• enero • junio • 2026
• ISSN 2007-4700 • e-ISSN 3061-7324
• TERCERA ÉPOCA •

Revista Penal México

28

INSTITUTO NACIONAL DE CIENCIAS PENALES

INACIPE
INSTITUTO NACIONAL DE CIENCIAS PENALES

INACIPE 50 ANIVERSARIO 1976 • 2026

Revista Penal México 28
• enero • junio 2026 •
e-ISSN: 3061-7324

5

Problemática en la persecución en la red de los delitos en la *darknet*

Challenges in the Online Investigation of Crimes on the Darknet

• **Susana María Barón Quintero** •

Abogada de Ilustre Colegio de Abogados de Huelva
Doctoranda de la Universidad de Huelva
susana.baronquintero@gmail.com

Problemática en la persecución en la red de los delitos en la *darknet*

Challenges in the Online Investigation of Crimes on the Darknet

• Susana María Barón Quintero • Universidad de Huelva •

Fecha de recepción
15-09-2024

Fecha de aceptación
26-10-2025

Resumen

La dificultad de perseguir y sancionar los delitos realizados mediante la *darknet* radica en la compleja estructura de internet que, al ser mundial, sin control fronterizo ni de las comunicaciones, dificulta la identificación de los ciberdelincuentes, quienes se benefician de las lagunas legales existentes. Esto apunta a la obligación de revisar las legislaciones nacionales e internacionales para establecer un sistema de control de comunicaciones informáticas, con rastreo y supervisión de contenidos delictivos. Es necesario, además, reforzar tanto la cooperación policial y judicial europea e internacional como la capacitación y especialización de los operadores policiales y del ámbito jurídico y judicial, para disminuir el riesgo en la red.

Palabras clave

Darknet, *deep web*, TOR, cibercrimen, TIC, ciberseguridad, cooperación, Unión Europea.

Abstract

The difficulty in prosecuting and sanctioning crimes committed through the darknet lies in the complex structure of the Internet, which, due to its global nature and the absence of border controls or effective regulation of communications, hinders the identification of cybercriminals, who take advantage of existing legal loopholes. This situation highlights the need to review national and international legislation in order to establish a system for monitoring digital communications, including the tracking and supervision of criminal content. Furthermore, it is necessary to strengthen both European and international police and judicial cooperation, as well as the training and specialization of law enforcement officers and legal and judicial professionals, in order to reduce risks within the online environment.

Keywords

Darknet, deep web, TOR, cybercrime, ICT, cybersecurity, cooperation, European Union.

e-ISSN: 3061-7324

Sumario

1. Introducción. Análisis y estudio en la persecución de los delitos de internet profundo o internet invisible, internet oculto e internet oscuro (*deep web, invisible web, hidden web, darknet*)

Los delitos de la *deep web*, o también ya habitualmente llamados "delincuencia del futuro", son la criminalidad de la actualidad, la cual se vale de las nuevas tecnologías que tradicionalmente eran de uso de la inteligencia militar y los servicios secretos, pero que, actualmente, se utilizan para cometer delitos en el ámbito de la criminalidad organizada o por parte de cualquier delincuente que actúe de forma individual y aislada.

Estos delitos, perpetrados mediante la *deep web* y dentro de ésta la *darknet*, son realmente convencionales o tradicionales, aunque se canalizan y ejecutan mediante internet y las nuevas tecnologías. Como dice Espinosa Sánchez, los ciberdelitos son:

> […] aquellos actos ilícitos que, valiéndose de las ventajas surgidas de la revolución tecnológica, consiguen penetrar en las defensas de los sistemas informáticos, provocando la vulneración de éstos, y dando lugar a una pluralidad de delitos que pueden variar en su esencia delictiva.[1]

O, como dice Urbano Castrillo, el ciberdelito es un:

> […] tipo de delito, tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta. El convenio de Budapest ofrece un concepto basado tanto en la utilización de determinadas técnicas y modos de proceder informáticos […] como en ciertos contenidos cuya vulneración se ve facilitada por el medio Internet.[2]

La *darknet* es una parte de internet ubicada en la *deep web*, sin visibilidad, oculta estratégicamente para encubrir la identidad del ciberusuario en el propio tráfico, ya que

1 Jesús Francisco Espinosa Sánchez, "Ciberdelincuencia. Aproximación criminológica de los delitos en la red", *La Razón Histórica*, núm. 44, septiembre-diciembre, 2019, p. 155.

