ISSN 2007-4700

Revista Penal

MÉXICO

Número 23
julio - diciembre 2023

Revista Penal México 23
Doctrina
Núm. 23, julio - diciembre de 2023

Los delitos realizados mediante la Dark Net

Susana Ma. Barón Quintero

Abogada del Ilustre Colegio de Abogados de Huelva
Doctoranda Universidad de Huelva

***Resumen**: La sociedad de la información, el ciberespacio, Internet, las nuevas tecnologías y la aparición de nuevas formas de comisión de los delitos tradicionales mediante la Dark Net, que preserva el anonimato y genera problemas en la persecución y criminalización en el entorno digital, nos obliga a diseñar y establecer un régimen jurídico penal europeo, internacional, uniforme y coordinado por los que puedan perseguirse con instrumentos eficaces este tipo de criminalidad.*

***Palabras clave:** Dark Net- Deep Web- Ciberdelitos- Ciberespacio- Tecnologías de la información y comunicación (*TIC*)- Instrumentos de cooperación internacional.*

***Abstract:** The information society, cyberspace, the Internet, new technologies and the emergence of new ways of committing traditional crimes through the Dark Net, which preserves anonymity and generates problems in the prosecution and criminalization in the digital environment, obliges us to design and establish a European, international, uniform and coordinated criminal legal regime by which this type of criminality can be prosecuted with effective instruments.*

***Keywords:** Dark Net- Deep Web- Cybercrime- Cyberspace- Information and communication technologies (*ICTS*)- International cooperation instruments.*

Rec: 20/06/2023 | **Fav:** 19/07/2023

1. Introducción

El mundo digital es actualmente un escenario muy prolífero para la comisión de un delito informático, delito cibernético o ciberdelito, consistiendo ello en toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet.

En este ciberespacio existe, además de plataformas o sistemas de búsquedas *on line* tradicionales que permiten conocer solo con un seguimiento de historial de búsqueda por Internet en qué sitios web nos estamos moviendo, un Internet que no se muestra y opera de forma subrepticia y opaca, utilizando plataformas que permite encriptar la información a través de la aplicación llamada TOR.

Realmente no se comete ningún tipo de delito por navegar en la Dark Net, puesto que su uso es legal, y lícito también es el hecho de que un usuario quiera preservar su anonimato y no dejar rastros de los sitios por los que navega como ocurre, sin embargo, cuando entras en un portal tipo Google.

Así, lo que realmente se castiga y penaliza es utilizar esta Dark Net para cometer determinadas categorías de delitos y evitar la persecución y quedar impune al ser bastante difícil el localizar al autor o autores de los hechos delictivos por el tipo de plataforma opaca de la que se valen para su comisión y la complejidad en rastrear las IP de los ordenadores y dispositivos digitales utilizados.

Por tanto, los delitos realizados mediante la Dark Net, también llamada Deep Web, son aquellas infracciones y conductas delictivas que se realizan a través de la Deep Web que representa el 90% de Internet y a la que no se puede acceder o ingresar de forma habitual como cuando ingresamos a Google u otro buscador, porque son sitios que los motores de búsqueda normales no pueden registrar, de tal forma que conserva el anonimato y la información personal que se guarda en el entorno digital.

Debido a la cantidad de información sensible, a la Deep Web se le puede comparar con un mercado negro, ya que esta atrae la atención de personas que no siempre tienen buenas intenciones, y saca a relucir la parte más oscura del ser humano, que se aprovecha del anonimato existente dentro de los varios niveles de la Deep Web; se llega a encontrar pornografía infantil, incluso terrorismo o secretos de estado en los niveles más profundos. Hacer constar que Internet en general permite la transmisión y distribución de forma instantánea de cualquier tipo de dato de forma relativamente sencilla en relación con otros medios de comunicación.[1]

El uso de la informática es el *modus operandi* nuevo que plantea su propia forma comisiva respecto de las formas tradicionales de comisión. Existe en la persecución de estos ilícitos un claro problema de conciencia de culpabilidad por el autor de los delitos mediante Internet al cometerse en un espacio virtual que escapa al espacio terrenal, no asumiendo el reproche penal.

La criminalidad informática puede incluir delitos tradicionales como el fraude, el robo, chantaje, estafas, falsificación, malversación de caudales públicos, prostitución y pornografía infantil, tráfico de armas y de drogas, terrorismo islámico, en los que los ordenadores y redes han sido utilizados como medio y la comisión de estos. Con la evolución y el desarrollo de Internet son más frecuentes y sofisticados a fin de evitar la criminalización y condena.

Las nuevas tecnologías y el mundo digital y ciberespacio se usan en todos los ámbitos de nuestras vidas. Es este entorno digital el que eligen determinados tipos de delincuentes para realizar hechos delictivos valiéndose de la tecnología informática como instrumento o medio para su perpetuación, y ofrece contornos singulares y problemas propios.

Los hechos delictivos que se realizan mediante Internet plantean numerosos problemas a la hora de su persecución e incriminación, puesto que en la mayoría de los casos surgen dificultades al plantear la ubicación y lugar de comisión de tales hechos ilícitos, indispensable para la determinación de la jurisdicción y competencia penal, para su enjuiciamiento y aplicación de la correspondiente ley penal; la localización y obtención de las pruebas de tales hechos delictivos; la insuficiente regulación legal de los ilícitos que pueden realizarse a través de la red o de las diligencias procesales de investigación aplicables para el descubrimiento de los mismos —normativa igualmente desbordada por el imparable avance de las innovaciones tecnológicas—; la cooperación europea e internacional para su lucha y persecución, o incluso la significativa afectación que la investigación policial

[1] Cohen-Almagor, R. "Online Child Sex Offenders: Challenges and Counter-Measures". *The Howard Journal of Criminal Justicie*. Vol 52. Mayo 2013.

en Internet tiene sobre los derechos fundamentales de los ciudadanos.

En aras de su persecución de forma global, además de las leyes nacionales que tienen por objeto la protección y seguridad de los sistemas y tecnologías de la información y la prevención y sanción de los delitos cometidos por medios informáticos, la Unión Europea ha establecido una serie de medidas dirigidas a garantizar y preservar una seguridad en las redes y sistemas informáticos, de tal forma que nació la Directiva NIS, que impone a los Estados miembros y a sus entidades gestoras de servicios esenciales y digitales la obligación de establecer sistemas de control-gestión de seguridad de la información y de supervisión de dicha información y el intercambio y cooperación trasnacional.

2. Perspectiva y tratamiento de los delitos realizados mediante la Dark Net en el Código Penal

Los delitos realizados mediante la Dark Net o Dark Web, son en definitiva infracciones delictivas que se encuadran dentro de la delincuencia o criminalidad informática. Las definiciones que a lo largo de los últimos cuarenta años se han aportado del concepto de delito informático van necesariamente unidas a la evolución que ha sufrido la implantación de las TIC (tecnologías de la información y comunicación) en la sociedad y a las propias conductas delictivas, o merecedoras de serlo, vinculadas con las nuevas TIC. Así, las primeras infracciones que aparecieron vinculadas al uso masivo de los ordenadores se centraban, principalmente, en el ámbito empresarial y consistían en conductas lesivas contra el patrimonio.

En el Código Penal español vigente los delitos realizados mediante la Dark Net no tienen su encuadre en ninguna conducta tipificada penalmente y tampoco existe un título en el Código Penal sobre los delitos informáticos, encontrándose las distintas conductas delictivas vinculadas con los sistemas informáticos, ya sea por el medio de comisión, ya por el objeto del delito, ya incluso por ambos aspectos, dispersas en diferentes títulos del código en una ubicación en que lo que prima es el bien jurídico afectado.

La doctrina mayoritaria prefiere emplear el término de "delincuencia informática" o "criminalidad informática"[2] para incluir en ellas todos los comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera, y todos aquellos en que dicho sistema sea el propio objeto sobre el que recae la acción delictiva.

Tiedemann[3] considera que con la expresión "criminalidad mediante computadoras" se alude a todos los actos antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos. Como el mismo autor señala, el concepto abarca el problema de la amenaza a la esfera privada del ciudadano y, por otra parte, se refiere además a los daños patrimoniales producidos por el abuso de datos procesados automáticamente.

Como afirma Gutiérrez Francés:[4]

> … con carácter general, la delincuencia mediante computadoras se inscribe dentro de las formas de criminalidad de "Cuello Blanco", propias de la delincuencia económica, por lo cual desde el punto de vista criminológico, presentan las mismas peculiaridades que ésta, con las notas específicas que aporta lo informático.

De esta forma podemos decir que no existe una definición como tal del concepto de delito informático que sea unánime a todos los países, es más, en el Código Penal español, como ya hemos señalado, no viene siquiera definido como tal dicho concepto.

En España se han ido adoptando diversas modificaciones legislativas al objeto de adecuar la legis-

[2] ROMEO CASABONA, Carlos María, *Poder informático y seguridad jurídica*, Fundesco, Madrid, España, 1987. En ese orden de ideas y siguiendo al profesor Romeo Casabona, el cual señala: "En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información".

