamento Europeo en cuyo informe de sesión del 25 de julio de 2017, ha considerado la posibilidad que mediante el *hackeo* o pirateo informático de las cosas conectadas a Internet puedan suponer una amenaza concreta para la vida de los seres humanos[15] (Informe A8-0272/2017 p. 7), en virtud de lo cual se requiere a los fabricantes de equipos y desarrolladores de *software* invertir en soluciones de seguridad que impidan los delitos cibernéticos, con arreglo a la legislación de la Unión Europea y a la Directiva de Seguridad de las redes y de la información[16] (SRI).

Desde el punto de vista del Derecho Penal Económico, IoT tiene relevancia en la ocurrencia del delito de espionaje y consecuente revelación de secretos comerciales, así como la proclive incidencia en la seguridad laboral. De este modo se

[15] https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_ES.html consultado el 10 de junio de 2020

[16] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32013L0040 consultado el 10 de junio de 2020

observa que la amenaza a distintos bienes jurídicos, incluyendo los que protegen el derecho a la privacidad e intimidad, con la utilización de esta NT para obtener datos privados de los usuarios, es totalmente cierta y grave.

En la actualidad se están presentando casos de entidades que se dedican a prestar servicios de espionaje corporativo de acuerdo a las necesidades y requerimientos de los clientes. Tal es el caso reportado por Kapersky Lab una empresa global de seguridad informática en el año 2016, en el cual detectaron la actuación de la empresa Saguaro de origen mexicano, que se encargaba de espiar y robar información confidencial de empresas y particulares mediante una combinación de *pishing*, macros, *malware* y *back door*.

Se puede afirmar que la figura del *insider*, esa persona que valiéndose de su posición laboral y con la obligación de guardar reserva en una empresa presta sus credenciales o claves para accesar a la base de datos o *cloud* de su empleador que está penado en el CP, en el art. 279, ha quedado en un plano de menor importancia para las estructuras de delincuencia organizada. El riesgo de que sea develada la autoría intelectual del acceso a los datos corporativos, queda prácticamente disminuido ante la utilización de *outsourcing* de delincuencia cibereconómica dedicada a prestar este servicio[17].

La protección de los bienes jurídicos que se han señalado en líneas anteriores, considerados relevantes para la sociedad por parte del Estado, en los actuales momentos se encuentra limitada a obligaciones de carácter administrativo, para las empresas prestadoras de servicios y fabricantes de *software* y *hardware* de IoT, que deben invertir en soluciones de seguridad para evitar la consumación de los delitos mediante el uso de esta tecnología. Por tanto, las transgresiones que ocurran con el uso de IoT como instrumento, serán penadas con los tipos penales vigentes.

[17] Uno de los mas utilizado es Pegasus, un software malicioso de origen Israelí destinado a recabar información de teléfonos móviles.

III. La criminalidad cibereconómica como forma de delincuencia organizada transnacional

3.1. Rasgos definitorios

En un primer momento al escuchar el término de delincuencia organizada transnacional (en lo sucesivo DOT) nos llega a la memoria la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (en lo sucesivo UNTOC) conocida como Protocolo de Palermo[18], aprobado en el año 2000 por la Oficina de las Naciones Unidas Contra la Droga y el Delito (en lo sucesivo UNODC) la cual tiene como finalidad el diseño y armonización de políticas públicas con el fin de luchar contra la delincuencia estructurada que comete delitos graves y que afectan a diferentes países. De acuerdo a la UNODC la DOT abarca prácticamente todos los actos delictivos de carácter internacional cometidos con fines de lucro y relacionados con más de un país [19].

El ataque a los bienes jurídicos más importantes para las naciones libres por cuenta de grupos estructurados, dedicados a cometer delitos de drogas u otros delitos graves que afecten a varios países, de forma reiterada y sostenida en el tiempo, fue el fundamento principal de la Convención. Es decir, si la delincuencia atraviesa las fronteras, lo mismo ha de hacer la ley. Si el imperio de la ley se ve socavado no sólo en un país, sino en muchos países, quienes lo defienden no se pueden limitar a emplear únicamente medios, procedimientos y arbitrios nacionales.

Ahora bien, cabe preguntarse ¿los delincuentes cibereconómicos podrían ser considerados grupos de delincuencia organizada? Y de ser afirmativa la respuesta, aplicarles las leyes, tratados internacionales y normas de asistencia en el proceso de investigación propias de este tipo de delincuencia.

Los delitos de DOT son considerados *numerus apertus*, en sus inicios destacaban en el elenco el blanqueo de capitales producto de la comisión de delitos

[18] Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf consultado el 17 de mayo de 2020.
[19] https://www.unodc.org/toc/es/crimes/organized-crime.html consultado el 17 de mayo de 2020.

de DOT, delitos de corrupción, trata de personas, tráfico de inmigrantes, tráfico de armas y órganos y, venta de medicamentos adulterados, no obstante, se pueden catalogar de DOT todos aquellos delitos graves, cuya pena establecida como castigo supere los cuatro (4) años y sean realizados por un tres o más personas, organizadas estructuralmente para cometerlos. Como producto de esta característica la Convención es aplicable a la lucha contra las nuevas conductas, que tengan un fin económico y que se vayan originando en el tiempo, siendo una de ellas la criminalidad cibereconómica.

Es menester distinguir en la cibercriminalidad, con o sin fines económicos, al igual que un *hacker* puede actuar en forma individual o integrar grupos de DOT. También puede ocurrir que quien actúa en solitario se convierte en un eslabón de la estructura de un grupo de DOT, para cumplir un fin o misión en específico integrándose con sus conocimientos sobre las TIC o las NT.

La participación en un grupo de delincuencia organizada por parte del ciberdelincuente puede tener uno o varios roles, como podría ser el proveer un servicio externo o tercerizado (*outsourcing*) a los grupos de DOT sin pertenencia fija en la estructura. Ejemplo de ello sería el caso del blanqueo de capitales mediante la adquisición de criptomonedas, en la cual los delincuentes cibereconómicos tiene como fin convertir el dinero producto de la comisión de delito en dinero lícito. Otra modalidad de actuación del ciberdelincuente en la DOT puede ser con la asistencia tecnológica en el proceso de comisión de delitos graves, ya sea en el momento de producción del delito o a posterioridad para evadir la persecución.[20]

Antes de avanzar en el análisis de los mecanismos diseñados por la comunidad de Estados en la lucha contra la DOT es pertinente señalar con base al documento de la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave de 2019, las características que en algunas ocasiones son compartidas por grupos de DOT.

1. Las actividades ilegales desarrolladas, tiene una finalidad económica, la obtención de dividendos es su principal distinción;

2. Tienen una estructura jerárquica compleja donde están delimitados los roles, funciones, responsabilidades y actividades de cada uno de sus miembros;

[20] Is the mafia taking over cybercime? https://i.blackhat.com/us-18/Wed-August-8/us-18-Lusthaus-Is-The-Mafia-Taking-Over-Cibercrime-wp.pdf fue consultado el 18 de mayo de 2020

3. Son constituidos para actuar durante un período de tiempo largo, tienen un carácter de permanencia dedicados a cometer delitos graves;

4. Tienen previstos los canales para la incorporación de los beneficios obtenidos producto de la comisión de delitos en la economía de los países, utilizando para ello corporaciones que realizan actividades lícitas;

5. Ante la respuesta punitiva del Estado que persigue y sanciona las actividades de los grupos de DOT, estos se reinventan y adaptan creando nuevas formas de acción, métodos y rutas para evadirlas;

6. Otra de sus principales características es su transnacionalidad, se aprovechan de la globalización para actuar más allá de las fronteras de sus países;

7. Toman medidas de protección para contrarrestar el riesgo que otros grupos de DOT quieran competir en su campo de acción o para salvaguardarse de las acciones del Estado. En algunos casos, establecen lazos con individualidades o grupos políticos para ejercer presión en aspectos de su interés[21].

Las características antes señaladas en dicho documento presentan semejanzas con los factores mencionados en el Informe Anual del año 1997 de la Unión Europea sobre la situación del Crimen Organizado [22] citado por LÓPEZ-MUÑOZ (2015 p. 40-41) considerándose indispensables los siguientes: número de colaboradores, la permanencia en el tiempo, la comisión de delitos graves y la búsqueda de beneficio o poder económico.

En palabras de GONZÁLEZ (2017) el aporte de la ciberdelincuencia en la comisión de delitos tradicionales, está permitiendo a los grupos del crimen organizado, no sólo ampliar sus esferas de actuación, sino también su influencia a nivel internacional y su capital al aumentar enormemente sus ganancias y ámbitos de operación. Así, el cibercrimen otorga beneficios de enormes y crecientes dimensiones a los grupos de la delincuencia organizada transnacional, favoreciendo su expansión y empoderamiento a lo largo y ancho del planeta.

Partiendo del análisis de la tipología, medios de comisión y estructura organizativa para cometer los ilícitos penales, y una vez satisfechos los requisitos

[21] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-2442 consultado en fecha 18 de mayo de 2020

[22] Documento 6204/1/97 (EMFOPOL 35 rev. 2, de 1997)

anteriormente señalados en la lucha contra la criminalidad cibereconómica, se puede aplicar el marco regulatorio establecido por las Naciones Unidas, la Unión Europea y las organizaciones de países latinoamericanos para la investigación y persecución de los delitos cometidos, las cuales veremos a continuación.

3.2 Marco regulatorio de la cooperación judicial internacional

En criterio de SANCHEZ (2008, p. 257) «la cooperación judicial se dirige a ayudar a otro Estado a reparar un déficit procesal causado porque el autor o los medios de pruebas necesarios están fuera del Estado», y distingue tres pilares esenciales integrantes de la cooperación, que se mencionan a continuación.

La forma tradicional de ayuda en materia penal, conocida como extradición[23] que consiste en un procedimiento penal[24] que ocurre entre dos Estados soberanos mediante el cual, el Estado requerido entrega al Estado requirente -actuando con plena jurisdicción para juzgar el hecho- a una persona que está siendo procesada o fue condenada por la comisión de delitos tipificados en las legislaciones de ambos países con pena superior a 1 año de privación de libertad.

Existen otros mecanismos de asistencia judicial que complementan a la extradición y que nacieron después de la segunda guerra mundial, entre los cuales tenemos, la restitución de objetos producto de delito, el traslado temporal de un Estado a otro, de detenidos con fines de investigación, la toma de declaraciones testimoniales mediante la telemática, las entregas vigiladas en territorio de otro Estado, establecimiento de equipos de investigación conjunta, facilitación en la entrega de documentos, información u otros elementos de prueba, etc.

Son diversos los tratados bilaterales y multilaterales que han sido suscritos por los Estados en las últimas décadas en la lucha contra la delincuencia organizada

[23] La convención sobre extradición fue suscrita en 1933, en Montevideo en el marco de la VII Conferencia Internacional Interamericana, consultado el 4 de junio de 2020. http://cedhvapp2.sytes.net:8080/derechos_humanos/file.php/1/Instrumentos%20internacionales%20DH/22abis.pdf

[24] Existen varias excepciones para que un Estado niegue la extradición, entre las cuales se puede citar: que la persona sea nacional del Estado requerido, que la acción penal o la pena para perseguir el delito de acuerdo a la legislación de ambos Estados esté prescrita antes de la detención del individuo; cuando esté siendo juzgado en el Estado requerido por el delito perseguido en el Estado requirente; cuando se trate de un delito político o conexo por el cual se persigue; cuando se refiera a delitos militares o religiosos, entre otros.

transnacional. En el presente capítulo nos detendremos a señalar de forma sucinta los principales, con el propósito de elevar los métodos diseñados y empleados en la lucha contra la DOT, y por ende dar a conocer los instrumentos con que cuentan los Estados a la hora de perseguir y sancionar la criminalidad cibereconómica.

En el ámbito de las Naciones Unidas la promoción de la cooperación internacional en la materia repercute con mayor importancia en el V Congreso de Naciones Unidas sobre la Prevención del Crimen y el Tratamiento de los Delincuentes (Ginebra 1975). A posterioridad, continuaron trabajando sobre las herramientas de cooperación internacional, siendo la Conferencia Mundial Interministerial sobre el Crimen Organizado Transnacional de Nápoles de 1994 el paso más trascendental tomado por los Estados y concluyó en la elaboración de la Convención sobre el tema.