2 Eduardo de Urbano Castrillo, "Los delitos informáticos tras la reforma del cp de 2010", *Revista Aranzadi Doctrinal*, núm. 6, octubre, 2011, p. 18.

no la registran los distintos motores de búsqueda. En la *darknet* o *darkweb* encontramos material, información y páginas no indexadas en buscadores habituales como Google, Bing y Yahoo!, y por lo tanto, no accesibles mediante los navegadores web usuales y tradicionales.

La *darknet* es la esfera oculta de internet, donde sucede una pluralidad de hechos delictivos gravosos, como la contratación de sicarios, compraventa de pasaportes y cuentas bancarias, secuestros virtuales, pornografía infantil, tráfico de drogas y armas, estafas virtuales, blanqueo de dinero e, incluso, intercambio de información política *top secret* de países importantes en el panorama mundial.

Para combatir los ataques criminales realizados mediante internet, lo primero que se debe hacer es acceder a los medios y formas de comisión, con el fin de adoptar las diferentes respuestas legales para proteger, en cualquier caso, los derechos fundamentales que pudieran verse comprometidos.

El delincuente en solitario, con el uso de las tecnologías, consigue preservar su identidad, ya que actúa bajo la protección y garantía del anonimato, por lo que su conducta merece un mayor reproche penal. Esto mismo también sucede con las organizaciones criminales dotadas de estructuras complejas, jerárquicas, por lo que la acción dañosa, en muchos casos, queda impune a causa de la enorme dificultad de identificar al autor, lo cual se agrava, aun si cabe, con los problemas de localización y las competencias jurisdiccionales internacionales.

De esta forma, también prolifera una nueva configuración de crimen organizado que hace de la actividad ilícita un negocio por medio de internet y de las Tecnologías de la Información y la Comunicación (TIC), "al servicio de toda la humanidad internacional y en contra de ella".

Como mantiene el profesor Miró Llinares, respecto del cibercrimen y de la delincuencia en internet:

> [...] hoy en día se caracterizan por encontrarse completamente determinados por el uso de Internet y las tics. Esto se traduce en que ya no se utilizan exclusivamente los medios electrónicos para delinquir, sino que además Internet se convierte en una oportunidad para la comisión de infracciones tradicionales, de forma que los ciberdelitos quedan determinados por los medios electrónicos y por Internet.[3]

2. Dificultades probatorias. La prueba. Prueba pericial informática. Admisibilidad y legalidad

La detección y la práctica de las diligencias de investigación probatorias y la práctica procesal que se necesita recabar para la persecución de este tipo de delitos que navegan y proliferan en la red oscura, generan multitud de problemas que afectan y pueden atentar contra los derechos fundamentales amparados en la Constitución Española (CE).

En concreto, el artículo 18 de la CE, sobre entrada, registro, ocupación, intervención de comunicaciones, etcétera, junto con la legislación sobre protección de información y datos, dificultan enormemente la obtención de prueba plena, legítima, legalmente constituida, válida y suficiente que permita desvirtuar el principio de presunción de inocencia y nos ofrezca elementos de culpabilidad.

3 Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid: Marcial Pons, 2013, pp. 37-38.

A todo ello hay que sumar los problemas que, en el contexto y desarrollo de la investigación penal, generan los prácticamente casi nulos vestigios del ciberdelincuente, además de la eliminación de las pruebas o su difícil custodia y complejo cotejo.

La Ley de Enjuiciamiento Criminal (LECrim) prevé expresamente los requisitos, procedimiento y garantías para recabar pruebas tecnológicas que puedan utilizarse en el proceso penal, sin posibilidad de que se invaliden o impugnen.

Los actuales medios de investigación que tenemos en nuestra legislación y en el sistema judicial y policial para perseguir la ciberdelincuencia, en muchas ocasiones, no constituyen "prueba de cargo", por lo que el modo de su adquisición determinará que la prueba sea lícita, legal y válidamente constituida para poder encausar al acusado y someterlo a un proceso penal justo con todas las garantías.

En consecuencia, en el Estado social y democrático de derecho, para recabar la prueba lícita con éxito y frente al delincuente, al que se le reprocha penalmente por su conducta infractora, se deberá proceder del modo que prevean los mecanismos legales existentes, de la forma menos invasiva y con respeto y mínima o nula afectación a los derechos fundamentales.