[3] TIEDEMANN, Klaus, *Poder informático y delito*, Barcelona, 1985.

[4] GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*. Ministerio de Justicia. Secretaría General Técnica. Centro de Publicaciones. 1991

lación a las directivas comunitarias y así facilitar la cooperación con otros estados en materia penal. Por todo esto, para poder acercarnos a la definición del delito informático es necesario recurrir al *Convenio sobre Ciberdelincuencia, del Consejo de Europa de 2001*,[5] ya que en su preámbulo indica que se hace necesario la tipificación como delito de "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".

En el convenio se establecen los delitos informáticos en cuatro grupos, donde vienen a definirse los tipos penales que deben considerarse delito informático. Estos grupos son los siguientes:

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

Mencionar la Instrucción 2/2011[6] dictada por la Fiscalía General del Estado por la que se crea la figura del fiscal de Sala de Criminalidad Informática y en la que, además, se trata de concretar el catálogo inicial de delitos a los que se extiende el marco competencial de esta área. El catálogo se ha estructurado en tres categorías:

> … delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICS, delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICS y delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICS, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia.

En cualquier caso, todo lo que es cibernético o telemático es también, al mismo tiempo, informático; mientras que no ocurre lo mismo en sentido inverso, siendo por tanto mucho más omnicomprensiva esta última categoría.

Los ciberdelitos, que han aumentado con la expansión y proliferación de Internet, son en definitiva los delitos sancionados en el Código Penal mediante un nuevo canal, medio, plataforma, que facilita su comisión y genera problemas de persecución y sanción, y todos o prácticamente todos los delitos que están regulados en nuestro sistema punitivo pueden cometerse a través de un sistema informático que es merecedora de la tutela penal y judicial.

Parece existir, en síntesis, una categoría criminológica que puede denominarse criminalidad informática, delincuencia informática o delitos informáticos,

[5] Convenio sobre Ciberdelincuencia del Consejo de Europa. Budapest. 23-11-2001. España firmó el tratado el 23 de noviembre de 2001 y lo ratificó mediante el instrumento de ratificación del convenio el 1 de octubre de 2010.

El Convenio cuenta con 64 Estados Parte, incluidos países de nuestro continente americano como Argentina, Canadá, Chile, Colombia, Costa Rica, Estados Unidos, Panamá, Paraguay, Perú y República Dominicana.

Es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de la seguridad en redes. También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la intercepción de comunicaciones privadas.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Los principales objetivos de este tratado son los siguientes:

1. La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.
2. La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.
3. Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

[6] Completada posteriormente por la Instrucción de la FGE n° 4/2011 y nº1/2015.

que incluye todas las conductas sancionadas por el Código Penal que tengan vinculación con la informática, bien en su medio comisivo, bien en el objeto sobre el que recae la conducta, bien en ambos u otros ilícitos que en su momento puedan entrar a formar parte de él; pero no existe tipificación alguna de los delitos realizados como tal en la Dark Web.

3. Aproximación a los delitos realizados mediante la Dark Net

Los delitos realizados mediante la Dark Net pueden manifestarse con una tipología delictiva plural. Son delitos que se pueden realizar en la forma que establece nuestro sistema punitivo, castigado por el Código Penal, que afectan y ponen en peligro a bienes jurídicos distintos, y el único elemento diferenciador es la plataforma por medio de la cual se ejecuta y despliega sus efectos la actividad delictiva, en este caso "a través del internet profundo, oscuro, Dark Web".

La Dark Net es una red que forma una pequeña parte de la Deep Web donde todo es anónimo y está cifrado, de tal forma que no es posible entrar en ella con navegadores o buscadores normales, sino con el famoso navegador TOR. Esta red permite que los cibercriminales puedan compartir fácilmente contenidos ilegales sin poder ser rastreados.

La utilización de foros o canales encriptados o el uso de la Dark Net ha servido para que los ciberdelincuentes o grupos criminales establezcan sus comunicaciones e interactúen, lo que dificulta la actividad de las fuerzas de inteligencia policial y el acceso a pruebas esenciales en la investigación. En la Dark Net se puede disponer de casi todo. Se ha utilizado para el intercambio de material de explotación sexual infantil y para otros tipos de actividades ilícitas como el tráfico de drogas o armas. Los grupos criminales tenían técnicas para realizar ciberataques limitados, pero la disponibilidad de herramientas y servicios para los delitos informáticos que se disponen en la Dark Net les ofrece posibilidades de cambio, teniendo que prestar mucha atención a los actores terroristas en este fenómeno. La Dark Net engloba un mundo paralelo delincuencial que escapa al mundo exterior.

Una de las amenazas más importantes es el ciberespionaje tanto de carácter económico como político. El primero afecta la propiedad intelectual de empresas públicas y privadas, y, el segundo, se ha detectado entre estados.

4. Concepto de los delitos en la Dark Net

Esto hace referencia a una clase de contenido que no puede ser accedido por motores de búsqueda tradicionales, pues dicho contenido ha sido deliberadamente no indexado.

El primer antecedente de esta red profunda se remonta a la creación de la Silk Road, el primer mercado negro online, creado por Ross Ulbricht, y en el cual los distintos usuarios podían encontrar todo tipo de productos de contrabando, principalmente drogas ilegales, hasta que fue desmantelada por el FBI en 2013.[7] Este tipo de mercados negros abriría paso a más ventas ilegales.

Los criminales aprovechan la excepcionalidad del anonimato de la red oscura; sus actividades son indetectables, y los recursos, invisibles.[8] Por tal motivo, la red oscura ha sido utilizada para la comisión de delitos y acceso a recursos de todo tipo de magnitud y nivel.[9]

Las acciones que principalmente hay que destacar son:

- Financiero: lavado de bitcoins, cuentas robadas de PayPal, tarjetas de crédito clonadas y prepagadas, falsificación de dinero.
- Comercial: explotación sexual, mercado negro, gadgets robados, armas y municiones, falsificación de documentos, venta de drogas, medicamentos, software.
- Anonimato y seguridad: instrucciones para reforzar la seguridad del acceso; acceso a mercado negro de sicarios.
- Servicio de hosting: sitios de alojamiento con absoluta privacidad.
- Blogs, foros y tablones de imágenes: compraventas, hacking e intercambio de imágenes; foros de crackers en busca de víctimas.
- Servicio de correo y mensajería: gratis y de pago con SSL y soporte de IMAP. Los chats sobre IRC o XMPP.
- Activismo político: archivos censurados, hack-

[7] SUI, CAVERLEE & RUDESILL, "The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box". Woodrow Wilson International Center for Scholars, STIP 03, October 2015.

[8] Cooper & Chikada, Dark Web: "A Boon or a Bane" Encyclopedia of Criminal Activities and the Deep Web (pp.152-164) Publisher: IGI Global. 2015.

[9] Gallardo J." La Mitad invisible". Editorial Planeta. 2017.

tivismo y anarquía; documentos clasificados.
- Secretos de Estado y soplones: un mirror de WikiLeaks y lugares para publicar
- Páginas eróticas: pornografía de pago y libre acceso, sin límite moral.
- Hackeo por encargo: Ataques DDOS, troyanos, phishing, spamming, botnet agents.
- Libros: miles de e-books libres de copyright y en distintos formatos, así como descargas ilegales.

5. Problemática general ante una nueva y particular forma de delincuencia

5.1 Aspectos generales

La sociedad de la información, y su medio más espontáneo y representativo como es Internet, y la aparición de una serie de conductas delictivas que no se ejecutaban por Internet y actualmente si (puesto que supone una mayor garantía en los resultados y un mínimo riesgo de represión por parte de las leyes penales), nos obligan a diseñar y establecer un régimen jurídico penal europeo, internacional, uniforme y coordinado por los que puedan perseguirse.

La nueva comisión delictiva surgida a través de la red, los llamados delitos informáticos, teniendo en cuenta que gran parte de los delitos tipificados en nuestro Código Penal son susceptibles de ser delitos informáticos (es decir, pueden ser cometidos a través de Internet), supone que la investigación penal hay que llevarla a efecto sobre las nuevas tecnologías en general, dado que hay sistemas o datos informáticos que pueden servir de soporte a información personal y confidencial: teléfonos móviles, agendas electrónicas, utilización de un cajero automático, etc. Todos ellos contienen sistemas informáticos y en particular cuando los delitos sean realizados utilizando no el Internet al que accedemos para acceder a cualquier información, búsqueda, objeto, etc., sino que se trata de un Internet profundo, oculto, que preserva el anonimato del usuario. Recalcar que no toda navegación en dicho Internet profundo es delictiva, sino que lo que hace el uso del Internet delictivo es la comisión de las acciones tipificadas como delictivas en nuestro Código Penal y en el ámbito europeo e internacional, que atentan contra bienes jurídicos dignos de protección penal.

Así, los propios delitos convencionales se pueden vehiculizar a través de la red de redes que es Internet, y en este caso de análisis el Internet oscuro-profundo, e incluso en cualquier otro delito clásico para cuyo descubrimiento o comisión se hayan utilizado en todo o parte esas nuevas tecnologías.