Para el año 2000, en la ciudad de Palermo, Italia se firmó la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional que se complementó con tres protocolos[25], siendo el resultado del trabajo que habían desarrollado en las reuniones de alto nivel bajo el amparo de las Naciones Unidas. El principal objeto de esta Convención es promover la cooperación entre los Estados para prevenir y combatir más eficazmente la delincuencia organizada transnacional[26] y dispuso en su articulado, además de la figura de la extradición[27] formas de cooperación internacional, tales como el auxilio para ejecutar un decomiso a solicitud de un Estado parte sobre bienes ubicados en un tercer Estado[28], la transmisión de información sobre procesos penales entre los Estados partes de forma espontánea[29], el traslado de detenidos o condenados para colaborar en investigaciones en curso[30], la recepción de declaraciones testimoniales a testigos o peritos mediante videoconferencia[31], presentación de documentos judiciales, examen de objetos y lugares (inspecciones), suministro de originales o copias certificadas de documentos

[25] Protocolo para la prevención para la prevención, supresión y punición del tráfico de personas, especialmente de mujeres y niños; Protocolo contra el contrabando de emigrantes por tierra, mar y aire; Protocolo contra la fabricación y tráfico ilícito de armas de fuego, sus partes y componentes de municiones.
[26] Art. 1, UNTOC
[27] Art. 16 UNTOC
[28] Art. 13 UNTOC
[29] Art. 18.4 UNTOC
[30] Art. 18.10 UNTOC
[31] Art. 18.11 UNTOC

y expedientes pertinentes, creación de órganos mixtos para desarrollar investigaciones que afectan a dos o más Estados[32], entre otros.

La Convención de Palermo representa un instrumento fundamental en la lucha contra la DOT, ha sido ratificada por muchos países y sus estándares de cooperación judicial pueden ser aplicados en el proceso de investigación de los delitos cibereconómicos y la persecución de la cibercriminalidad en general. La Convención de Palermo si bien es el tratado referente en la lucha contra la DOT, sin embargo, no es el más longevo. En el seno del Consejo de Europa estaba vigente desde 1957 el Convenio Europeo de Extradición, ratificado por España el 6 de agosto de 1982[33] y el Convenio Europeo de Asistencia Judicial en Materia Penal[34] suscrito en el año 1959, el cual tiene una vigencia fundamental ya que los tratados posteriores que rigen la materia hacen referencia a este convenio (SANCHEZ 2008, p 260).

Es de resaltar que en el Convenio Europeo de Asistencia Judicial en Materia Penal se basa en la cooperación activa entre los Estados partes en los procesos penales que sean competencia del Estado requirente, y se podrá denegar la asistencia en los supuestos de infracciones de carácter político, fiscales o cuando lo solicitado pudiese afectar el interés público o soberanía del estado requerido (Art. 2). El ámbito de cooperación referido en el convenio, tiene que ver con la transmisión de piezas o partes del expediente, toma de declaración bajo juramento de testigos y peritos, envío de copias certificadas de expedientes solicitados (Art. 3), notificación de documentos procesales y resoluciones judiciales y expedición de antecedentes penales (Art. 13).

Con la entrada en vigencia de la Unión Europea, a partir de la firma del Tratado de Maastrich en 1992 los Estados partes han desarrollado mecanismos más expeditos de apoyo en la cooperación judicial, en cuyas materias queda incluida la penal. La tendencia que se observa en la asistencia, es hacia la facilitación de la extradición, prevención de conflictos de jurisdicción y fomento de la cooperación entre autoridades en relación con las causas y ejecución de decisiones que se inició con la firma del Tratado de Amsterdam en 1997 (SANCHEZ, 2008 p. 265).

---

[32] Aer. 19 UNTOC

[33] https://www.boe.es/buscar/doc.php?id=BOE-A-1982-13611, consultado el 5 de junio de 2020

[34] https://www.boe.es/buscar/doc.php?id=BOE-A-1982-23564 , consultado el 5 de junio de 2020

Finalmente, en el Tratado de Niza (2001) se concibe la creación de la Unidad Judicial de Cooperación Judicial, denominada Eurojust[35] conformada por fiscales, jueces y policías, teniendo como fin la lucha contra la delincuencia grave, entre las cuales se observa la delincuencia informática (Art. 4.1, b). En resumen, la Eurojust tiene un papel fundamental en la coordinación para lograr la efectiva cooperación judicial entre los Estados partes, y debe mantener una estrecha cooperación con la Europol, organismo al que vamos a dedicar un apartado por su relevancia en la lucha contra la ciberdelincuencia.

La piedra angular de la cooperación penal en la Unión Europea es la orden de detención y entrega europea, conocida como euroorden, que en palabras de DÍAZ (2010, p. 185) supone la evolución natural de la extradición, constituyendo un procedimiento expedito y con escasos condicionantes para la entrega de una persona que está siendo peticionada por la autoridad judicial de otro estado miembro.

En definitiva, la cooperación de la Unión Europea ha estado evolucionando para lograr el espacio de libertad, seguridad y justicia propugnado por los Estados que la conforman y con el Programa de Estocolmo en el año 2009, se profundizó en la modernización de los instrumentos de trabajo o el refuerzo de la cooperación policial contra las formas graves de delincuencia y delincuencia organizada, entre las que cuenta, la delincuencia cibernética (ALLI, 2016 p. 205).

En el contexto de los países de América fue adoptado por los Estados miembros de la Organización de Estados Americanos (en lo sucesivo OEA) en el año 1981 la Convención Interamericana sobre Extradición[36] en la cual se reafirma la obligación de los Estados Partes de entregar a las personas requeridas judicialmente bien para procesarlas o las que hayan sido declaradas culpables. Además, se cuenta con una Convención Interamericana sobre Asistencia Mutua en Materia Penal (1992)[37] que prevé un mecanismo expedito para la ayuda judicial en investigaciones, juicios y actuaciones con ocasión a la práctica de notificación de resoluciones y sentencias, recepción de testimonios, citación de testigos y peritos, práctica de

[35] Decisión 2002/187/JAI del Consejo de 28-02-2002 https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32002D0187 consultada el 7 de junio de 2020
[36] https://www.oas.org/juridico/spanish/tratados/b-47.html consultada el 7 de junio de 2020
[37] https://www.oas.org/juridico/spanish/tratados/a-55.html consultada el 7 de junio de 2020

embargos y secuestro de bienes, práctica de inspecciones en lugares y a objetos, remisión de documentos, traslado de personas detenidas, entre otros.

Sin diferencias notables en el contexto del ámbito de cooperación judicial el Consejo del Mercado Común del Sur (en lo sucesivo Mercosur) también dispuso de instrumentos similares, el Protocolo de Asistencia Jurídica Mutua en Asuntos Penales[38] y el Acuerdo sobre Extradición entre los Estados Partes del Mercosur[39].

3.3 Participación de la Europol en la lucha contra la cibercriminalidad

Como punto previo es importante destacar la importancia que tiene la Organización Internacional de Policía Criminal (en lo sucesivo Interpol) en la lucha contra los delitos transnacionales. Esta organización tiene su sede en Lyon, Francia y mantiene representación permanente -Oficina Central Nacional de Interpol- en ciento noventa y cuatro (194) países, tiene como fin principal facilitar el intercambio y acceso a la información sobre delitos y delincuentes, aporta apoyo técnico y operativo de diversa índole[40]. La Interpol coloca a disposición de los estados un sistema tecnológico cifrado denominado I-24/7 conectado a dieciocho (18) bases de datos policiales con información sobre delincuentes y delitos, apoya a los Estados miembros en el proceso de investigación, en materia forense y en la localización de fugitivos.

Sin ánimos de restar la relevancia que tiene la Interpol en la lucha contra la DOT el presente trabajo se centrará en la actuación de la Europol tomando en cuenta que es un órgano adscrito a la Unión Europea y creó el Centro Europeo de Cibercrimen (en lo sucesivo EC3) dedicado exclusivamente a la lucha contra la cibercriminalidad.

Desde la firma del Tratado de Masstricht, uno de los pilares fundamentales de la integración ha sido la creación de un mercado único con libertad de circulación de

[38] http://www.oas.org/juridico/spanish/tratados/sp_proto_asis_jur%C3%AD_mutua_asun_pena_mercosur.pdf consultado el 7 de junio de 2020

[39] http://www.oas.org/juridico/spanish/tratados/sp_acuer_sobre_extra_ent_esta_part_mercosur.pdf consultado el 7 de junio de 2020

[40] https://www.interpol.int/es/Quienes-somos/Que-es-INTERPOL fue consultado el 18 de mayo de 2020

mercancías, servicios, personas y capitales, por los veintisiete (27) países que conforman la zona euro. La agencia de la Unión Europea para la cooperación policial, conocido como Europol con sede en la Haya (Países Bajos), fue constituida inicialmente como una unidad de drogas (EDU)[41] e inició sus actividades en enero de 1994.

Posteriormente y vistos los nuevos riesgos a los cuales estaban expuestos los nacionales europeos fueron agregando nuevas áreas, hasta que en 1999 fue redefinida la estructura como se conoce en la actualidad. La Europol es la organización de cumplimiento de la ley de la Unión Europea que gestiona informaciones sobre el delito, su objetivo es mejorar la efectividad y la cooperación de las autoridades competentes de los Estados miembros en la prevención y la lucha contra la delincuencia internacional organizada grave y el terrorismo.[42]

La Unión Europea ha estado consciente de los riesgos y amenazas que comporta para los Estados el uso y avance de las tecnologías de la información, considerándose oportuno mencionar las decisiones marco que crearon la EC3, de las cuales se puede evidenciar el interés puesto por los Estados para la protección de la ciudadanía en la utilización de las TI. En el año 1999, fue publicada la Decisión No. 276/1999, en la cual se dispuso como objetivo, propiciar una mayor seguridad en la utilización de Internet y fomentar a nivel europeo la creación de un entorno favorable para el desarrollo de la industria respectiva.[43]

Para el año 2005, este plan es repotenciado en la decisión No. 854/2005/CE «Una Internet más segura plus» vista la creciente penetración de Internet y el uso de nuevas tecnologías, como la telefonía móvil. En esta época resultaba de importancia a la Unión Europea al contenido ilícito -pornografía infantil y material racista- y potencialmente nocivo a los niños, así como el contenido no deseado (*spam*)[44]. En la

[41] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELLAR:7f9036bd-ac1d-4305-887d-4c5841f9279b&from=FR fue consultado el 6 de mayo de 2020

[42] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELLAR:7f9036bd-ac1d-4305-887d-4c5841f9279b&from=FR fue consultado el 6 de mayo de 2020

[43] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31999D0276 Consultada el 6 de mayo de 2010

[44] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32005D0854 consultado el 6 de mayo de 2020

decisión No. 1351/2008/CE denominada plan de Internet más segura, los objetivos son los mismos que en la anterior.[45]

En enero de 2013 fue inaugurado formalmente el EC3 con el fin dar impulso a la capacidad de la UE para luchar contra la ciberdelincuencia y defender la existencia de Internet libre, abierto y seguro[46], dedicándose a la investigación y desarrollo de las capacidades de las autoridades responsables de la aplicación de la ley.