La multiplicidad y universalidad de la acción criminal que las TIC permiten, generando multitud de víctimas, la complejidad y perdurabilidad de las aplicaciones técnicas que cotidianamente se ven afectadas a través de Internet, unido a la problemática que para la investigación penal suponen la rápida desaparición de los rastros que deja el delincuente, la mutabilidad en la conservación de los mismos o la necesidad de su traducción a soportes no electrónicos que faciliten su observación y comprensión, genera la necesidad de configurar un marco legal específico que, debidamente encajado en el régimen jurídico vigente, otorgue las armas jurídicas para combatir este tipo de delincuencia virtual.

5.2 Regulación en el sistema español

Este apartado se trata de analizar si, en el estado actual, nuestro ordenamiento jurídico ofrece mecanismos de tutela suficientes y adecuados para proteger a los ciudadanos en general frente a las infracciones cometidas por medio de Internet profunda. El derecho nacional, junto al derecho de la Unión Europea, ha configurado en los últimos años un sistema que permite obtener la protección de los usuarios de Internet ante los tribunales españoles; ahora bien, la eficiencia de esta tutela se plantea como un reto que exige conocer las particularidades de la materia y utilizar de forma correcta los distintos instrumentos procesales, tanto en el ámbito español como trasnacional.

La normativa española en ciberdelincuencia se genera tras el Convenio sobre la Ciberdelincuencia, firmado en Hungría el 23 de noviembre de 2001,[10] ratificado por España el 3 de junio de 2010, entrando en vigor el 1 de noviembre del 2010.

En junio de 2022, 66 Estados eran partes del Convenio de Budapest. Forman parte la mayoría de estados europeos, EE. UU. y varios países de América Latina, entre otros: Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú, República Do-

[10] Convenio sobre Ciberdelincuencia del Consejo de Europa. Budapest. 23-11-2001

minicana, Australia, Cabo Verde, Canadá, Filipinas, Ghana, Israel, Japón, Marruecos, Mauricio, Senegal, Tonga y EE. UU.

El 12 de mayo de 2022 España firma el segundo protocolo, que había sido adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021 y mejora y complementa lo establecido en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, firmado en Budapest en 2001, así como el protocolo adicional del mismo, firmado en Estrasburgo en 2003.

Los objetivos principales del Convenio y sus protocolos son armonizar la tipificación de una serie de conductas como delito entre los diferentes estados firmantes, dotar de herramientas procesales para la investigación y enjuiciamiento de ciberdelitos y establecer procedimientos de cooperación internacional.

Otro elemento clave para el desarrollo de la normativa española es el papel armonizador que desempeña la Unión Europea, como ente supranacional, de acuerdo con lo establecido en el art. 83.1 del Tratado de Funcionamiento de la Unión Europea (TFUE) que otorga competencias a la UE para determinar y regular infracciones penales y sus correspondientes sanciones en lo referido a delincuencia informática, entre otros ámbitos. Resaltar en este sentido las directivas y decisiones marco que han derivado en normativa interna del Estado de acuerdo con el procedimiento de transposición.

Señalar especialmente la Directiva 2013/40/UE que dice

> … aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación entre las autoridades competentes, incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

Esta Directiva 2013/40/UE motivó las reformas de 2015 del Código Penal, con la inclusión de nuevos tipos delictivos cometidos a través de las TIC, y la Ley de Enjuiciamiento Criminal (LECrim), que contempla nuevas medidas de investigación tecnológica y la creación de la figura del agente encubierto informático.

También mencionar la Directiva 2000/31/CE, que provocó la aprobación de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI) que contempla y limita la responsabilidad de prestadores de servicios, operadores de red y proveedores de acceso.

Otra medida relevante en el ordenamiento español que refleja la importancia de la ciberdelincuencia ha sido la creación de la Fiscalía Especializada en Delitos Informáticos a raíz del Real Decreto 1735/2010. Como define la Instrucción nº 2/2011, de 11 de octubre, sobre el fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las fiscalías, el objeto de esta Fiscalía comprende tres categorías: delitos cuyo objeto delictivo son los propios sistemas informáticos o las TIC (sabotaje informático, acceso sin autorización a datos, programas o sistemas informáticos, revelación de secretos, entre otros); delitos cuya actividad criminal se sirve de las TIC (estafas informáticas, delitos contra la propiedad intelectual, corrupción de menores y personas discapacitadas, pornografía infantil, entre otros) y, por último, delitos cuya actividad criminal, además de servirse de las TIC, requieren conocimientos técnicos para su investigación (falsificación documental, injurias y calumnias contra funcionarios públicos, amenazas y coacciones, delitos contra la integridad moral, apología o incitación a la discriminación, el odio y la violencia, justificación de los delitos de genocidio, entre otros).

El régimen jurídico en España, tras las modificaciones operadas por la reforma del Código Penal por la Ley Orgánica 5/2010, de 22 de junio, tras el Convenio de Budapest de 2001 y las directivas europeas que han generado reformas en el Código Penal del 2015, se ha ido perfilando, y actualmente nos encontramos que, a efectos de poder probar estos delitos, se debe incidir, por un lado, sobre derechos fundamentales de nueva generación, cuyo tratamiento está configurando todavía la última jurisprudencia, pero a la vez, y por otro lado, en derechos fundamentales ultra clásicos, que están aportando las nuevas tecnologías, por lo que deberá hacerse desde la perspectiva que menos afecte a los derechos fundamentales recogidos en el artículo 18 de la Constitución española (entradas y registro, ocupación de efectos en soportes electróni-

cos, intervención de telecomunicaciones, detención de correspondencia, etc.) y a la legislación ordinaria referente a la sociedad de la información, las nuevas telecomunicaciones (correo electrónico, SMS, chats, etc.) y la protección, cesión y conservación de datos, sin olvidar las especificidades de la prueba reina en la materia: la pericial informática, con sus peculiaridades sobre la cadena de custodia, el volcado, clonado, y análisis de datos, etcétera.

También, la filmación de lugares, la videograbación y la videoconferencia y otras técnicas de investigación penal vinculadas a las nuevas tecnologías (rastreos, señas IP, entregas vigiladas a través de Internet, infiltración y agente encubierto en Internet o tecnovigilancia, balizas y GPS) o la intervención de las líneas ADSL o la introducción de virus "troyanos" espías para la investigación criminal, así como las diligencias policiales, las medidas cautelares y restrictivas en Internet (retirada, bloqueo e interdicción de acceso en España de Webs ilícitas), y el comiso, las consecuencias accesorias y la responsabilidad de los agentes que operan a través de Internet.

Las continuas y variadas formas de los ataques criminales tecnologizados obligan a conocer sus vías de comisión para combatirlas, a ensayar nuevas maneras de hacerlas frente desde la legalidad y a tratar de interpretar la afección a los derechos fundamentales.

Para ello, se ha ido desarrollando cada vez más a partir de la proliferación de este tipo de delincuencia lo que se denomina como ciberseguridad, entendida como la técnica que combina informática y telemática con el objetivo de proteger el buen funcionamiento de sistemas informáticos y redes, evitando que se comprometa o sabotee la información que por ellos circula. Actuando en consecuencia como técnica de prevención y detección de determinados ciberdelitos.

En cualquier caso, hay que hacer una distinción o precisión en la terminología jurídica y distinguir entre cibercrimen y ciberdelincuencia, que a priori pueden parecer sinónimos y tienen un matiz más bien criminológico, ya que hacen referencia al conjunto de conductas llevadas a cabo a través de las TIC y que podemos considerar "desviadas" de lo comúnmente aceptado en un entorno social determinado, sin que se considere conducta desviada el hecho de que se trate de un delito tipificado en el Código Penal.

Así, los ciberdelitos son las conductas típicas expresamente previstas y recogidas como delito en el Código Penal y cuya característica principal radica en que su objetivo o medio de comisión son los sistemas informáticos o las TIC en general, pero ciertamente por la utilización masiva y extensa de las TIC, lo podría encuadrar a la casi totalidad de delitos recogidos en el Código Penal.[11]

Los ciberdelitos en sentido estricto son exclusivamente aquellas conductas en las que el Código Penal haga específica alusión a la afectación o utilización de sistemas informáticos o los que presenten una modalidad de comisión habitual a través de las TIC.

A nivel técnico, es cierto que hay muchos tipos de ciberataques, pero se han de encajar en estos tres bloques y en sus delitos correspondientes como el phishing, todo tipo de spyware, etcétera.

El Código Penal español no tiene tipificado en sí un tipo autónomo de ciberdelito, sino que su regulación se determina en función del bien jurídico protegido en el ámbito de los delitos informáticos, definiéndose como delito informático la que utiliza la Unión Europea: "aquellas actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas".

De este modo, existen ciberdelitos que atentan contra la intimidad, patrimonio, libertad, honor o libertad e indemnidad sexual, entre otros. Por otro lado, se han incluido modalidades en tipos tradicionales, existiendo dispersión en todo el Código Penal.

En síntesis, la tipología delictiva se puede clasificar en los siguientes tipos:

a. Conductas delictivas de tipos penales tradicionales que se desarrollan a través de las TIC.
   Ejemplo: delito de estafa del art. 248.2 CP.
b. Publicación de contenidos ilegales en la red.
   Ejemplo: enaltecimiento del terrorismo del art. 158.2 CP.
c. Delitos específicos de las TIC.
   Ejemplo: Sabotaje informático del art. 264 C.p, hacking.

A continuación, se muestra el listado de los delitos informáticos tipificados desde la reforma del 2015 del Código Penal y a consecuencia del mandato europeo.[12]

[11] Galán Muñoz, A. "Los Ciberdelitos en el ordenamiento español." 2019. Editorial: Universitat Oberta de Catalunya (UOC).

[12] CANO TERUEL, Q. *Ciberdelincuencia en el Código Penal. 4-12-202.*

1. Descubrimiento y revelación de secretos de empresa

La diferencia respecto al descubrimiento y revelación de secretos personales es que en la empresa el bien jurídico protegido no es la intimidad personal o familiar, sino el patrimonio y el orden socioeconómico. Así, el art. 278.1 CP prevé el descubrimiento en los mismos términos que el 197.1 CP, mientras que el 278.2 CP castiga la revelación del secreto.

El art. 197.1 del CP se refiere a dos modalidades de conducta: la del apoderamiento y la de interceptación de telecomunicaciones o utilización de artificios técnicos de escucha, transmisión… 1) Apoderamiento de "papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales". El apoderamiento es un aspecto fundamental de la conducta típica, y lo es hasta tal punto que —como destaca Muñoz Conde[13]—, si se llegan a conocer los secretos documentales de otro sin apoderarse de sus documentos o efectos personales, no podrá apreciarse este tipo del inciso Io del art. 197.1 del CP. El objeto material de la acción típica se amplía considerablemente en comparación con el precepto correlativo del CPA (art. 497.2ª), pues en este el objeto material se circunscribía a los "papeles o cartas" y ahora, en él primer inciso del art. 197.1 del CP, se amplía a los "mensajes de correo electrónico" —como, por ejemplo, las comunicaciones por telefax—[14] o a "cualesquiera otros documentos o efectos personales", haciendo uso el legislador de una cláusula general que permite comprender cualquier clase de documentos. Los "efectos personales" pueden entenderse como cualquier objeto de uso personal que permita identificar al titular de la intimidad.[15]

2) La interceptación de las telecomunicaciones de otro o la utilización de "artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación".

La interceptación de las telecomunicaciones se refiere a la conducta —llevada a cabo por un tercero— de introducirse en la conversación ajena con la finalidad de descubrir los secretos de otro o de vulnerar su intimidad,[16] y comprende tanto las conversaciones telefónicas convencionales o por cable como las que tienen lugar por telefonía móvil, siendo indiferente el sistema que utilicen los interlocutores.[17]

El art. 279 CP se refiere a la difusión, revelación o cesión del secreto llevada a cabo por quien tuviere obligación legal o contractual de reservarlo.

2. Daños informáticos

Se regulan diferentes tipos cuyo bien jurídico protegido es el patrimonio de la víctima. En la reforma de 2015, el legislador optó por crear un tipo específico donde se encuadran los daños informáticos. Así, el art. 264 CP tipifica la conducta consistente en borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas o documentos ajenos, sin autorización y de manera grave. El art. 264 bis CP hace alusión a la obstaculización o interrupción del funcionamiento de un sistema informático (por ejemplo, ataques DOS). El art. 264 ter CP hace referencia a la producción, adquisición o facilitación de programas (por ejemplo, un *exploit*) o contraseñas destinadas a cometer alguno de los delitos anteriores (art. 400 CP).

3. Falsedades informáticas

Aquí tienen cabida todos los tipos de falsedades comunes que utilicen algún artificio informático para llevarse a cabo. Se consideran: la falsificación de moneda y timbre (art. 386 a 389 CP); la de documento público, oficial y mercantil (art. 390 a 394 CP); de documento privado (art. 395 a 396 CP); de certificado (art. 397 a 399 CP); de tarjetas de crédito, débito o cheques de viaje (art. 399 bis CP). También se consideran delito de falsificación la fabricación, recepción, obtención o tenencia de instrumentos, datos o

https://cibercrim.com/ciberdelincuencia-en-el-codigo-penal/.

[13] MUÑOZ CONDE, F. Derecho *Penal*, P.E., 13a ed., 2001, p. 245.

[14] MORALES PRATS, W. AA., Comentarios a la PE del Derecho Penal, cit., p. 33

[15] QUERALT JIMÉNEZ, Derecho Penal, P.E., p. 194.

[16] LOZANO MIRALLES, VV.AA., Compendio, P.E., II, p. 212, y SEGRELLES DE ARENAZA, VV.AA., Compendio, P.E., p. 278.

[17] GONZÁLEZ GUITIÁN, Protección penal de la intimidad y escuchas telefónicas, VV.AA., Comentarios a la legislación penal, VII, dir., M. COBO y coord. M. BAJO, 1986

programas informáticos destinados a la comisión de los tipos indicados.

4. Estafa informática

   La estafa informática o ciberfraude se ha dibujado como el delito estrella tal y como ofrecen los datos del Portal Estadístico de Criminalidad, donde constan los delitos conocidos por el Ministerio del Interior, que son las denuncias presentadas ante los cuerpos de policía que operan en territorio nacional.

   En términos generales, el derecho penal y el derecho procesal penal clásicos fueron construidos sobre la base de un modelo de criminalidad física, marginal e individual. No obstante, Internet ha supuesto una revolución tecnológica, pero al mismo tiempo un problema para la represión de los delitos, puesto que existe una especial dificultad para la detección y persecución de los delitos informáticos, entre otros motivos, por el anonimato, la insuficiente conciencia de los usuarios para mantener unas medidas preventivas de seguridad o incluso el carácter transnacional de determinadas conductas delictivas.[18]

   El Código Penal contempla como estafa la utilización del engaño, con ánimo de lucro, para obtener un beneficio o perjuicio sobre un tercero (art. 248 a 251 CP).

   Además, en el art. 248.2 CP se recoge de forma expresa como estafa informática: valerse de manipulaciones informáticas o artificio semejante (por ejemplo, el *phishing*) para la obtención no consentida de una transferencia patrimonial en perjuicio de un tercero; fabricar, poseer o facilitar programas informáticos (por ejemplo, un *ransomware*) con tal fin; realizar operaciones con tarjetas bancarias o cheques viaje en perjuicio de su titular o de un tercero.

5. Defraudación de telecomunicaciones

   Se regula la defraudación del fluido eléctrico o el agua, las telecomunicaciones (Internet, teléfono, TV de pago) valiéndose de mecanismos destinados a tal efecto, alterando maliciosamente las indicaciones y/o contadores o por cualquier otro medio (art. 255 CP).

   El art. 256 CP prevé la utilización de un terminal de telecomunicaciones sin permiso de su titular y causándole un perjuicio económico.

6. Ciberdelitos sexuales

   Comprende todos los tipos tradicionales de abuso sexual contemplados en el art. 181 y siguientes del Código Penal. Además, de forma específica debe destacarse el art. 183 ter CP, conocido como *child grooming*, que contempla como punible la utilización de las TIC para contactar con un menor de 16 años y embaucarlo para concertar un encuentro con el fin de llevar a cabo actos previstos en los art. 183 a 189 CP (183 ter 1 CP) o para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor (183 ter 2 CP).

   El acoso sexual (art. 184 CP) llevado a cabo a través de las TIC también debe atribuirse a la categoría de ciberdelitos sexuales. De igual forma, cabe considerar el exhibicionismo obsceno (art. 185 CP) ante menores de edad o discapacitados necesitados de especial protección, la venta o difusión de material pornográfico a estos (art. 186 CP) y los delitos relativos a la prostitución, explotación sexual y corrupción de menores (art. 187 a 189 bis CP).

7. Delitos contra la propiedad intelectual

   Contempla la reproducción, plagio, distribución o comunicación pública de una obra con ánimo de lucro y sin autorización de los titulares de los derechos de propiedad intelectual (art. 270.1 CP) y la facilitación activa y con ánimo de lucro del acceso o localización en Internet, especialmente mediante listados (*links*) de obras protegidas sin autorización de los titulares de los derechos de propiedad intelectual (art. 270.2 CP).

   También se subsume en este tipo: la acción de eliminar, modificar las medidas tecnológicas destinadas a proteger obras para favorecer la comisión de alguna de las conductas de los tipos comentados (art. 270.5 apartado C); la elusión o facilitación de estas medidas tecnológicas (por ejemplo, mediante un crack) para facilitar a un tercero el acceso a una obra protegida (art. 270.5 apartado D) y la fabricación, importación, distribución o posesión con fines comerciales de cualquier medio destinado a

[18] Fernández Teruelo, J.G. Revista de Derecho Penal y Criminología, 2ª Época, n.19 (2007), págs. 217-243.

neutralizar dispositivos técnicos utilizados para proteger programas informáticos u obras protegidas (art. 270.6 CP).