Confronta las modalidades del *cibercrime*, entre las cuales se puede enunciar la creación de *back doors*, lavado de activos con instrumentos tradicionales y con monedas virtuales, fraudes en línea, la utilización de *malware* para infectar los aparatos informáticos con el fin de extraer información, robar *password* y deshabilitar antivirus, explotación sexual de niños *on line*, oferta de documentos de identificación falsa, tarjetas clonadas, venta de drogas y servicios profesional de *hackeo*, entre otros.[47]

La creación de la EC3 respondió a los lineamientos de la política europea vertida en el programa de Estocolmo, suscrito en el año 2010 y que marcó un hito en el desarrollo y evolución de la Unión en la mejora de la seguridad jurídica. «El programa de Estocolmo -Una Europa Abierta y Segura» que sirva y proteja al ciudadano contiene una serie de directrices dirigidas a los países de la unión para uniformar las políticas publicas en pro de la promoción de los derechos de los ciudadanos, facilitar y aumentar la calidad de vida, así como la seguridad jurídica de sus connacionales y el diseño e instrumentalización de una estrategia común en la lucha contra las formas graves de delincuencia y delincuencia organizada

En la materia que nos compete, el programa de Estocolmo instó a ratificar el Convenio Sobre la Ciberdelincuencia (en adelante CSC) y estimó que la Europol podría desempeñar un papel fundamental para centralizar la identificación de delitos económicos y prestar asistencia a las plataformas nacionales de los Estados partes. La lucha contra el flagelo de la ciberdelincuencia requiere de la articulación de instrumentos y mecanismos para garantizar una cooperación judicial penal, con el fin

[45] https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32008D1351 consultada el 6 de mayo de 2010
[46] https://ec.europa.eu/commission/presscorner/detail/es/IP_13_13 consultada el 6 de mayo de 2020
[47] https://www.EUROPOL.europa.eu/crime-areas-and-trends/crime-areas/cibercrime consultado el 6 de mayo de 2020

de fortalecer el Espacio de Libertad, Seguridad y Justicia de la Unión Europea (ANGUITA 2018, p. 7).

Para concluir el presente Capítulo, se debe acotar que en la actualidad se encuentra en vigor Europol 2016-2020 en la cual se reconoce expresamente que existe una escalada de la delincuencia, incluyendo la ciberdelincuencia. Para controlar los riesgos generados, las instituciones europeas, los Estados miembros y la Europol, deben trabajar de forma coordinada, ya que los desarrollos tecnológicos han aumentado el volumen de datos disponibles, mientras que Internet, redes sociales y tecnologías móviles han cambiado la interconectividad del mundo, por lo cual se requiere de mayores esfuerzos para establecer soluciones y abordar estos problemas mundiales.[48]

[48] https://www.EUROPOL.europa.eu/publications-documents/EUROPOL-strategy-2016-2020, consultado el 6 de mayo de 2020.

IV. Intervención de las nuevas tecnologías en el derecho penal económico

4.1. Principales reformas del Código Penal vinculadas con la criminalidad cibereconómica

Como punto de partida, resulta pertinente preguntarse ¿con el Código Penal de 1995 y sus posteriores reformas se ha satisfecho la necesidad de protección jurídico penal ante la comisión de graves hechos punibles cometidos por la criminalidad cibereconómica?. De seguidas, con el desarrollo del presente capítulo se tratará de generar una respuesta a esta interrogante.

En los países europeos son pocos los sistemas de protección penal que han optado por incluir las disposiciones de naturaleza informática en una ley penal especial, tal como el caso de Portugal que los incluyó en la Ley de criminalidad informática aprobada en junio de 1991. En Francia, al contrario, se creó un capítulo especial (CAPÍTULO III) del TITULO II (OTROS ATENTADOS CONTRA LOS BIENES) del LIBRO III (CRÍMENES Y DELITOS CONTRA LOS BIENES) en los cuales se aglutinaron las conductas vinculadas a los abusos informáticos, siendo las principales novedades del Código Penal Francés de 1992 el incremento de las penas, inclusión de nuevos ilícitos y la responsabilidad de personas jurídicas por estas conductas. (MORÓN 2007, p. 93).

Se comparte el criterio expuesto por MESEGUER (2013, p. 13) en el sentido que el Código Penal español no contemplaba ni definía en sus inicios como delitos las conductas que atacaban los sistema de información -intrusismo, sabotaje, daños- debiendo acudir a otras normativas y definiciones, al punto que en palabras de DE LA MATA (2007, p. 44) lo que existía era un derecho penal que, con necesarias matizaciones, hacía referencia a conductas típicas, medios comisivos, objeto de ataque, etc., con el uso de las TIC.

En apoyo a dicho punto de vista, la tendencia legislativa de los últimos años había quedado inerte ante las sugerencias de tipificación autónoma dispuestas en el Convenio sobre la Ciberdelincuecia (2001), destacando la reforma del artículo 264 en la Ley 5/2010 de 22 de junio en el cual se incorporó como delito el daño a los sistemas

de información y en el artículo 197, bis Ley Orgánica 1/2015, de 30 de marzo el acceso indebido a datos o programas infomáticos y la interceptación de datos no públicos.

En el criterio adoptado por el CP de 1995 y las reformas de 2010, 2015 y 2019 se incorporan medidas precisas para agotar las posibilidades de protección que ofrece el derecho penal, sobre la base de la protección de los bienes jurídicos tradicionales (GONZÁLEZ 2007, p. 29) en concordancia con la opinión mayoritaria de los doctrinarios de la época.

Resulta propicio resaltar que la creación de tipos agravados o circunstancias cualificadoras que tomen en cuenta el desvalor de acción o de resultado de figuras de delito ya existentes, ayudan a la interpretación y aplicación de los delitos y su vinculación con el bien jurídico protegido en las mismas tal como señala GONZÁLEZ (2007, p. 36).

Con respecto a la utilización de los avances tecnológicos para cometer delitos con contenido económico, consideramos plausible la técnica de incorporar circunstancias cualificadoras del tipo penal para aumentar en grados la pena o para establecer penas mayores en los tipos penales clásicos (fraude, hurto, blanqueo de capitales, entre otros) con fundamento a las características que hemos analizado en el apartado anterior.

Ha sido escasa, como veremos más adelante, la incorporación en los tipos penales la agravante del uso de las NT para la comisión del delito, a tal punto que, en el documento de la Estrategia Nacional de Ciberseguridad de 2019, que será objeto de análisis en el capítulo V del presente trabajo, se prevé como línea de acción el refuerzo del marco jurídico para responder eficazmente a la cibercriminalidad, tanto en el derecho sustantivo, estableciendo nuevos tipos penales o adecuando los existentes a los nuevos riesgos, como en el plano adjetivo, regulando las medidas de investigación.

El legislador español en el área del derecho penal económico le prestó especial atención desde la promulgación del CP en 1995, a la utilización de tecnologías de la información para cometer delitos que atenten contra el patrimonio de los particulares, tal es el caso de la estafa cometida mediante alguna manipulación informática (Art. 248, 2 CP), el descubrimiento o revelación de secretos de empresas con base al apoderamiento de datos o documentos tecnológicos (Art. 278, 1 CP).

Señalan VALLEJO Y PERRINO (2015, p. 100) que el legislador de 1995, como consecuencia de la demanda hecha por la doctrina para resolver los casos vinculados a la utilización de tarjetas electrónicas, sin la autorización de su propietario, se introdujo la figura de la estafa de computación (*Computerbetrug*), considerando punible la obtención de un activo patrimonial mediante la manipulación informática o el uso de un artificio semejante, en perjuicio de un tercero. Dicha manipulación puede ser *input*, es decir, en el momento de la incorporación o suministro de datos en los sistemas de computación, *v.gr*. cuando se digita la clave para extraer dinero de un cajero. Al igual la manipulación en desarrollo, referidas a la intervención incorrecta en el procesamiento y tratamiento de datos.

Posteriormente, en la reforma promulgada en Ley Orgánica 5/2003[49], de 25 de noviembre fue modificado el artículo 286 CP que consagra como delito el facilitamiento de acceso inteligible a un servicio interactivo prestado a distancia vía electrónica, mediante la importación, fabricación, distribución, venta, alquiler o posesión de equipo o programa informático o la instalación, mantenimiento o sustitución de los equipos o programas informáticos con los cuales se logre el acceso a dicho servicio.

En otro orden de ideas, la falsificación, copia, alteración o reproducción de tarjetas de crédito o debito o cheques de viaje, fue incorporado como delito en la reforma producto de la Ley Orgánica 5/2010 [50], de 22 de junio en el artículo 399, bis, 1 del CP al igual que el uso de dichas tarjetas a sabiendas de su falsedad y en perjuicio de terceras personas. Este tipo penal ha generado problemas de situación concursal entre el uso de tarjetas de debito o crédito falsificadas y el delito de estafa informática (art. 248.2 apartado c, CP) resueltos por el Tribunal Supremo con base al principio de alternatividad, es decir, que se aplicaría el delito que disponga la pena más alta que en este caso sería la del art. 399, bis 1 del CP (STS 330/2014 [51], de 23 de abril y STS 711/2012 [52]de 26 de septiembre).

[49] https://www.boe.es/buscar/doc.php?id=BOE-A-2003-13022 consultado el 26 de mayo de 2020
[50] https://www.boe.es/buscar/doc.php?id=BOE-A-2010-9953 consultado el 26 de mayo 2020
[51] http://www.poderjudicial.es/search/AN/openDocument/02a2336685e61ccd/20140505 consultado el 26 de mayo de 2020
[52]http://www.poderjudicial.es/search/AN/openDocument/571349c74b50a172/20121016 consultado el 26 de mayo de 2020

Analizando la evolución legislativa referida al delito de estafa, en contraste con la amplificación del uso de las criptoactivos, principalmente el *bitcoin*, se observa que no existe disposición alguna que regule la utilización de esta NT como instrumento para engañar a los propietarios con el fin de obtener un beneficio económico. Para tipificar estas conductas ilícitas se apela al uso del tipo genérico de estafa, contenido en el artículo 248 CP, siendo oportuno citar la sentencia de la Sala Segunda del Tribunal Supremo, número 326/2019, de 20 de junio en la cual fue condenado el autor a cumplir dos años de prisión e inhabilitación especial para ejercer el derecho del sufragio pasivo, a indemnizar a la víctima y pagar los gastos de abogado. Los hechos dados por probados se refieren a un contrato de *trading* de alta frecuencia entre la víctima y la sociedad Cloudtd Trading & Devs LTD, por el cual la víctima le entregó al acusado 35 *bitcoin,* aproximadamente. Quedó demostrado en el juicio que el acusado tenía la intención de apropiarse de dichos *bitcoins* para obtener un beneficio económico. Como se puede apreciar, en el CP no existe una cualificante por la utilización como medio de engaño de los criptoactivos. Se colige, que esta circunstancia no representa una lesión grave al bien jurídico tutelado y por eso no ha sido incorporada en las reformas. Sobre la naturaleza y posibilidad de afectación a otros bienes jurídicos por parte de los criptoactivos será analizado más adelante.

Con fundamento en el criterio de SÁNCHEZ (2016, p. 329), se puede afirmar que algunas de las reformas introducidas en la Ley Orgánica 1/2015, de 30 de marzo, así como la producción de otros cuerpos normativos, se basan en las amenazas y ámbitos de atención preferente, dispuestas en la Estrategia de Seguridad Nacional del año 2013, en la cual se identificó como riesgo y amenaza, el cibercrimen. Los compromisos internacionales del Estado español derivados de su condición de miembro de la Unión Europea, en la adopción de medidas homogéneas para generar un espacio más seguro, fue el principal motivo tomado en consideración al dar relevancia al cibercrimen, y por ende a las reformas del Código Penal en los años 2010 y 2015, en materia de protección de bienes jurídicos, contra los atentados producidos por la ciberdelincuencia.

En lo referente a los delitos de espionaje y sabotaje informático, la reforma del CP de 2015, destaca en la exposición de motivos que se deben «superar las

limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea», llevando a cabo una transposición de la Directiva Europea 2013/40/E del Parlamento Europeo y del Consejo de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal.

En el artículo 197, bis apartado 2 CP se incorporó como conducta delictiva, llevar a cabo sin autorización y mediante la utilización de artificios u instrumentos técnicos, la interceptación de transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos. En el mismo artículo 197, ter fue incorporada la protección jurídico penal a la producción, así como la importación o facilitación a terceros, de programas informáticos diseñados o adaptados para cometer delitos informáticos, y también proporcionar contraseñas de ordenador o códigos de acceso que permitan acceder a todo o parte de un sistema de información.