8. Delitos contra el honor
   El honor es el bien jurídico protegido que puede verse lesionado mediante calumnias e injurias. La calumnia, prevista en el art. 205 CP, consiste en la imputación de un delito con conocimiento de su falsedad. La injuria, tipificada en el art. 208 CP, es la acción expresión destinada a mermar la dignidad personal (por ejemplo, mediante insultos). Se regula concretamente el hecho de la publicidad, que suele concurrir cuando se difunden los mensajes a través de, por ejemplo, redes sociales o grupos de mensajería (art. 211 CP).
9. Amenazas y coacciones
   Las amenazas y coacciones constituyen el segundo grupo de ciberdelitos más denunciados, solo superados por el ciberfraude. En el caso de las amenazas (art. 169 a 171 CP) las conductas en el entorno virtual no distan de las del físico, si bien cabe destacar como habitual el chantaje que se produce cuando, por ejemplo, el autor obtiene una imagen comprometida de la víctima y amenaza con difundirla si esta no le recompensa con alguna cantidad económica o similar (art. 271.2 CP).

   En cuanto a las coacciones (art. 172 a 172 ter CP), sucede como con las amenazas y las conductas llevadas a cabo a través de las TIC: se asemejan a las del mundo físico. No obstante, destaca el conocido como ciberacoso o *ciberstalking* (art. 172 ter CP), consistente en el establecimiento de contacto de forma reiterada e insistente por parte del autor respecto de la víctima, alterando gravemente el desarrollo de su vida cotidiana.
10. Odio y apología del terrorismo
    El uso masivo de redes sociales y aplicaciones de mensajería ha propiciado el incremento de conductas como el del delito de odio y la apología del terrorismo. En relación al odio, se trata de una conducta que atenta contra derechos fundamentales y libertades básicas y castiga a quienes directa o indirectamente y de manera pública fomenten, promuevan, inciten al odio, hostilidad, discriminación o violencia por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad (art. 510 CP).

    Se les castiga porque su mensaje puede dar lugar a la aparición en quien lo reciben de unas ideas (las del odio) que se consideran tan peligrosas y se valoran tan negativamente que se trata de impedir que puedan propagarse mediante la amenaza de sanción penal a aquel que las puede difundir mediante su publicación o transmisión.[19]

    Respecto a la apología del terrorismo (art. 578 CP), se refiere al enaltecimiento o justificación pública del terrorismo, de manera agravada cuando hubiere difusión a través de las TIC.

Hay dispersión por todo el Código Penal y resulta ser demasiado genérico, lo que ha llevado a que sean los tribunales los que vayan interpretando cada acción para después subsumirla en los tipos penales que tenga encaje

Después de la reforma del Código Penal en 2015 debemos destacar una serie de aspectos en relación con los ciberdelitos, significando que la reforma ha endurecido las penas por delitos contra la libertad sexual y la protección de menores.

La Directiva 2011/93/UE14 obliga a los estados miembros a endurecer las sanciones en este ámbito de menores, sancionando la producción, difusión o asistencia a espectáculos pornográficos en los que participen menores de edad, y se amplía la tipificación del *child grooming* (acciones emprendidas por adultos con el fin de abusar sexualmente de las víctimas), considerándose delito agravado la participación de menores de dieciséis años en este tipo de actos. Posteriormente, tras la reforma, se tipifica la revelación de secretos si se han conseguido imágenes con la aquiescencia de una persona, pero luego se divulgan contra su voluntad, lesionando gravemente la intimidad de la víctima. Finalmente se introdujo como delito la supresión o alteración de medidas de seguridad tecnológicas para proteger programas de software o

[19] Galán Muñoz A. "Delitos de odio. Discurso del odio y derecho penal ¿hacia la construcción de injustos penales por peligrosidad estructural?" Revista Penal nº 46. Tirant Lo Blanch. Julio 2020.

ejecución de estos sin autorización de los titulares de los derechos de propiedad intelectual.

Todo ello ha dado paso a una nueva regulación de los ciberdelitos, dando paso así a una mayor ciberseguridad.

No obstante, es importante hacer referencia al hecho de que existen vacíos legales como son la usurpación de identidad en Internet. Previsto en el art.401 del Código Penal, establece que "El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años". En el delito de usurpación de estado civil, el bien jurídico protegido es la fe pública, que se concreta en la confianza de la sociedad en una correcta identificación de las personas. Por lo tanto, la conducta que se sanciona en este tipo penal es la utilización de un falso nombre y la filiación a ese nombre de otra persona que existe realmente, independientemente de que esté viva o haya fallecido y no la mera utilización de un nombre ajeno.

Un delito relacionado con la usurpación de identidad en Internet es el ya referenciado *phishing* (estafa informática), que se considera una forma de suplantación consistente en el uso de un tipo de ingeniería social caracterizado por adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o bien información privada sobre tarjetas de crédito o cualquier otro tipo de información bancaria detallada.

Hay un proyecto muy curioso y necesario desarrollado conjuntamente por el Instituto Nacional de Ciberseguridad (INCIBE) y el Boletín Oficial del Estado (BOE), que publicaron en el año 2016 (y siguen actualizando a día de hoy), dando como resultado el primer Código de Derecho de la Ciberseguridad, donde han compilado todos aquellos artículos, disposiciones y leyes relacionadas con la ciberseguridad que hagan referencia o tengan que ver con las nuevas tecnologías. Esto no se limita solo a ciberdelitos, incluyendo desde la Constitución española la LO 3/2018 sobre Protección de Datos, Seguridad Nacional hasta las menos conocidas, como el Reglamento que establece condiciones de protección del dominio público radioeléctrico.

Respecto a la forma que tiene la ley de prever los delitos, a veces no tiene tan en cuenta la parte técnica del fenómeno. Así, con el delito de sabotaje informático o *cracking* del art. 264.1 del CP se tipifica: "El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años". En esto podemos plantearnos ¿cualquier medio incluye ataques físicos o solo informáticos? ¿Qué es de manera grave? Si los hace inaccesibles, pero tengo una copia de seguridad y ya son accesibles, ¿es delito? ¿Es grave? Este tipo de cuestiones que se generan deben de ser respondidas por los tribunales en su labor de aclaración-interpretación-aplicación de las leyes o jurisprudencia en el caso concreto.

6. Los instrumentos de persecución de los delitos realizados mediante la Dark Net

Debemos señalar que la Dark Net no es en sí misma ilegal, sino que lo que resulta ilegal es valernos de dicha red para la realización de determinadas actividades que sí son consideradas ilegales.

Los delitos actuales son cada vez más internacionales. Es esencial que haya coordinación entre todos los agentes para mantener la estructura de seguridad mundial.

Existen muchos compromisos de cooperación internacional en la lucha contra la ciberdelincuencia. España participa activamente en el Centro de Excelencia de Ciberdefensa Cooperativa (Cooperative Cyber Defence Centre of Excellence, CCD COE) que la OTAN estableció en Tallín, Estonia, tras firmar el 14 de mayo de 2008.

INTERPOL, como organización internacional de policía criminal y organización intergubernamental, aporta esta plataforma de cooperación, facilitando a la policía el trabajo directo con sus homólogos, incluso entre países que no mantienen relaciones diplomáticas.

INTERPOL conecta a todos los países miembros (195) a través de un sistema de comunicación denominado I-24/7. Los países utilizan este sistema protegido para ponerse en contacto entre sí y con la Secretaría General. También les permite acceder a las bases de datos y servicios en tiempo real, tanto desde localizaciones centrales como remotas, todo ello genera una plataforma internacional.

Asimismo, proporcionan voz a la policía en el ámbito internacional, trabajando con los gobiernos al

más alto nivel para alentar esta cooperación y el uso de los servicios.

Todas las acciones son políticamente neutrales y se ejecutan dentro de los límites de legislaciones existentes en los diferentes países.

En el marco de la UE, se creó el Centro Europeo de Cibercrimen (EC3), dependiente de Europol, que se ocupa de los delitos relacionados con ciberterrorismo desde enero de 2013, centrándose principalmente en delitos de fraude económico, los relacionados con ataques informáticos a empresas o infraestructuras críticas y explotación sexual infantil, así como a la recogida de información de inteligencia, de gran variedad de fuentes tanto públicas como privadas a fin de alimentar una base de datos policiales, que permita facilitar información a los países miembros.

En el ordenamiento español no existe específicamente una ley de cooperación judicial en materia de ciberdelincuencia. Tenemos una referencia en el artículo 276 de la Ley Orgánica del Poder Judicial, que establece que las peticiones de cooperación internacional se tramitarán de conformidad con lo previsto en los tratados internacionales, las normas de la Unión Europea y las leyes españolas que resulten de aplicación. Por tanto, hay que acudir a los convenios internacionales de los que España es parte, que en el ámbito europeo son:

- Convenio Europeo de Asistencia Judicial en Materia Penal, hecho en Estrasburgo el 20 de abril de 1959.[20]
- Convenio de aplicación del Acuerdo de Schengen de 19 junio de 1990.[21]
- Convenio Europeo relativo a la Asistencia Judicial en Materia Penal entre los Estados miembros de la Unión, hecho en Bruselas el 29 de mayo de 2001.[22] Fuera del ámbito europeo habrá que acudir a los convenios existentes o, en su defecto, a la reciprocidad (277 LOPJ).
- La Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la Orden Europea de Investigación en materia penal, porque sustituye, a partir del 22 de mayo de 2017, a las disposiciones correspondientes de convenios ya citados aplicables a las relaciones entre los Estados miembros vinculados por la presente Directiva.

7. Equipos y órganos de investigación en los delitos de Dark Net en España

7.1 Fiscales especializados en delincuencia informática

La Fiscalía General del Estado, en la instrucción 2/2011 del fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de la Fiscalía, establece una clasificación de delito intentando diferenciar los delitos informáticos en sentido estricto de aquellos otros delitos que la informática simplemente aparece de forma accidental. Se establece un catálogo inicial de delitos informáticos en los que intervendrán fiscales especializados pero sin limitar en sus *numerus clausus* los tipos penales susceptibles de encuadrarse en la categoría de criminal informática, pues según la propia instrucción es más previsible:

> … la aparición en un futuro más o menos próximo de nuevas formas de delincuencia nuevos mecanismos de comisión de ilícito y a tipificar de los que los elementos determinantes sean también la utilización de la tecnología de la información y la comunicación TICS de forma que su análisis y valoración demanda de conocimiento específico para aconsejable su especialización.

Entre las figuras dentro de la Fiscalía especializada se encuentra:

- Fiscal de sala coordinador para la criminalidad informática.
- Las secciones de criminalidad informática de la Fiscalía.

7.2 Fuerzas y cuerpos de seguridad del Estado

Existen cuerpos especializados en la lucha contra la cibercriminalidad, Policía Nacional Guardia civil, Mossos d´EScuadra, Ertzaina.

[20] Ratificado por España el 14 de julio de 1982, BOE núm. 223, de 17 de septiembre de 1982.

[21] Ratificado por España el 23 de julio de 1993, BOE núm. 81, de 5 de abril de 1994.

[22] Ratificado por España el 23 de julio de 1993, BOE núm. 81, de 5 de abril de 1994.

7.2.1 Unidad Especial Tecnológica del Cuerpo Nacional de Policía (UIT)

Tienen como misión fundamental la prevención y represión de los delitos tecnológicos como unidad central con competencia en todo el territorio nacional, así como en todo lo relativo a la colaboración internacional, formación y apoyo técnico a otras unidades. Esta unidad especializada está compuesta por la Brigada Central de Investigación Tecnológica y la Brigada Central de Seguridad Informática. También cuenta con el apoyo del cuerpo nacional de policía con unidades territoriales periféricas para la prevención y represión de los delitos tecnológicos en sus propios ámbitos policiales.

Y señalar a los equipos conjuntos de investigación penal en el ámbito de la Unión Europea en la que participa la policía y el Ministerio Fiscal, así como la ciberpatrulla con policías de otros países.

España, a través de la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía, es colíder en la subprioridad de ciberataques del proyecto en EMPACT de Europol.

7.2.2 Grupo de Delitos Telemáticos de la Guardia Civil (GDT)

El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos actos delictivos que se cometen a través de sistemas de telecomunicaciones y mediante las tecnologías de la información. En 1996, cuando las investigaciones sobre delitos informáticos empezaron a adquirir especial relevancia, se vio la necesidad de crear un grupo específicamente destinado a perseguir esta clase de delincuencia constituido por agentes que unieran a su preparación en investigación criminal una buena formación informática.

A mediados de 1999, dado que el campo de actuación se había ampliado a los fraudes en el sector de las telecomunicaciones, se adoptó una terminología más en consonancia con la realidad, pasando a llamarse Departamento de Delitos de Alta Tecnología (DDAT).

En 2000, se produce una mayor especialización de sus miembros, estructurándose en las áreas delictivas de pornografía infantil, fraude y estafa, propiedad intelectual y delito de hacking en consonancia con el convenio de ciberdelincuencia del Consejo de Europa en el que participa personal de la Guardia Civil como expertos policiales.

En el 2003 la unidad toma su actual nombre Grupo de Delitos Telemáticos (GDT) y se crean a nivel provincial los equipos de Investigación Tecnológica (EDITE).

Desde el año 2002, la Guardia Civil organiza anualmente un Foro Iberoamericano de Encuentro de Ciberpolicía, que se ha constituido en un referente de colaboración internacional entre unidades de lucha contra la delincuencia informática a nivel latinoamericano es en otro foro a opinión en otro foro a nivel europeo.

Los fines específicos son fundamentalmente los siguientes:

- Llevar a cabo investigaciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones, bien por propia iniciativa, a requerimiento de las Autoridades Judiciales, o por denuncia de los ciudadanos.
- Detección de delitos informáticos en la red patrulla cibernética (patrullas cibernéticas).
- Apoyo a las investigaciones del resto de las unidades de la Guardia Civil.

El Grupo de Delitos Telemáticos se integra en la Unidad Central Operativa de la Guardia Civil los equipos de Investigación Tecnológica (EDITE) se encuentran las unidades orgánicas de Policía Judicial de la Guardia Civil desplegados a nivel provincial.

Actualmente el GDT dispone de una estructura para luchar contra los hechos delictivos cometidos en la red que, consiste en diferenciar lo que serán unidades de seguridad ciudadana, como Policía Judicial genérica y encargado de prestar los servicios de atención al ciudadano de las unidades policiales Policía Judicial específica. La Policía Judicial genérica recibe la inmensa mayoría de las denuncias y son el primer contacto con el que cuentan las víctimas de ciberdelito; son las unidades de Policía Judicial sobre las que recae la responsabilidad de investigar aquellos hechos delictivos que puede ser de especial dificultad o por la propia sensibilidad del bien jurídico protegido que requieran una formación específica. Las unidades orgánicas de Policía Judicial cuentan con una sección de investigación que aborda los casos más graves.

Su estructura se conforma tratando de contar con una especialización delictiva en relación a los delitos tecnológicos relativos a la ciberdelincuencia. Y se investigan desde dos frentes distintos:

- Desde el ámbito de delitos relacionados con las personas donde se encuentran los EMUME (Equipo de Mujer/Menor), encargados de realizar las investigaciones relacionadas con la pornografía infantil y los delitos cometidos contra los menores (*grooming*, *cyberbullying*, etcétera). Pero, además de investigar ciberdelito, el objetivo último de esta actuación es lograr la identificación de los menores víctimas y en el caso de autores menores se busca también que sean investigados por personal especializado.
- Desde el ámbito de los delitos relacionados con el patrimonio donde se engloban los EDITE (Equipos de Investigación Tecnológica), responsables de hacer frente a toda delincuencia que se sirve para su comisión de los elementos tecnológicos a excepción de los relativos a menores y los que por dificultades técnicas necesitan de una preparación especializada. En esfera nacional también se encuentra el Grupo de Delitos Tecnológicos (GDT) de la Unidad Central Operativa (UCO), que desarrolla la investigación de este tipo de hechos cuando revista especial dificultad o complejidad o trascendencia y presta los apoyos técnicos operativos requeridos por las unidades territoriales.

7.3 Equipos Conjuntos de Investigación (JIP)

Estos equipos tienen un carácter transnacional, pero en España es un instrumento que prácticamente no se utiliza.

Esta figura fue creada por la Decisión Marco 2002/465/JAI del Consejo de 13 de junio de 2002 para que los Estados miembros pudieran constituir equipos conjuntos de investigación cuando se precisa una acción coordinada. Estos JIT (Join Investigation Team) tienen un objetivo preciso con una duración limitada. A fin de cumplir con dicha decisión marco y sin esperar su aprobación definitiva y en atención a la utilidad que los JIT podrían tener en la investigación frente a la lucha contra el terrorismo de ETA, España adelantó la regulación nacional y promulgó dos leyes:

- La ley 11 del 2003 de 21 de mayo reguladora de los equipos conjuntos de investigación penal en el ámbito de la Unión Europea, donde se define el equipo conjunto de investigación como el constituido por acuerdo de las autoridades competentes de dos o más Estados miembros de la Unión Europea para llevar a cabo investigaciones penales en el territorio de alguno de todos ellos que requieran una actuación coordinada con un fin determinado y por un período limitado.
- la Ley Orgánica 3 del 2003 de 21 de mayo complementaria de la ley reguladora de los equipos conjuntos de investigación penal en el ámbito de la Unión Europea anteriormente referenciada, por la que se establece el régimen de responsabilidad penal de los miembros destinados en dichos equipos cuando actúen en España.

En el ámbito de las Naciones Unidas, el artículo 19 del Convenio Contra la Delincuencia Organizada Transnacional adoptado en Nueva York el 15 de noviembre de 2000, conocido como Convenio de Palermo, prevé la investigación conjunta a través de acuerdos bilaterales o multilaterales entre los países que los suscriben o de acuerdos específicos en casos concretos

De igual forma, la Convención de Naciones Unidas Contra la Corrupción, adoptada en Nueva York el 31 de octubre del 2003, conocida como convenio de Mérida, recoge en su artículo 41 las investigaciones conjuntas como método de investigación de estos delitos.