Las reformas de los años 2015 y 2019, también tienen normas que penalizan la indebida utilización de las nuevas tecnologías en la comisión de hechos punibles. Tal es el caso de la Ley Orgánica 1/2015, de 30 de marzo[53] en cuyo artículo 270. 2 sanciona a las empresas prestadoras de servicios de la sociedad de la información, que facilite la ubicación o acceso en internet de obras protegidas por la propiedad intelectual, sin la autorización de sus dueños y con el fin de obtener un beneficio económico directo o indirecto.

Mediante la Ley Orgánica 1/2019, de 20 de febrero[54] se introduce en el compendio de delitos que protegen el mercado y los consumidores un nuevo supuesto en el artículo 284, 2 del CP con miras a preservar la estabilidad de los precios de un instrumento financiero o un contrato de contado sobre precios de materias primas o la forma en que se calculan los precios de referencia de un producto en el mercado con la utilización de un medio de comunicación o por medio de Internet o mediante el uso de las tecnologías de la información y será punible cuando obtuviere para sí o para un tercero un beneficio económico, siempre que se den las siguientes

[53] https://www.boe.es/buscar/doc.php?id=BOE-A-2015-3439 consultado el 30 de mayo de 2020
[54] https://www.boe.es/buscar/act.php?id=BOE-A-2019-2363#au consultado el 30 de mayo de 2020

condiciones: que el beneficio obtenido o perjuicio causado fuera superior a doscientos cincuenta mil euros; que el importe de los fondos empleado fuera superior a dos millones de euros o que causara con la conducta un grave impacto en la integridad del mercado.

Como se ha podido observar en las últimas reformas del CP ha habido una constante actualización de los tipos penales, incorporando las nuevas tecnologías como medio de comisión o como un tipo cualificado. De seguidas, pasaremos a analizar algunos tipos penales que han quedado por fuera o conductas que no fueron debidamente contempladas y que pudieran considerarse para una futura reforma.

4.2. Delito de blanqueo de capitales y el aumento exponencial del uso de los criptoactivos

La figura del lavado de activos o blanqueo de capitales sufrió una criticada reforma en la Ley Orgánica 5/2010, de 22 de junio, en la cual el requisito relativo al conocimiento del «delito» antecedente, fue cambiado por «en una actividad delictiva». Esta variación conceptual en palabras de ABEL SOUTO (2012, p. 31) se le atribuye un afan expansivo del legislador, incorporándose en el CP los mismos términos utilizados en las Directivas 2001/97 y 2005/60 del Consejo y Parlamento Europeo.

Otra controversial adición fue la expresa tipificación del autoblanqueo que había sido objeto de una extensa discusión por parte de la doctrina y la jurisprudencia, en cuanto a si violaba o no el principio *nen bis in idem*, y en caso de su admisión respecto a cuáles delitos podría conjugarse o no dicha modalidad. Esta inclusión pone fin a dicha discusión al agregar en el artículo 301 CP el inciso «cometida por él o por cualquier otra persona».

Existe un tema relacionado con el blanqueo de dinero que ha sido objeto de análisis por parte de la doctrina. Nos referimos a la utilización como instrumento para la estratificación del dinero producto de la comisión de hechos punibles a los criptoactivos, se pretende con su uso ocultar el origen de los activos y borrar toda huella contable del mismo. Desde el inicio la posibilidad de la adecuación típica de esta conducta es admitida en el tipo penal, con la cláusula atemporal del art. 301 CP

que dice literalmente «o de cualquier otro modo», (GOMEZ INIESTA, 2015, p.2) lo cual hace concluir que la utilización de esta NT se puede integrar como un mecanismo para blanquear capitales.

Desde el año 2008 cuando fue presentado el protocolo del Bitcoin por Satoshi Nakamoto, con el fin de crear una moneda virtual de intercambio, descentralizada, transfronteriza y pseudoanonima, se ha desarrollado un mercado deseoso de invertir en estos *commodities*. A la par han salido a la luz pública otros criptoactivos basados en la misma tecnología *blockchain* usada por Nakamoto, a tal punto que, de acuerdo al registro del *ranking coinmarketcap*, existen 5599 criptoactivos[55].

Los criptoactivos *per se* no representan un peligro para la sociedad, ni afecta directamente a un bien jurídico tutelado. No obstante, en criterio de BEDECARRATZ (2018, p. 95) pueden ser usados como instrumentos para cometer ciertos delitos, entre los cuales se citan, blanqueo de capitales, estafas, financiamiento al terrorismo, siendo que la simple posesión, conductas de creación, uso y transferencia no lesionan ni amenazan a bien jurídico alguno. El desvalor de la acción viene dado por su utilización como instrumento, herramienta o medio para lograr el agotamiento e impunidad de dichos delitos.

Hay que tener claridad que el empleo de nuevas modalidades de transacción financiera y económica, como las criptomonedas, para el tráfico y el comercio de bienes y prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío a la seguridad por su sofisticación y complejidad, tal como fue reconocido en el documento de la Estrategia Nacional de Ciberseguridad 2019, estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una fuente de ingresos para el crimen organizado y por tanto, son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen.

[55] Dato obtenido el día 18 de junio de 2020, 16:00. https://coinmarketcap.com/all/views/all/ es de resaltar que en esa fecha el *bitcoin* tenía un precio de $9.380,7 y en las 24 horas anteriores se transaron $17,659,907,765. Después del BTC las criptoactivos de mayor valor son el *bitcoin cash* y *etherum* con un valor de $235.33 y $229.93, respectivamente.

La *red flag* -bandera roja- había sido otorgada por el Grupo de Acción Financiera Internacional (en lo sucesivo GAFI) en la directriz para un enfoque basado en riesgo de las monedas vrituales (GAFI, 2015, p. 34-35). Para esta respetada organización las monedas virtuales son potencialmente vulnerables al abuso en el lavado de activos y la financiación al terrorismo, al permitir un mayor anonimato en comparación con los métodos de pago tradicionales, así como el alcance global que estas presentan, por cuanto son accedidos para su comercialización mediante Internet, y pueden ser utilizados para pagos transfronterizos o transferencias de fondos.

Siguiendo las sugerencias del GAFI la Unión Europea incorporó mediante la Directiva 2018/843, del Parlamento Europeo y del Consejo de 30 de mayo de 2018, a los proveedores de servicios de custodia de monederos electrónicos y de cambio de monedas virtuales por monedas fiduciarias, al ámbito de aplicación de la Directiva 2015/849, de fecha 20 de mayo de 2015, con el fin de luchar contra el blanqueo de capitales y financiamiento al terrorismo. De esta forma las medidas de vigilancia y control dispuestas en la IV Directiva son aplicables a las transacciones basadas en criptoactivos, debiendo los Estados partes adaptar sus legislaciones en este aspecto. Se pone bajo análisis la obligación que deben tener los usuarios hagan una autodeclaración voluntaria ante la autoridad designada en cada Estado, respecto a su identidad, domicilio y titularidad de criptoactivos.

En el fundamento 10 de la Directiva se reconoce el riesgo que rodea a las monedas virtuales de ser utilizadas para blanquear capitales y financiar el terrorismo, con el apoyo del anonimato que rodea su titularidad, motivo por el cual se hace necesario la regulación de las empresas que prestan servicios de *exchange* que permite la convertibilidad de criptoactivos a dinero *fiat* -de uso diario y reconocido por los Estados, *v.gr*. euro, dólar, libras esterlinas- y las que prestan servicios de *wallet* o cartera donde se custodian las criptomonedas.

Esta directiva ha tenido efectos inmediatos en el poder judicial, especialmente en la negativa a reconocer a los criptoactivos como dinero electrónico. En la citada decisión (STS 326/2019) se negó la petición de la parte querellada que pretendía la restitución de los *bitcoins*, a tenor de lo dispuesto en el artículo 110 CP. La Sala argumentó que el engaño efectuado por los acusados se materializó sobre los

euros entregados para la adquisición de los *bitcoins*, aunado a que es un activo patrimonial inmaterial en forma de unidad de cuenta, que puede ser utilizado en cualquier transaccion bilateral en que las partes contratantes lo acepten. En conclusion el *bitcoin* no es una moneda ni puede contener tal consideración legal.

La propia Directiva establece un lapso para que los Estados miembros adopten las disposiciones legales, reglamentarias y administrativas en sus ordenamientos jurídicos, venciendo el 10 de enero de 2020. Con base a ello, el Ministerio de Asuntos Económicos un poco retrasado presentó el Anteproyecto de Ley para cumplir con ello y modificar le Ley 10/2010, de prevención del blanqueo de capitales.

V. Prevención y persecución de la criminalidad cibereconómica

5.1. Medios tecnológicos de investigación en la Ley de Enjuiciamiento Criminal

En esta parte de la investigación se prestará atención a los cambios legislativos en el campo del derecho penal adjetivo relacionados con el uso de las nuevas tecnologías. Con el fin de dotar a los órganos investigadores y de prevención de herramientas para combatir los ciberdelitos, se promulgó la Ley Orgánica 13/2015, de 5 de octubre en la cual se realizó una profunda reforma de la Ley de Enjuiciamiento Criminal, adoptando nuevas medidas de investigación tecnológicas, procedimientos para el registro, almacenamiento y conservación de datos[56]. Las novísimas normas para la interceptación de comunicaciones telefónicas y telemáticas, previa autorización judicial, pueden durar tres meses, prorrogables hasta alcanzar dieciocho meses, siendo aplicables a los delitos con una pena superior a los tres años, los que sean cometidos por organizaciones de delincuencia organizada y en caso de delitos de terrorismo (Art. 588, ter CP).

El uso de estos medios tecnológicos en el proceso de investigación criminal no es novedoso, inclusive ya había sido reconocida su legalidad por el Tribunal Supremo. Siguiendo a ORTIZ (2013, p. 26) podemos afirmar que se ha aceptado la legalidad del Sistema Integrado de Interceptación Telefónica (SITEL), por cuanto cumple con todas las exigencias y garantías propias de esta clase de diligencias de investigación y probatorias, entre ellas la previa autorización judicial para su práctica.

La Ley Orgánica parte de la utilización de las mismas tecnologías con las que contamos en la actualidad, para luchar en contra de la delincuencia que las usa, que casi siempre es organizada (GOMEZ, 2019, p. 242); acomete la regulación en forma explícita de los procesos de obtención de evidencias de interés criminalístico referidos a las tecnologías de la información, mediante la colaboración y aporte de la información almacenada en sus bases de datos por las empresas prestadoras de

[56] https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10725 Fue consultado el 4 de mayo de 2020.

servicios de telecomunicaciones, de acceso a la red o servicios de la sociedad de la información, así como cualquier otra persona jurídica que contribuya a la comunicación telemática, lógica o virtual.

Con mucho acierto señalan RAYÓN y GÓMEZ (2014, p. 218) que los proveedores de servicios tienen en sus sistemas de información evidencias de interés criminalístico de suma relevancia para el desarrollo de la investigación, entre las cuales se puede citar: la dirección IP[57] asignada a los ordenadores, *ipad*, *laptop* u otro instrumento tecnológico conectados a Internet, los datos de identificación y ubicación junto con la hora y duración de la comunicación; los medios de pago asignados a la cancelación del servicio; copia de los ficheros que disponga el sospechoso en su *web site*, entre otros.

En la reforma fue incorporado un nuevo Capítulo IV del libro II de la LECrim, referido a las disposiciones comunes a todas las técnicas de investigación tecnológicas. Estos principios rectores y garantías constitucionales son fruto de la más avanzada jurisprudencial constitucional y ordinaria de los tribunales en los últimos años (GÓMEZ, 2019, p. 244) y tienen como finalidad establecer fehacientemente que la decisión judicial q las autorice es legítima, fundamentada y es procedente en derecho.

Para practicar los actos de investigación se debe contar con una autorización judicial emanada de un juez instructor, en el contexto de una investigación de un delito en concreto -principio de especialidad-, que no se encuentren a disposición del Ministerio Fiscal o la policía otras medidas menos gravosas que atenten contra los derechos fundamentales del investigado o encausado, sea pertinente para ubicar su paradero y logar el total esclarecimiento de los hechos -principio de necesidad.

Dichas medidas deben ser, además, idóneas para determinar los hechos investigados, la extensión, duración y forma de ejecución de la medida, designar el componente policial que la va a practicar y la identificación de los sujetos sobre los cuales va a recaer -principio de idoneidad- y por último, el sacrificio de los derechos

[57] IP, significa Internet Protocol, que hace posible la interconexión e intercambio de información a través de Internet. Las IP son distribuidas por ramales a las empresas prestadoras de servicio de internet (ISP) y los Estados donde funcionan. Cada usuario tendría una IP asignada ubicable en tiempo y espacio. Para evadir la ubicación, los ciberdelincuentes usan VPN u otros programas de enmascaramiento de IP.

e intereses particulares afectados no debe ser superior al beneficio obtenido por la colectividad con el esclarecimiento de los hechos -principio de proporcionalidad-. Cada medida tendrá el lapso de duración que en específico el legislador dispuso para ellas y podrá prorrogarse por el mismo juez instructor a solicitud del ministerio fiscal o la policía antes del vencimiento del plazo, se haga por escrito, indicando las razones que justifiquen la prórroga y se indique el resultado obtenido hasta esa fecha con la práctica de la medida.

Con base al contenido del artículo 588, bis se puede inferir que el trámite de las medidas -solicitud, decisión, actuaciones realizadas- deben constar en una pieza separada y secreta. El resultado de dichas diligencias puede afectar a terceros tomando en cuenta cada medio de investigación, así, por ejemplo, un tercero que utilice un teléfono o medio de comunicación intervenido tiene relevancia jurídico penal para la investigación, a tal punto que los resultados en esa investigación pueden ser usados en otro procedimiento distinto, tal como lo autorizó el pleno de la Sala Segunda del Tribunal Supremo, en acuerdo no jurisdiccional de 26 de mayo de 2009[58].

Las medidas acordadas podrán ser cesadas por el juez que las dictaminó cuando desaparezcan las circunstancias fácticas que la justificaron o las considere inútiles, al no obtener los resultados esperados.

De dichas diligencias se dejará copia por parte del letrado de la Administración de Justicia por un lapso de cinco (5) años después que la pena se haya ejecutado, cuando la acción penal para perseguir el delito se encuentre prescrita o cuando haya sido proferida sentencia de sobreseimiento definitivo o absolutoria, definitivamente firme.

De forma taxativa la Ley Orgánica 13/2015 estableció las técnicas de investigación mediante medios tecnológicos, entre las cuales se pueden destacar:

5.1.1. La intervención de las comunicaciones telefónicas y telemáticas.

[58] http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdo-del-26-de-mayo-de-2009-sobre-Habilitacion-de-escuchas-telefonicas-procedentes-de-diligencias-distintas-a-las-que-corresponden-al-juicio consulado el 7 de junio de 2020

Siguiendo a GÓMEZ (2019, p. 250), se entiende por interceptación la toma de conocimiento por parte de la autoridad judicial o policial de comunicaciones efectuadas por dos o más personas que se encuentran distantes, mediante el uso de la telefonía -verbal-, telemática -escrita- sea cual fuere el *software* utilizado para comunicarse, usando para ello instrumentos técnicos especializados.

Antes de la mencionada reforma no se encontraba dispuesta esta técnica de investigación, no obstante, ya era utilizada por los instructores para presentar como prueba pantallazos de conversaciones sostenidas por los investigados mediante las redes sociales -*facebook*, *twitter*, etc- o las sostenidas mediante *whatsApp* y el Tribunal Supremo se había pronunciado favorablemente[59].

El derecho al secreto de las comunicaciones -telefónicas, telegráficas, postales, entre otras- está consagrado como derecho en el artículo 18.3 CE, y la orden judicial de intervención se manifiesta como una excepción rodeada de requisitos impretermitibles.

Entre ellos tenemos, que dicha autorización emane del juzgado de instrucción mediante resolución motivada, en el contexto de una investigación penal y debe contener además de los requisitos dispuestos en el art. 588, bis b) a saber: identificación del número de abonado, del terminal o el serial IMEI del aparato; identificación de la conexión objeto de la intervención y los datos necesarios para identificar el medio de telecomunicación que se trate.

En el auto que se decrete dicha medida debe establecerse los indicios existentes en la investigación que la fundamente la cual puede autorizarse por un lapso de tres meses, prorrogables por períodos sucesivos hasta un plazo máximo de dieciocho meses[60]. La intervención debe ser necesaria por no contar con otro medio para descubrir la existencia del delito[61] solo proceden en investigaciones de delitos dolosos castigados con pena superior a tres años de prisión, delitos cometidos en el seno de un grupo u organización criminal y en caso de delitos de terrorismo[62].

[59] https://www.iberley.es/jurisprudencia/sentencia-penal-n-850-2014-ts-sala-penal-sec-1-rec-10269-2014-26-11-2014-14918871 criterio reiterado en http://www.poderjudicial.es/search/AN/openDocument/588d270cb80152a8/20150527 consultadas el 7 de junio de 2020

[60] Art. 588, ter g) LECrim

[61] Art. 588, ter a) LECrim

[62] Art. 579.1 LECrim

En el caso que sean urgentes, como bien podrían ser las investigaciones penales por hechos cometidos por bandas armadas o elementos terroristas y existan razones fundadas que hagan necesaria la intervención, el Ministro del Interior o el Secretario de Estado de Seguridad podrá ordenarla, debiendo notificar al juez competente dentro de un plazo de veinticuatro horas, indicando los fundamentos, la actuación realizada, la forma en que se ha desarrollado y el resultado, esto con el fin de que el juez lo revoque o confirme, en un plazo de setenta y dos horas desde que fue ordenada la medida.

Esta excepción a la necesidad de la autorización judicial para la práctica de esta diligencia de investigación, ha sido avalada por el Tribunal Constitucional en reiteradas decisiones, entendiendo que la valoración de la urgencia y necesidad de la intervención policial ha de realizarse *ex ante* y es susceptible de control *ex post*, al igual que el respeto del principio de proporcionalidad. La constatación *ex post* de estas dos circunstancias implicaría la vulneración de un derecho fundamental y acarrearía la nulidad de la prueba obtenida por ilícita. (STS 173/2011, de 7 de noviembre).

De acuerdo al artículo 588, ter b) los terminales o medios de comunicación a interceptar son los de uso habitual u ocasional por el investigado. Pueden ser solicitados mediante autorización judicial los datos electrónicos referidos a la identidad y operatividad (conectividad) de los abonados y usuarios de servicios de telecomunicaciones conservados por las empresas prestadoras de servicio o personas que faciliten la comunicación[63]; la localización IP e identificación del equipo o dispositivo de conectividad[64] -celulares, *ipad*, *tablets*, etc- usados para cometer delitos.

5.1.2 Captación o grabación de comunicaciones orales, con la utilización de dispositivos electrónicos.

Otra técnica de investigación dispuesta en la mencionada reforma se refiere a la captación o grabación de comunicaciones orales, con la utilización de dispositivos electrónicos. La autorización judicial puede versar sobre comunicaciones que

[63] Art. 588, ter i) LECrim
[64] Art. 588, ter k) LECrim

mantenga el investigado en vía pública o en otro espacio abierto, en su domicilio o en otro lugar cerrado.

El proceso de grabación se realiza mediante la instalación de dispositivos en el sitio donde se prevea la reunión de las personas investigadas. En caso que la grabación se vaya a efectuar en el domicilio, el juez competente deberá extender su motivación a esos lugares. De acuerdo al artículo 588, quáter b) para la procedencia de esta medida se requiere además del indicado en el artículo 579 LECrim, que se pueda prever racionalmente que con la utilización de los dispositivos se obtendrán datos esenciales y relevantes para la investigación.

Una medida menos intrusiva en el derecho a la intimidad de los ciudadanos que protege el artículo 18.1 CE es la posibilidad de utilizar dispositivos técnicos de captación de imágenes mediante cámaras callejeras de video vigilancia, seguimiento y localización (GPS) en sitios públicos, para lo cual se requiere también autorización judicial.

El fin de esta diligencia de investigación se refiere a la necesidad de identificar a la persona investigada, localizar instrumentos o efectos delitos o ubicar datos importantes para la causa. Al igual que en la medida de interceptación, esta técnica puede ser acordada por la autoridad policial, siempre que sea racionalmente evidenciable que su no utilización con la premura del caso podría frustrar la investigación, debiendo el órgano policial informar al juez competente en un plazo de veinticuatro horas, quien podrá ratificar o no en igual lapso.

5.1.3. El registro de dispositivos de almacenamiento masivo

El registro de dispositivos de almacenamiento masivo (en lo sucesivo DAM) de información, por ejemplo, *pendrive*, discos duros externos, memorias extraíbles, entre otros, fue expresamente normativizado en el capítulo VIII del Título VIII del libro II LECrim. Esta regulación tiene precedentes con base a decisiones jurisdiccionales del Tribunal Supremo que regulaban dicha técnica de investigación y le reconoció a la información vertida en dichos dispositivos como parte informador del derecho a la intimidad y el secreto de las comunicaciones.

En STS 342/2013, 17 de abril[65], se catalogaba dicha protección como «derecho al propio entorno digital» en virtud de lo cual se requería de autorización judicial para acceder a su contenido. Ordena el art. 588, sexies c) que la resolución del juez de instrucción que autorice el acceso a la información contenida en los DAM fijará los términos y el alcance del registro y podrá autorizar la realización de copias de datos informáticos. De igual forma se evitará la incautación de los soportes físicos, salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen.

Es de resaltar que la incautación de un DAM en la práctica de una visita domiciliaria, no legitima al acceso de su contenido, debiendo extender una autorización judicial particular para esa diligencia de investigación[66]. En casos de urgencia puede ser realizada por la policía judicial, siempre que se aprecie un interés constitucional legítimo que haga imprescindible la medida, debiendo el órgano policial informar al juez competente en un plazo de veinticuatro horas, quien podrá ratificar o no en un lapso de setenta y dos horas.

5.1.4. La técnica de investigación de observación, análisis y extracción de información de un ordenador e instrumento de almacenamiento masivo, dispositivo electrónico o sistema de base de datos

Una completa novedad es la consagración de la técnica de investigación de observación, análisis y extracción de información de un ordenador e instrumento de almacenamiento masivo, dispositivo electrónico o sistema de base de datos, mediante la aplicación de técnicas de fuerza bruta para acceder a los sistemas de información, e inclusive la instalación de *software* vía *pishing* u otra técnica de intrusión que permita establecer las responsabilidades penales en los delitos cometidos en el seno de organizaciones criminales, delitos de terrorismo, los cometidos contra menores e inhábiles, contra la Constitución, de traición o relativos a la defensa nacional, así como todos aquellos que utilizan como instrumentos de

[65] https://supremo.vlex.es/vid/438315958 consultada el 7 de junio de 2020

[66] Art. 588, sexties a) -2, LECrim

acción, los de carácter informáticos o de cualquier otra tecnología de la información o telecomunicaciones.

De acuerdo al artículo 588, septies a)-2 el juez competente podrá autorizarlo mediante auto, por el lapso de un mes, prorrogable por igual período hasta un máximo de tres meses[67]. En dicho auto se indicará la identificación de los dispositivos sobre los cuales va a recaer la técnica, la forma en que se procederá al acceso y el *software* que se usará, los agentes autorizados para ejecutar la medida y las medidas precisas para preservar la integridad de los datos almacenados.

Las empresas prestadoras de servicio indicadas en el artículo 588, ter e) están obligados a colaborar con la justicia en la práctica de esta diligencia. Esta técnica de investigación intrusiva prevé la posibilidad que las autoridades competentes induzcan a un particular que tenga conocimiento acerca del funcionamiento de los sistemas de información para que preste su colaboración para la buena realización de esta diligencia. Ya por último se estima procedente la ampliación a otros dispositivos en los cuales se presuma la existencia de información importante, para lo cual se pedirá autorización judicial.