También los convenios bilaterales suscritos por España suelen tener en cuenta esta técnica. En este sentido, citamos el artículo 16 ter del Acuerdo de asistencia judicial en materia penal entre la Unión Europea y los Estados Unidos, celebrado en Washington el 25 de junio de 2003, y el protocolo adicional 12 de julio de 2005 al Convenio de Cooperación Colombia de 20 de mayo de 1997.

Los JIT pueden ser bilaterales, constituidos por dos Estados, y multilaterales si son más de dos Estados. Por su naturaleza, pueden ser policiales, fiscales o judiciales, dependiendo del órgano que realice la investigación.

Cabe destacar que no requiere de una comisión rogatoria, por lo que se acelera la práctica de las diligen-

cias de investigación y es mucho más ágil y eficaz. La legislación que rige la práctica de esta diligencia es la del Estado en el que se han de practicar las diligencias. Así que para el caso de practicarse fuera del territorio español se deberá de pedir que se adopten las mismas condiciones que si fueran practicadas en el marco de una investigación española.

Para la constitución del equipo JIT se requiere autorización previa de la Autoridad Nacional, y el art. 3 de la Ley 11/2003 especifica que autoridad competente será atendiendo a una serie de circunstancias:

- La Audiencia Nacional será competente cuando la investigación recaiga sobre los delitos cuyo enjuiciamiento corresponda a dicho órgano jurisdiccional y participen en el equipo miembros de la carrera judicial o fiscal.
- El Ministerio de Justicia cuando la investigación recaiga sobre los delitos para cuyo enjuiciamiento no resulte competente la audiencia nacional y participen en el equipo miembros de la carrera judicial o fiscal.
- El Ministerio de Interior a través de la Secretaría de Estado de seguridad en todos los supuestos en que no participen miembros de la carrera judicial o fiscal.

En este escenario, se plantea si la previa necesaria autorización del Ministerio de Justicia por la constitución o ampliación de los JIT puede ser contraria al artículo 117 de la Constitución española, ya que supone una intromisión directa en la labor judicial la medida que otorga a la autoridad administrativa competencias importantes dentro del procedimiento penal.

7.4 Las empresas proveedoras de Internet (ISP)

La colaboración y ayuda de los proveedores de Internet *(Internet service provider)* es esencial en la investigación de los delitos cometidos utilizando las TIC al ser estos quienes disponen y pueden proporcionar los datos de cualquier interacción en el ciberespacio.

En la ISP hay que distinguir entre los proveedores de acceso y los proveedores de servicio. Los primeros son las compañías que proporcionan el acceso a Internet, que normalmente suelen ser operadores de telecomunicaciones, como es el caso de las empresas, por ejemplo: Movistar, Orange, Vodafone, Jazztel. Mientras que los segundos son aquellos que proporcionan ciertos servicios de uso común como el correo electrónico: Hotmail, Gmail, redes sociales como Facebook, Telegram, Twitter, almacenamiento de archivos como Dropbox Google Drive, publicación de vídeos y fotos como Youtube, Panoramio, Flickr o mensajería como Whatsapp, Line, Messenger, etcétera.

Para la obtención de la prueba es fundamental el papel de las empresas de telecomunicaciones y servidoras de Internet en su colaboración con la justicia.

Estas empresas han de tratar de compatibilizar el desarrollo de la libertad de expresión, de comercio, conocimiento y comunicaciones que potencia Internet a través de sus múltiples mecanismos y posibilidades con la exclusión del mayor número de contenidos ilícitos posibles.

Por ello, es necesario tener y recabar la cooperación de estos operadores de telecomunicaciones y los proveedores de servicios de Internet al tener la información necesaria sobre los abonados y subscriptores.

Estas empresas tienen todo detalle en los datos sobre el tráfico de comunicaciones, datos del día, la hora, la duración y la fecha de cualquier comunicación, así como los implicados y el tipo de servicio y actividad.

Los datos se conservan por lo general durante un periodo de tiempo limitado según las necesidades comerciales del operador o proveedor y de los requisitos legales y comerciales para la protección de la esfera privada.

Los ISP tienen la obligación de conservar estos datos asociados a la comunicación y su cesión siempre y cuando medie autorización judicial por medio de la Ley 25/2007 de conservación de datos y la Ley de Enjuiciamiento Criminal incurriendo en responsabilidad en caso de incumplimiento.

La LECrim impone el deber de colaboración a las ISP en estos supuestos:

a. En la conservación y cesión de datos en virtud del artículo 588 ter j LECrim, los sujetos pasivos destinatarios de la obligación de conservar los datos de la ley 25/ 2007 son los proveedores de servicios de Internet y operadores que prestan servicios de comunicaciones electrónicas disponibles al público o explota en redes públicas de comunicaciones.

   Y en este sentido los sujetos obligados son los determinados por el registro de operadores dependiente del Ministerio de Industria Energía y Turismo a través de la Comisión Nacional de

los Mercados y la Competencia, regulada en el artículo 7 de la Ley 9/2014 de 9 de mayo, General de Telecomunicaciones.

Así la LECrim amplía esto a los que conserven por propia iniciativa por motivos comerciales o de otra índole.

Además de las responsabilidades penales que pudieran derivarse del incumplimiento de la obligación de conservación y cesión de los datos a los agentes facultados, establece también una responsabilidad administrativa.

b. En la intervención de las comunicaciones, artículo 588 ter de LECrim, se establece como deber de colaboración y de secreto por parte de los operadores cuyo incumplimiento será constitutivo de un delito de desobediencia.

   El sujeto obligado se amplía con respecto a los destinatarios de la obligación de conservar los datos previstos en la Ley 25/ 2007. El artículo 588 ter de la LECrim obliga a la compañía de telecomunicaciones tradicional que suministra acceso a la red telefónica y a la compañía de videojuegos online o cualquier persona que facilite la comunicación.

   Es así como todos deberán favorecer a los agentes facultados la intervención de las comunicaciones entre aquellos usuarios que queden afectados por una orden judicial.

   El problema estriba en que dicha intervención sea técnicamente factible o que las compañías extranjeras que faciliten estos servicios se consideren vinculadas con la legislación española.[23]

c. La orden de conservación de datos del artículo 588 octies de la LECrim tiene por objeto los datos informáticos vinculados a investigaciones concretas por lo que ha de solicitarse en cada supuesto, aunque se estime necesaria la preservación de determinada información incluida en un sistema informático o de almacenamiento de datos.

   Se refuerza esto con el delito de desobediencia en caso de incumplimiento a cualquier persona física o jurídica, extendiéndose así no solo a los operadores de telecomunicaciones, sino a cualquier otro sujeto que almacene los datos o informaciones como pueden ser los propios particulares que puedan canalizar el tráfico de la red TOR o aquellos ordenadores hayan sido empleados por el acceso fraudulento a Internet cuyo examen puede necesitarse por los investigadores.

d. En el registro remoto, artículo 588 septies b de la LECrim, quedan obligados a colaborar para la práctica de la medida del acceso al sistema los prestadores de servicio y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro, incurriendo en desobediencia en caso contrario. Según la Ley 34/ del 2002 de servicios de la sociedad de la información y del comercio electrónico no son responsables los proveedores de los contenidos que transmitan o alojan o los que faciliten acceso si no participan en su elaboración o no tienen conocimiento de la ilegalidad de los mismos.

   Sin embargo, son responsables solo si conocen su ilicitud y no actúan rápidamente para retirarlos o imposibilitan el acceso a ellos, por lo que tienen obligación de denunciar los contenidos delictivos que detecte en sus servidores.

   En cualquier caso, las solicitudes de bloqueo de acceso y retirada de contenidos o sitios Web deberán ser requeridas con autorización judicial.

Mencionar también el reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46 del Reglamento General de Protección de Datos, que establece la obligación de las empresas que prestan servicios de la conocida como sociedad de la información[24] de comunicar a las autoridades nacionales cuando sufran un incidente relacionado con la seguridad de la información. Por lo que con este artículo acabará con las grandes compañías que no daban cuenta de estos incidentes para evitarse perjuicios en su reputación con el consiguiente perjuicio para los usuarios.

[23] BERMUDEZ GONZÁLEZ, J. *Deber de colaboración de particulares en la LECrim.* Ponencia presentada en el curso de formación de fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios jurídicos los días 27 al 28 de octubre de 2016.

[24] La sociedad de la información suele distinguir entre abonado a un servicio de telecomunicaciones y suscriptor a un servicio de Internet.

Resaltar que afortunadamente nuestro ordenamiento jurídico permite la imputación de delitos a persona jurídica por ciberdelincuencia y utilizando para ello también la Dark Net, por lo que es posible realizar cualquier diligencia procesal en el marco de una investigación cuando ha intervenido la empresa o ha sido utilizada para la comisión de alguno de estos delitos:

a. Delitos relacionados con ordenadores y ataques contra los sistemas de información, al amparo de la reforma por la Ley Orgánica 1/2015, que ha incorporado un nuevo artículo 197 quinquies al capítulo dedicado "al descubrimiento y revelación de secretos del Código Penal", con el objeto de regular la responsabilidad de una persona jurídica en los casos de los delitos relacionados con ordenadores y sistemas de información en particular los ataques contra los mismos.
b. Delitos relacionados con el abuso sexual de menores en línea y con la pornografía infantil. La nueva redacción del Código Penal recoge en el artículo 183 ter del Código Penal dos conductas delictivas en la lucha contra los abusos sexuales a menores en Internet:
   - El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de 16 años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento.
   - Este supuesto es el caso de delito de *grooming***,** que se define como el proceso por el cual una persona, de manera deliberada, se hace amigo de un niño o establece una relación o un control emocional sobre el menor, a través de medios informáticos, para tener contacto sexual en línea y/o un encuentro físico con ellos, con el objetivo de cometer abuso sexual.
   - La reforma llega en el mismo momento en que el Tribunal Supremo condena por *grooming* en la Sentencia 823/2015 de 24 de febrero:
   - Un contacto por medio tecnológico con un menor de 16 años para su captación.
   - Por proponer un encuentro para cometer cualquiera de los delitos descritos en los arts. 183 a 189. La consumación se conseguirá cuando la cita propuesta por el delincuente fuese aceptada por el menor y se inician actos encaminados a que se ejercite la misma.
   - La realización de actos materiales encaminados al acercamiento, esto es actos que pretenden ganarse la confianza del menor y que deben repercutir y reflejarse más allá del mundo digital.
   - La voluntad de cometer cualquiera de los delitos de los arts. 183 y 189 que comprenden ataques a la indemnidad sexual de menores de 16 años.
   - El desconocimiento de la edad del menor no es suficiente para la exculpación, sino que ha de ser probado en base a alguna circunstancia excepcional.
   - El grooming se castigará, como tal, solo cuando no se haya llegado a materializar efectivamente la conducta sexual.
   - El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de 16 años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor.
   - Este segundo supuesto es una novedad en el Código Penal español, y se refiere a la explotación de imágenes relacionadas con pornografía infantil y la exposición a este tipo de material.
   - Los cuerpos y fuerzas de seguridad del Estado tienen dificultades para encontrar pruebas digitales porque los delincuentes usan técnicas de cifrado, redes de servidores y sofisticados métodos que les garantizan el anonimato y que se valgan de la Dark Net.
c. Delitos en que ordenadores o sistemas y tecnologías de la información fueron herramientas para delinquir u objeto principal del delito en particular el fraude en línea y con tarjetas de pago.

Los delincuentes utilizan varios métodos para capturar los datos, como el *skimming* (robo de datos en cajeros o máquinas expendedoras para la clonación de tarjetas) y el *phishing*. A menudo las personas solo se dan cuenta de la sustracción de los datos de su tarjeta cuando ya es demasiado tarde. Estos datos pueden servir para fabricar tarjetas falsas o utilizarse posteriormente para cometer fraudes sin presencia física de tarjeta.

Los estafadores utilizan la información para adquirir bienes en nombre de las víctimas o para obtener fondos no autorizados de sus cuentas.

Los datos de estas tarjetas también pueden ponerse a la venta en mercados de la red oscura, Dark Net. En muchos casos los datos robados en un país se utilizan en otros lugares, dificultando su rastreo, por lo que es fundamental la cooperación internacional.

d. Para los delitos de daños informáticos referidos a las rúbricas "interferencia ilegal en los datos", "interferencia ilegal en los sistemas de información" e "instrumentos utilizados para cometer la infracción tipificado en los artículos 264 del C. P., 264 bis del C.P y 264 ter del C. P.".

   La modalidad básica del artículo 264.1 castiga con una pena de prisión de seis meses a tres años al que por cualquier medio o procedimiento y sin estar autorizado de manera grave borre, deteriore, altere, suprima o haga inaccesibles los datos informáticos, los programas informáticos o cualquier documento electrónico ajeno y provoque un resultado grave en los mismos.

   El legislador, por tanto, abarca todas las posibles conductas susceptibles de afectar a los elementos informáticos, tanto las que implican su destrucción (total o parcial) como alteración (sea esta por eliminación, supresión o borrado parcial del elemento o por la incorporación de datos nuevos que supongan la modificación de su alcance o contenido inicial).

   Asimismo, hacer inaccesibles los datos, programas informáticos o documentos electrónicos implica que, sin afectar a su existencia o esencia, acceder a los mismos se hace imposible, sea para conocer su contenido u operar con ellos de cualquier forma.

   Por poner un ejemplo, piénsese en el programa malicioso conocido como *ransomware*, el cual actúa restringiendo el acceso a partes o archivos del sistema a través, por norma, de su cifrado.

   La acción típica merece mayor reproche penal a juicio del legislador cuando se emplee alguna de las herramientas que recoge el artículo 264 ter del Código Penal: programas informáticos concebidos o adaptados para cometer los delitos o contraseñas, códigos de acceso o similares que posibiliten acceder a todo o parte del sistema de información. El caso paradigmático es el de los denominados programas informáticos maliciosos o malware.

e. Los llamados delitos de odio. La definición de "delitos de odio" (*hate crime)* que usan los distintos Estados que recogen esta figura en sus legislaciones coincide en identificar estos como actos criminales que se cometen basándose en un prejuicio, y consta de dos elementos:
   - Que el acto constituya una infracción penal.
   - Que sea producto de un prejuicio del autor hacia la víctima por pertenecer a un colectivo vulnerable al odio. La víctima (o el objetivo) se elige intencionadamente por el autor por su pertenencia (real o presunta) a un colectivo que consideramos desde este punto de vista especialmente protegido. Por tanto, los elementos distintivos de estos delitos en relación con otros son: que la víctima (o víctimas) tiene una condición simbólica al no ser atacada por ser ella sino por lo que representa, y podría ser ella o cualquier otra que tenga sus mismas características (o aparente tenerlas). La intencionalidad de este tipo de violencia es no solo atacar a la víctima, sino transmitir un mensaje de rechazo, hostilidad e intimidación a todo el colectivo al que pertenece. La participación en este tipo de crímenes suele ser múltiple, no se trata de un hecho aislado.

     Se les castiga porque su mensaje puede dar lugar a la aparición en quien lo reciben de unas ideas (las del odio) que se consideran tan peligrosas y se valoran tan negativamente que se trata de impedir que puedan propagarse mediante la amenaza de sanción

penal a aquel que las puede difundir mediante su publicación o transmisión.[25] Señalar que en nuestro Código Penal no existe una regulación estructurada de los "Delitos de Odio" a través de ningún título o capítulo y que tampoco existe una mención definitoria de "delitos de odio".

La definición del delito de odio afín a las ya existentes es la que se recoge en la Recomendación General Nº 15 de la Comisión Europea contra el Racismo y la Intolerancia (ECRI):

> … el discurso de odio […] debe entenderse como el uso de una o más formas de expresión especificas —por ejemplo, la defensa, promoción o instigación al odio, la humillación o el menosprecio de una persona o grupo de personas, así como el acoso, descrédito, difusión de estereotipos negativos o estigmatización o amenaza con respecto a dicha persona o grupo de personas y la justificación de esas manifestaciones— basada en una lista no exhaustiva de características personales o estados que incluyen la raza, color, idioma, religión o creencias, nacionalidad u origen nacional o étnico al igual que la ascendencia, edad, discapacidad, sexo, género, identidad de género y orientación sexual.

Partiendo de esa conceptualización, el artículo 510 CP castiga con una pena de prisión de 1 a 4 años y multa de 6 a 12 meses a quien realice públicamente el fomento, promoción o incitación directa o indirectamente al odio, hostilidad, discriminación o violencia contra las personas por motivos racistas, antisemitas, por la ideología, religión o creencias, situación familiar, pertenencia a una etnia, raza o nación, su origen nacional, sexo, orientación o identidad sexual y razones de género, enfermedad o discapacidad.

También castiga con la misma pena a quien produzca, elabore, posea con la finalidad de distribuir, facilite a terceros el acceso, distribuyan, difundan, que como en el resto de los delitos que se han mencionado en este artículo el problema de su persecución y sanción estriba en multitud de problemas de prueba y en la identidad de la autoría, máxime valiéndose de la plataforma de la Dark Net, que protege como sabemos el anonimato del infractor-ciberdelincuente, por lo que algunas conductas a pesar de los medios e instrumentos tecnológicos de los que disponemos, desgraciadamente quedan impunes.

[25] Galán Muñoz A. "Delitos de odio. Discurso del odio y derecho penal ¿hacia la construcción de injustos penales por peligrosidad estructural?" Revista Penal nº 46. Tirant Lo Blanch. 2020.

ISSN 2007-4700

Universidad de Huelva
Universidad de Salamanca
Universidad Pablo de Olavide
Universidad de Castilla-La Mancha
Cátedra de Derechos Humanos Manuel de Lardizábal

·INACIPE·
INSTITUTO NACIONAL DE CIENCIAS PENALES