5.2. Prevención, detección y respuesta ante la cibercriminalidad como política de Estado

El Convenio sobre la Ciberdelincuencia suscrito en Budapest, el 23 de noviembre de 2001 bajo el marco del Consejo de Europa[68], es considerado el cuerpo normativo preponderante en pro de la lucha coordinada de los Estados en contra de la ciberdelincuencia y tuvo como fundamento la necesidad de aplicar, con carácter prioritario, una política común encaminada a proteger la sociedad contra la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional[69].

Los representantes estadales estaban para esa fecha preocupados por los riesgos del uso dado a las redes informáticas para cometer delitos, como

[67] Art. 588, septies c) LECrim
[68] Para completar el Convenio sobre la Ciberdelincuencia se promulgó el Protocolo Adicional al convenio criminalizando los actos de racismo y xenofobia relacionado con las nuevas tecnologías.
[69] Preámbulo del Convenio sobre la Ciberdelincuencia.

efectivamente ha ocurrido a posterioridad. Especial atención fue prestada al ámbito operativo, en cuanto a la obtención de evidencias en la etapa investigativa, las cuales quedaban almacenadas en los sistemas informáticos de las empresas prestadoras de servicios de TIC, al punto que estos sufrían modificaciones en sus datos, haciéndose necesario controlar su incolumidad, en pro de lograr un equilibrio entre los intereses del ejercicio de la acción penal y los derechos de los particulares.

Cabe mencionar que, en el Convenio de Budapest, se especificaron las conductas que los Estados partes debían adoptar como delitos, entre las que resaltan, a los fines de este trabajo de investigación, el acceso ilícito a la totalidad o una parte de un sistema informático con el fin de obtener datos; la interceptación ilícita de datos informáticos en transmisiones privadas y el fraude informático que causa un daño o perjuicio patrimonial a otra persona mediante un sistema informático.

Como hemos podido observar, la ratificación por España del Convenio de Budapest contra la cibercriminalidad del 20 de mayo de 2010, y el auge e incremento de las manifestaciones criminales cometidas contra sistemas informáticos o el uso de estos sistemas para atentar contra bienes jurídicos; sirvieron de fundamento de la reforma 5/2010 de 22 de junio y la creación de la fiscalía especializada en criminalidad informática.

Con el fin de contar con un recurso humano capacitado para dirigir las investigaciones penales en esta materia, el Estado Español mediante Real Decreto No. 1735/2010 de 23, de diciembre creó la plaza de Fiscal Coordinador en materia de Criminalidad Informática. La creación de esta dependencia se amoldó al criterio de especialización que el Ministerio Fiscal había estado desarrollando con la creación de otras dependencias especializadas, para garantizar la eficiencia, dirección y coordinación de las funciones fiscales en materia de delincuencia organizada [70].

[70] Para llevar a cabo las investigaciones penales de hechos con sustrato económico de especial trascendencia o cometidos por funcionarios públicos en el ejercicio de su cargo, fue creada en 1995 la Fiscalía Contra la Corrupción y la Criminalidad Organizada la cual tiene competencia a nivel nacional adscrita a la Fiscalía General de la Nación y de acuerdo al artículo 19.4 del Estatuto Orgánico del Ministerio Fiscal, en las siguientes áreas: a) Delitos de abuso o uso indebido de información privilegiada; b) Delitos contra la hacienda pública, contra la seguridad social y de contrabando; c) Delitos de fraudes y exacciones legales; d) Defraudaciones; e) Delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores; f) Blanqueo de capitales y conductas afines a la receptación, salvo cuando por su relación con delitos de tráfico de drogas o de terrorismo corresponda conocer a otra fiscalías especiales, entre otros.

El conocimiento de las investigaciones de esta nueva dependencia fiscal, fue delimitada por la Instrucción 2/2011 emanada de la Fiscalía General del Estado para aquellos supuestos en los cuales la utilización de dichas tecnologías resultare ser determinante en el desarrollo de la actividad delictiva y/o dicha circunstancia implicare una elevada complejidad en la dinámica comisiva y, en consecuencia, una mayor dificultad en la investigación del hecho e identificación de sus responsables. [71]

Es de hacer constar que en el proceso de investigación de los delitos cibereconómicos pudiese existir un conflicto de competencia entre la Fiscalía contra la Corrupción y la Criminalidad Organizada y el fiscal de la sala de Criminalidad Informática, correspondiéndole al Fiscal General del Estado establecer la participación de esta o aquella en el proceso penal correspondiente.

En el año 2013, fue publicado el documento «Estrategia de seguridad nacional. Un proyecto compartido» en el cual se reafirmó la seguridad como un fundamento esencial para el desarrollo y el progreso de una sociedad libre, ante los riesgos y amenazas que el ciberespacio congrega[72]. La ciberseguridad es considerada (a diferencia de las políticas desarrolladas con anterioridad), uno de los principales ámbitos de actuación[73].

El objetivo principal del plan de estrategia nacional fue garantizar el uso seguro de las redes y los sistemas de información, con base al fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques y, dejó entrever

[71] Doctrina de la Fiscalía General del Estado, Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías. Referencia: FIS-I-2011-00002

[72] En el año 2013 ocurrió otro evento trascendental en la construcción de la política criminal española, como fue la creación del Consejo Nacional de Ciberseguridad (CNS) órgano colegiado que actúa en apoyo al Consejo de Seguridad Nacional y se constituyó por acuerdo el 5 de diciembre de 2013. Está compuesto por el espectro de ámbitos de los departamentos, organismos y agencias públicas con competencias en materia de ciberseguridad, para coordinar las acciones conjuntas con el propósito de elevar los niveles de seguridad. Dentro de sus funciones y en línea con el desenvolvimiento de este trabajo, resalta que el CNS tiene dentro de sus funciones realizar la valoración de riesgos y amenazas, analizar los posibles escenarios de crisis, evolución y elaborar y mantener actualizados los planes de respuesta. Desde el punto de vista del análisis de resultados, tiene como función diseñar directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y evaluar los resultados.[72] Dentro del catálogo de las instituciones que conforman la DNS se pueden citar la Agencia Española de Protección de Datos, el Centro Nacional de Protección de Infraestructura Críticas, el Instituto Nacional de la Ciberseguridad (INC) y el Centro Criptológico Nacional (CCN).

[73] Estrategia de Seguridad Nacional. Un proyecto compartido. Presidencia de Gobierno, Madrid 2013.

que los planes de seguridad concebidos con anterioridad habían quedado parcialmente ejecutados[74].

Unas estrategias mejores elaboradas, son las propugnadas en el Real Decreto 1008/2017[75], de 1 de diciembre que aprobó la Estrategia de Seguridad Nacional 2017, en la cual se catalogó la vulnerabilidad del ciberespacio como una amenaza y desafío que se desarrolla en los espacios comunes globales en los cuales no existen fronteras físicas, la soberanía y jurisdicción por parte de los Estados es débil al igual que la regulación y persecución de los ilícitos cometidos[76].

Como corolario de todos los esfuerzos que a nivel de estrategias preventivas y represivas ha operativizado el gobierno de España para la lucha contra el cibercrimen, en el año 2019 el Consejo de Seguridad Nacional dictó la orden PCI/487/2019, de 26 de abril mediante la cual aprobó la Estrategia Nacional de Ciberseguridad 2019[77], documento dirigido específicamente a la determinación de las amenazas y desafíos que existen en el ciberespacio.

En el mismo orden de ideas, se fijó el convencimiento que el ciberespacio al ser un ámbito común global, donde las sociedades y los Estados interactúan con fácil acceso y dinamismo, de forma soberana y sin límites territoriales ofrece

---

[74] http://www.realinstitutoelcano.org/wps/wcm/connect/c06cac0047612e998806cb6dc6329423/EstrategiaEspanolaDeSeguridad.pdf?MOD=AJPERES&CACHEID=c06cac0047612e998806cb6dc6329423 fue consultado el 7 de mayo de 2020.

[75] Basados en un enfoque comparativo, podemos afirmar que la estrategia nacional de 2017, tiene una marcada diferencia con las estrategias diseñadas en los años 2011 y 2013 con fundamento en la preponderancia que se le daba a la participación ciudadana en las dos primeras y la radical postura de concebir el problema de la cybercriminalidad como una amenaza que traspasa las fronteras, que amerita para su control y prevención la participación de otros estados y organizaciones internacionales, que en forma programática y colaborativa aportan sus recursos y conocimientos para poder controlarla. La adecuación a nuevas tecnologías y su utilización en la comisión de delitos, está ínsita en el contenido del documento al determinar que se debe operar desde la resiliencia, adaptándose a los cambios y luchas por establecer estructuras y sistemas que puedan aminorar los riesgos de comisión de hechos punibles. En conclusión, se le da un espacio propio y diferencial a la ciberseguridad desde la óptica de la política criminal por parte del Estado Español. En el capítulo 5, referido a los objetivos generales y líneas de acción de la seguridad nacional, tiene escalada (*scale up*) relevancia en la materia que nos compete el fortalecimiento de las medidas de prevención, detección y respuesta a los ciberataques, con el propósito de garantizar un espacio seguro para los ciudadanos, al momento de usar las redes y los sistemas de información. Por vez primera se consideró como estrategia la adaptación tecnológica de las industrias españolas de ciberseguridad, promoviendo la investigación, desarrollo e innovación para conducirla a la par de las nuevas tecnologías. Esta área de desarrollo se homogeneiza con la promoción del alcance y mantenimiento de conocimientos, habilidades y experiencia para sustentar los objetivos de seguridad en España.

[76] Estrategia de Seguridad Nacional 2017. BOE No. 309, de 21 de diciembre de 2017. Fue consultado el 3 de mayo de 2020. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-15181

[77] https://www.boe.es/buscar/act.php?id=BOE-A-2019-6347 fue consultado el 7 de mayo de 2020

innumerables oportunidades de desarrollo económico, flujo de información, conectividad universal, con unos serios de desafíos en materia de seguridad.

Se reconoce en dicha estrategia la necesidad del uso y desarrollo del ciberespacio, sin abandonar la consecuente amenaza que representa el uso desviado de los recursos y plataforma tecnológica. Las nuevas tecnologías han sido tomadas en consideración reconociéndoles que aun el potencial transformador de la inteligencia artificial, la robótica, el *big data*, el *blockchain* e Internet de las cosas está por ser descubierto.

En consonancia con el área que nos compete que es el derecho penal económico, la Estrategia Nacional de Ciberseguridad (2019), estableció como línea de acción el refuerzo del marco jurídico para responder eficazmente a la cibercriminalidad, tanto en el derecho sustantivo, definiendo los tipos penales, como en el adjetivo, regulando las medidas de investigación.

Pretende también dicho documento, reforzar las acciones con miras a potenciar las capacidades de investigación, atribución y persecución penal de la cibercriminalidad. Asimismo, estableció medidas para desarrollar una cultura de ciberseguridad, donde las empresas y los ciudadanos deben ser concienciados de la obligación y corresponsabilidad en contribuir a la ciberseguridad nacional.

A manera de conclusión de lo expuesto en este subcapítulo, se puede afirmar que la política criminal en materia de lucha contra la ciberdelincuencia por parte de España ha sido diseñada en un marco de prevención, sobre la base de la creación de conciencia en el uso de los instrumentos informáticos por parte de los particulares y la colaboración de las empresas prestadoras de servicios de TI. En igual sentido, se han incorporados en el CP las Directrices generadas por la UE.

No obstante, se observa que del análisis de la reciente estrategia de ciberseguridad publicada en el año 2019 se presume que se va adelantar la creación o adaptación de tipos penales para sancionar las modalidades de conducta cometidas por la cibercriminalidad, con el apoyo de normas de procedimientos que establezcan los técnicas o procedimientos de investigación.

VI. Conclusiones

1. En un principio la Tecnología de la Información marcó un hito en el desarrollo de las relaciones sociales, abriendo canales de comunicación escrita y verbal hasta llegar a la transmisión de videos en tiempo real. La ampliación de la banda de Internet fomentó la economía globalizada entre países del mismo y de distintos continentes, creando un dinámico comercio que se basa y se sostiene en las comunicaciones sobre el protocolo de Internet. Todo ello hace que emerjan nuevos riesgos, que cuando se concretizan, lesionan o ponen en peligro bienes jurídicos relevantes para la sociedad y de interés para el derecho penal.

2. Ante la aparición de nuevas conductas no abarcadas por los tipos penales tradicionales, se han dispuesto elementos cualificadores -como por ejemplo la facilitación, fabricación, introducción o posesión de "programas de ordenador" para cometer una estafa incorporado en el artículo 248 CP, de la Ley Orgánica de reforma del CP 2003-, para prevenir la comisión de hechos punibles, sobre la base de la participación organizada de los Estados, quienes ante la evidente caracterización universal de las conductas ilícitas, impulsan la creación de una tipología uniforme, procedimientos y métodos de colaboración para lograr la aplicación de sistemas de asistencia en la investigación, observándose que a pesar de los esfuerzos tales acciones resultan insuficientes ante la evolución de nuevos *itters* criminales.

3. El desarrollo constante de los sistemas de información, ha incidido en la aparición de nuevas tecnologías como el *blockchain* -en el cual se basan los criptoactivos-, Internet de las cosas y el *computing cloud*, que generan condiciones utilizadas por los delincuentes para crear diferentes modalidades de delinquir. La posibilidad de salir impunes con el uso de estas nuevas tecnologías, debe ser contrarrestado con la adecuación tipológica de estas conductas, satisfaciendo el principio de legalidad penal y adecuando los métodos de investigación para adaptarse a ellos, usando inclusive, las mismas tecnologías para perseguirlos.

4. En sus inicios la cibercriminalidad dirigió sus ataques contra los sistemas de información, sin embargo, posteriormente con el ánimo de obtener mayores

beneficios económicos, estos delincuentes comienzan a utilizar las TIC, lesionando o poniendo en peligro bienes jurídicos de carácter patrimonial. En la actualidad la cibercriminalidad se ha amplificado exponencialmente, pudiéndose identificar áreas dedicadas al financiamiento, organización de grupos y ejecución de conductas terroristas (ciberterrorismo), el *hacktivismo*, los dedicados a pornografía infantil y la denominada criminalidad cibereconómica -analizada en el presente trabajo- que tiene como fin principal la obtención de un beneficio económico, mediante la utilización de las TIC y las NT.

5. Los ciberdelincuentes con marcado interés económico, pueden actuar en solitario para obtener beneficios y han evolucionado conformando grupos activos dedicados a cometer grandes fraudes o a establecer servicios ilícitos para ayudar a su vez a terceras personas a lucrarse. En los últimos años se ha evidenciado la incorporación de ciberdelincuentes en grupos de delincuencia organizada, que actúan en forma estructurada en diversos países, con cadena de mando y actividades asignadas a sus miembros con el propósito de obtener poder y dinero.

6. Esta evolución de la delincuencia cibereconómica debe ser atacada en forma coordinada entre los diversos países con sus operadores administrativos, policiales y órganos de justicia penal, ejerciendo una constante supervisión y control de los factores económicos. Se debe aprovechar el camino ya adelantado por los Estados en la cooperación internacional, con tratados bilaterales, multilaterales y demás instrumentos internacionales en la lucha contra la delincuencia organizada transnacional y así, intentar neutralizar el efecto negativo del ataque de estos grupos hacia los sistemas económicos y contra el patrimonio de sus ciudadanos.

7. El Estado español ha dispuesto desde el año 2010, la adecuación de la legislación interna para perseguir y luchar contra la cibercriminalidad, incluyendo la económica, ante el compromiso asumido como miembro de la Unión Europea y el Programa de Estocolmo.

8. La toma de conciencia sobre la gravedad que representa para la sociedad los ataques de estas conductas delictivas, ha incidido en la ratificación ese mismo año 2010 del Convenio sobre la Ciberdelincuencia de 2001, modificación de tipos penales para instrumentalizar las nuevas conductas, e inclusive crear tipos penales que prevén el intrusismo y los daños a sistemas de información. No obstante ello, se ha

observado que las nuevas tecnologías ya mencionadas (*blockchain*, Internet de las cosas y *computing cloud*) no han sido objeto de regulación expresa en el plano jurídico penal, existiendo solamente antecedentes y directivas emanadas de la Unión Europea que prescriben el establecimiento de controles administrativos que permitan regular las transabilidad y custodia de los criptoactivos y la instauración de obligaciones a los desarrolladores de los componentes o productos que conforman Internet de las cosas, para mantener actualizados los sistemas de seguridad y confidencialidad.

9. Con respecto al plano de la persecución penal, se ha observado que en el año 2015 fueron incorporados en la Ley de Enjuiciamiento Criminal técnicas de investigación que permiten utilizar esas tecnologías de información para perseguir las conductas desviadas, no obstante ello, se debe afirmar que las mismas deben ser instrumentalizadas para actuar conjuntamente con técnicas de investigación de delincuencia organizada, como por ejemplo, las entregas vigiladas, agentes encubiertos y colaboración de miembros activos de esas organizaciones para obtener un mejor resultado en la lucha contra el flagelo de la delincuencia cibereconómica.

10. Es fundamental la promulgación de normas internacionales para lograr que, de manera uniforme, las empresas prestadoras de servicios de tecnología de información, preserven y garanticen la incolumidad de los datos e informaciones concretas de toda clase que estén almacenados en sus sistemas informáticos. En la medida en que se generalicen estas obligaciones en la mayor cantidad de Estados posibles, aumentará la eficacia en la lucha contra este flagelo y mejores resultados en los procesos investigativos.

11. Por último, se debe resaltar la importancia que representa la tipificación de las nuevas formas delictivas a las que se ha hecho referencia a lo largo del presente trabajo, puesto que de lo contrario el derecho penal no dará respuesta oportuna y satisfactoria a la sociedad, ya que estas nuevas formas de delinquir cada día seguirán avanzando, tecnificándose y afectando gravemente a bienes jurídicos importantes para los individuos y el conglomerado social.

VII. Bibliografía

ABEL SOUTO, M. «*Blanqueo, innovaciones tecnológicas, amnistía fiscal de 2012 y reforma penal*». Revista Electrónica de Ciencia Penal y Criminología, No. 14-14 (2012). Madrid: 2012. Consulta: 18 de junio de 2020. ISSM 1695-0194. Disponible en: http://criminet.ugr.es/recpc/14/recpc14-14.pdf

ALLI TURRILLAS, I. Prevención de la delincuencia grave y organizada en la Unión Europea: De la cooperación a la integración. Madrid, Dykinson: 2016.

AAVV., *Delito e informática. Algunos aspectos*. Bilbao. Universidad de Deusto: 2007.

ANARTE BORALLO, E. «*Incidencia de las nuevas tecnologías en el derecho penal. Aproximación al derecho penal en la sociedad de la información*». Derecho Penal y Conocimiento, vol 1, Huelva: 2001. Consulta: 12 de mayo de 2020. ISNN 1578-8202. Disponible en: http://rabida.uhu.es/dspace/handle/10272/1557

ANGUITA OSUNA, J. «*Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea*». Revista de Estudios en Seguridad Internacional, Vol 4, No. 1, Granada: 2018. Consulta: 29 de abril de 2020. ISSN 2444-6157. Disponible en: http://www.seguridadinternacional.es/revista/?q=content/análisis-histórico-jur%C3%ADdico-de-la-lucha-contra-la-ciberdelincuencia-en-la-unión-europea

BEDECARRATZ SCHOLZ, F. *«Riesgos delicitivos de las monedas virtuales: Nuevos desafíos para el derecho penal».* Revista Chilena de Derecho y Tecnología, vol. 7 núm. 1. Santiago: 2018. Consulta: 17 de junio de 2020. ISSN 0719-2584. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/48515

CÁMAYA, S. «*Estudios criminológicos contemporáneos (IX): La cibercriminología y el perfil del delincuente*». Delito y Cambio Social. Consulta: 12 de mayo de 2020. ISSN 2224-4131 Disponible en: https://www.derechoycambiosocial.com/revista051/ESTUDIOS_CRIMINOLOGICOS.pdf

DÍAZ GÓMEZ, A. «*El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest*». Consulta: 10 de junio de 2020. REDUR, ISSN 1695-078X. Disponible en: https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

DE LA MATA BARRANCO, N. Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general. AAVV., Delito e informática. Algunos aspectos. Bilbao: Universidad de Deusto, 2007.

GARCÍA DE PAZ, I. La criminalidad organizada. Aspectos penales, procesales, administrativos y policiales. Madrid: Dykison, 2008.

GÓMEZ INIESTA, D. *Utilización de las nuevas tecnologías en la comisión del delito de blanqueo de dinero. Ponencia realizada en las V Jornadas Sobre Prevención y Represión de Capitales. Palma: 2017. Disponible en: https://derecho.usmp.edu.pe/cedp/revista/articulos/internacional/definitivo_tec.pdf https://www.youtube.com/watch?v=sRqZ5pFOzTg*

GÓMEZ COLOMER, J. Lección Décima. Los actos de investigación garantizados (II). Modernos medios tecnológicos de investigación. AAVV Derecho jurisdiccional III. Proceso Penal. Valencia: tirant to Blanch, 27 Ed, 2019.

GONZÁLEZ, M. «*La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado*». Grupo de estudios en seguridad internacional de la Universidad de Granada, 46/2017. Disponible en: http://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansión-y-empoderamiento-del-crimen

GONZALE RUS. Precisiones conceptuales y político-criminales sobre la intervención penal en Internet. AAVV., Delito e informática. Algunos aspectos. Bilbao: Universidad de Deusto, 2007

JAISHANKAR, K. «*Cyber criminology as an academic discipline: History, contribution and impact*». International Journal of cyber criminology, 2018. Consulta: el 12 de mayo de 2020. ISSN: 0973-5089. Disponible en: https://www.cibercrimejournal.com/JaiEditorialVol12Issue1IJCC2018.pdf

LÓPEZ-MUÑOZ, J. Criminalidad Organizada. Aspectos jurídicos y criminológicos. Madrid: Dykinson, 2015.

MATA Y MARTÍN, R. *Delincuencia informática y Derecho penal*. Managua: Hispamere, 2003.

MESEGUER GONZÁLEZ, J. «*Los nuevos modi operandi de los ciberdelincuencites durante la crisis económica*». Revista de Derecho UNE, Núm 12, 2013. Consulta: 12

de mayo de 2020. ISSN 2225-3436. Disponible en: http://revistas.uned.es/index.php/RDUNED/article/view/11704/11151

MIRÓ LLINARES, F. «*La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*». Revista Electrónica de Ciencia Penal y Criminología 13-07 (2011). Consulta: 12 de mayo de 2020. ISNN 1695-0194. Disponible en: http://criminet.ugr.es/recpc/13/recpc13-07.pdf

MIRÓ LLINARES, F. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons, 2012.

MORAIS GALLEGO, J. *Las nuevas tecnologías de la información y de la comunicación*. Implicaciones legales. Revista Gallega de Ensino, año 14, No. 14, 2006.

MORÓN LERMA, E. Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. AAVV., *Delito e informática. Algunos aspectos*. Bilbao: Universidad de Deusto, 2007**.**

ORTIZ PARDILLO, J. «*La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*». Estudios de progreso, fundación Alternativas. 2013. Disponible en: https://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf

RAYÓN BALLESTEROS, M. y GÓMEZ HERNÁNDEZ, J. *Cibercrimen: particularidades en su investigación y enjuiciamiento*. Anuario Jurídico y Económico Escurialense. XLVII, 2014. ISNN 1133-3677. Disponible en: http://www.rcumariacristina.net:8080/ojs/index.php/AJEE/article/view/189

SÁNCHEZ DIEZ, I. La estrategia nacional 2013 y las reformas legislativas en materia de seguridad de la X legislatura. Su contribución a la adopción de una nueva concepción de seguridad en España. Salamanca: Ediciones Universidad de Salamanca, 2016.

SÁNCHEZ GARCÍA DE PAZ, I. La criminalidad organizada. Aspectos penales, procesales, administrativos y policiales. Madrid: Dykinson, 2008.

SIEBER, U. Legal aspects of computer-related crime in the information society. Comcrime Study. Consultado el 9 de mayo de 2020. University of Würzburg 1998. Disponible en: https://www.law.tuwien.ac.at/sieber.pdf

VALLEJO, M. y PERRINO PÉREZ, A. La reforma penal de 2015 (Análisis de las principales reformas introducidas en el Código Penal por las Leyes Orgánicas 1 y 2/2015, de 30 de marzo). Madrid: Dykinson, 2015

VIII. Fuentes jurídicas utilizadas

Acuerdo del 26 de mayo de 2009 de la Sala en lo Penal del Tribunal Supremo de Justicia, sobre habilitación de escuchas telefónicas procedentes de diligencias distintas a las que corresponden al juicio. Disponible en: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdo-del-26-de-mayo-de-2009-sobre-Habilitacion-de-escuchas-telefonicas-procedentes-de-diligencias-distintas-a-las-que-corresponden-al-juicio

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, firmado en Palermo, Italia el 15 de noviembre de 2000. Oficina de las Naciones Unidas Contra la Droga y el Delito. Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

Decisión 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999 por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los medios ilícitos y nocivos en las redes mundiales. Diario Oficial No. L 003 de 06 de febrero de 1999, p. 0001 a 0011. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31999D0276

Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32002D0187

Decisión 854/2005/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32005D0854

Decisión 1351/2008/CE del Parlamento Europeo y del Consejo, por la que se establece un programa comunitario plurianual sobre la protección de los niños en el uso de Internet y de otras tecnologías de la comunicación. Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32008D1351

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. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32013L0040

Directiva 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) No. 648/2012, del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión. Disponible e: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015L0849

Directiva 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica las Directivas 2009/138/CE y 2013/36/CE. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32018L0843

Directrices para un enfoque basado en riesgo para Monedas virtuales. Grupo de Acción Financiera Internacional (GAFI), de junio 2015. Disponible en: https://www.fatf-gafi.org/media/fatf/documents/Directrices-para-enfoque-basada-en-riesgo-Monedas-virtuales.pdf

Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. *Boletín Oficial del Estado.* 22 de febrero de 2019, núm. 46, páginas 17048 a 17074. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-2442

Informe A8-0272/2017 del Parlamento Europeo, de 25 de julio de 2017, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32013L0040

Instrumento de ratificación de 14 de julio de 1982, del Convenio Europeo de Extradición hecho en Estrasburgo el 20 de abril de 1959. *Boletín Oficial del Estado.* 17 de septiembre de 1982, núm. 223, páginas 25166 a 25174. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1982-23564

Instrumento de ratificación de 21 de abril de 1982, del Convenio Europeo de Extradición hecho en París el 13 de diciembre de 1957. *Boletín Oficial del Estado.* 8

de junio de 1982, núm. 136, páginas 15454 a 15462. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1982-13611

La Convención sobre Extradición, firmada en Montevideo, Uruguay el 26 de diciembre de 1933. VII Conferencia Internacional Interamericana. Disponible en: http://cedhvapp2.sytes.net:8080/derechos_humanos/file.php/1/Instrumentos%20internacionales%20DH/22abis.pdf

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado.* 24 de noviembre de 1995, núm. 281, páginas 33987 a 34058. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1995-25444

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. *Boletín Oficial del Estado.* 23 de junio de 2010, núm. 152, páginas 54881 a 54883. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-9953

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. *Boletín Oficial del Estado.* 31 de marzo de 2015, núm. 77, páginas 27061 a 27176. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-3439

Ley Orgánica 1/2019, de 20 de febrero, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para transponer Directivas de la Unión Europea en los ámbitos financiero y terrorismo, y abordar cuestiones de índole internacional. *Boletín Oficial del Estado.* 21 de febrero de 2019, núm. 45. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2019-2363#au

Ley Orgánica 7/2003, de 30 de junio, de medidas de reforma para el cumplimiento íntegro y efectivo de las penas. *Boletín Oficial del Estado.* 1 de julio de 2003, núm. 156, páginas 25274 a 25278. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2003-13022

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 tecnológicas. *Boletín Oficial del Estado.* 6 de octubre de 2015, núm. 239, páginas 90192 a 90219. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10725

Orden PCI/161/2019, de 21 de febrero, por la que se aprueba el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional Contra el Crimen Organizado y la Delincuencia Grave. *Boletín Oficial del Estado.* 22 de febrero de 2019, núm. 46, páginas 17048 a 17074. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-2442

Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017. *Boletín Oficial del Estado.* 21 de diciembre de 2017, núm. 309, páginas 125966 a 126004. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-15181

Sentencia de 7 de diciembre de 2011, 173/2011, ES:TC:2011:173, apartado 5 de los fundamentos jurídicos. Disponible en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/22621

Sentencia de 26 de septiembre de 2012, 6215/2012, ES:TS:2012:6215. Disponible en: http://www.poderjudicial.es/search/AN/openDocument/571349c74b50a172/20121016

Sentencia de 17 de abril de 2013, 342/2013, ES:TS:2013:342. Disponible en: http://www.poderjudicial.es/search/AN/openDocument/2e85127950d8cc20/20130521

Sentencia de 23 de abril de 2014, 1486/2014, ES:TS:2014:1486. Disponible en: http://www.poderjudicial.es/search/AN/openDocument/02a2336685e61ccd/20140505

Sentencia de 26 de noviembre de 2014, 850/2014, ES:TS:2014:850. Disponible en: https://www.iberley.es/jurisprudencia/sentencia-penal-n-850-2014-ts-sala-penal-sec-1-rec-10269-2014-26-11-2014-14918871

Sentencia de 19 de mayo de 2015, 2047/2015, ES:TS:2015:2047. Disponible en: http://www.poderjudicial.es/search/AN/openDocument/588d270cb80152a8/20150527

Sentencia de 3 de octubre de 2018, 294/2018, ES:APTF:2018:1900. Disponible en: http://www.poderjudicial.es/search/AN/openDocument/ff276bf5ad0673a3/20190214

Sentencia de 20 de junio de 2019, 326/2019, ES:TS:2019:2019. Disponible en: http://www.poderjudicial.es/search/AN/openDocument/4531032d6c25c96f/20190705

IX. Otras fuentes

«***About CoinMarketCap***» *coinmarketcap* 18 de junio de 2020, 17:00. Disponible en: https://coinmarketcap.com/about/

«**Ashton, un tecnólogo visionario**» *eexcellence.es.* 26 de abril de 2020, 10:00. Disponible en: http://www.eexcellence.es/index.php/expertos-en-gestion/kevin-ashton-un-tecnologo-visionario

«**Cybercrime**» *europol.europa.eu*. 6 de mayo de 2020, 11:30. Disponible en: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Definicion de Aldea Global. *Definición.de*. 17 de junio de 2020, 17:00. Disponible en: https://definicion.de/aldea-global/

«Delincuencia Organizada transnacional: la economía ilegal mundializada». *Unodc.org.* 17 mayo 2020, 11:00. Disponible en: https://www.unodc.org/toc/es/crimes/organized-crime.html

«El Centro Europeo de Ciberdelincuencia (EC3) se inaugura el 11 de enero» *ec.europ.eu*. 6 de mayo de 2020, 11:00. Disponible en https://ec.europa.eu/commission/presscorner/detail/es/IP_13_13

«El hospital privado más grande de Europa afectado por ransomware en medio de la pandemia». *es.cointelegraph*. 18 de junio de 2020, 12:00. Disponible en https://es.cointelegraph.com/news/europes-largest-private-hospital-hit-by-crypto-ransomware-amid-pandemic

«El Ministerio de Asuntos Económicos y Transformación Digital avanza en el refuerzo de los sistemas de prevención de blanqueo de Capitales y Financiamiento al Terrorismo». *mineco.gob.es.* 19 de Junio de 2020, 11:00. Disponible en https://www.mineco.gob.es/portal/site/mineco/menuitem.ac30f9268750bd56a0b0240e026041a0/?vgnextoid=90b5bfcf4e8a2710VgnVCM1000001d04140aRCRD&vgnextchannel=864e154527515310VgnVCM1000001d04140aRCRD

«***Europol Strategy* 2016-2020**» *europol.europa.eu.* 6 de mayo de 2020, 10:00. Disponible en https://www.europol.europa.eu/publications-documents/europol-strategy-2016-2020

«**Información sobre Europol**» *eur-lex.europa.eu*. 6 de mayo de 2020, 09:00. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELLAR:7f9036bd-ac1d-4305-887d-4c5841f9279b&from=FR

«***Is the mafia taking over cybercrime*?**» *i.blackhat.com.* 18 de mayo de 2020. 7:00. Disponible en: https://i.blackhat.com/us-18/Wed-August-8/us-18-Lusthaus-Is-The-Mafia-Taking-Over-Cybercrime-wp.pdf

«**Los ataques a aplicaciones *cloud* aumentan un 65% en el primer trimestre de 2019**» *cuadernosdeseugirdad.com.* 24 de abril de 2020, 11:00. Disponible en: https://cuadernosdeseguridad.com/2019/03/los-ataques-a-aplicaciones-cloud-aumentan-un-65-en-el-primer-trimestre-de-2019/

«**Oculto a simple vista: el grupo 'Saguaro' ataca América Latina utilizando técnicas sencillas, pero eficaces**» *latam.kapersky.com* de 24 de junio de 2020, 11:00. Disponible en: https://latam.kaspersky.com/blog/oculto-a-simple-vista-el-grupo-saguaro-ataca-america-latina-utilizando-tecnicas-sencillas-pero-eficaces/7589/

«**Oficina Europea de Policía (Europol)**» *europa.eu*. 6 de mayo de 2020, 09:30. Disponible en: https://europa.eu/european-union/about-eu/agencies/europol_es

«**Qué es internet de las cosas y cómo funciona**» *hostgator.mx* 26 de abril de 2020, 11:00. Disponible en: https://www.hostgator.mx/blog/Internet-de-las-cosas/?__cf_chl_captcha_tk__=ca4b47be6c3be26359d2ab3bb9164e1c65bbc140-1587901341-0-AaeAUL5blDmYDFMZ2wZdUGO-d9XnLK4QcS4TKqJ7ZJVwIGkDB2N2Suo-DDM5hCKVexNl1qPio_x2zflzDcS7uqZDSrrj-TcLI9n7HE9PeD3L_G4bBgadT0j8NW1SzhFcwZq0Nc2lwZsZu6HtDR_Vmm7CDvNhxPdgy8-KDEc_yGVBPEpiaiguVF4yhsUHPYASXgn8UzcUew2BhTwzTjSsLsnj4jltp4nfRXBtMwysuOX3fM_hLce8BeROf3p-p6nuaOo0L2ljj44X9e-k4_AcR1oJedzt-KwhFp2xGzv6B-6AIUT_k9rA7j7bHOaSdVmdxaPyTj5wEs2ISwUq-MN9bYSD6dISv5hRlGBTvO0XshzKygBuunH0VI775cegsZRGj5wW5rKfV0CzxuSsTr8XsVptjIMENY3aZ3DS8WfjaBeveBNRfGKt5rI5MEPFpG12VOo2JD2AhEdMUgQk9rvxlGheqiLYyPWAdtQc2ZfOe2megOuu7l94a-dDPlbJ4JcfsEKmVWhPZ1g2fxSVpYf7kLY

«**Qué es Interpol**?» *Interpol.int.* 18 de mayo de 2020, 10:00. Disponible en https://www.interpol.int/es/Quienes-somos/Que-es-INTERPOL

«**Qué es un *Ransomware***?» *pandasecurity*. 18 de junio de 2020, 12:00. Disponible en: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

«***That 'Internet of things' thing***» *rfidjournal.com.* 25 de abril de 2020 09:00. Disponible en: https://www.rfidjournal.com/articles/view?4986

«***The NIST Definition of cloud computing***» *nvlpubs.nist.gov*. 24 de abril de 2020, 10:00. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

«***Tor y Deepweb*: todos los secretos del lado oscuro de la red**». *Pandasecurity.com*. 14 de abril de 2020, 11:00. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/

«Tratados Multilaterales». *Oas.org*. 18 de mayo de 2020, 15:00. Disponible en: https://www.oas.org/juridico/spanish/tratados/b-47.html