Es así como la prueba que realmente va a determinar la existencia o no de la actividad delictiva es:

> […] la prueba pericial informática con sus singularidades sobre la cadena de custodia, el volcado, clonado, y análisis de datos, entre otras, que unida a otras pruebas tecnológicas como rastreos, señales de ip, agente encubierto en internet, balizas, colocación de gps, la intervención de las líneas de internet adsl o la introducción de virus troyanos espías para la investigación criminal […] nos aportará el propio escenario criminal.[4]

Como afirma Josefina Quevedo González:

> Las pruebas informáticas están sometidas, en este sentido, a un doble juicio, a unos requisitos de admisibilidad.
>
> Tales requisitos consisten de una parte, en un previo juicio de licitud (es decir, que la prueba se haya obtenido sin violar derechos fundamentales pues, en otro caso, sería nula, ex art. 11.1 LOPJ), y de otra, en un juicio de fiabilidad, que consiste en examinar la autenticidad (no manipulación) y la integridad (conservación del contenido) del material aportado, la intangibilidad e inalterabilidad del mismo, y la ausencia de técnicas espurias en la obtención de la información recabada en el curso de tal medio de investigación, pues las dudas sobre la fiabilidad determinarán su inadmisibilidad probatoria.
>
> De conformidad con el art. 230.2 LOPJ, resulta necesario asegurar la autenticidad (garantizar la fuente de la que proceden los datos) y la integridad (que el activo de información no ha sido alterado de manera no autorizada) de la prueba informática incorporada al proceso, de tal manera que quede garantizado que la sometida al tribunal de enjuiciamiento es la misma que la que fue incautada o aprehendida.
>
> El juicio de fiabilidad determina, una serie de singularidades cuando se aplica a las pruebas informáticas.[5]

4 Eloy Velasco Núñez, *Delitos cometidos a través de Internet: cuestiones procesales*, Madrid: La Ley, 2011.

5 Josefina Quevedo González, *Investigación y prueba del ciberdelito* (tesis doctoral), Barcelona: Universidad de Barcelona, 2017.

En síntesis, en la legislación española contamos con un sistema de instrumentos y herramientas jurídicas en aras de conseguir las pruebas necesarias para luchar contra la ciberdelincuencia y, además de otros elementos probatorios, fundamentalmente la prueba informática es la determinante. Sin embargo, como ocurre con el resto de las pruebas, se imponen y exigen límites en cuanto a los procesos y el modo de obtención, preservación y utilización, que deben respetar los derechos fundamentales que pudieran verse afectados. Todo ello opera como una condición necesaria y de obligado cumplimiento.

2.1 Técnicas de investigación de la delincuencia digital

Encontramos la regulación de las técnicas de investigación de la delincuencia digital en la LECrim, en virtud de la reforma efectuada mediante la Ley Orgánica 13/2015 de 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta refuerza las garantías procesales en el marco de la protección de la sociedad democrática y ofrece solución a muchas de las cuestiones que plantea la investigación de los ciberdelitos, mediante una normativa específica de técnicas de investigación tecnológica, que se encuentran reguladas en el título VIII del libro II,[6] "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución".

Estas medidas de investigación que buscan adaptarse a la realidad cambiante del mundo digital se clasifican concretamente en las que puede practicar la policía por sí misma y no requieren autorización judicial y las que sí requieren de la autorización judicial. En realidad, son las mismas que se practicaban anteriormente; a pesar de que existe una regulación expresa en la LECrim, estaban amparadas en otras leyes y en la jurisprudencia.[7]

Plan Estratégico contra la Cibercriminalidad

El Plan Estratégico contra la Cibercriminalidad se creó con la finalidad de luchar de forma efectiva contra la delincuencia tecnológica y fue aprobado por el Comité Ejecutivo de Coordinación (CECO) del Ministerio del Interior el 18 de febrero de 2021. Se estructuró en cinco áreas: detección, prevención, protección, persecución y respuesta a las víctimas del delito.

La elaboración y configuración del plan dirigido por la Oficina de Coordinación de Ciberseguridad (OCC) contó con una pluralidad de autoridades, especialistas y expertos del ámbito de la fuerzas y cuerpos de seguridad del Estado, esto es, Policía Nacional y Guardia Civil, policías autonómicas, del ámbito judicial y operadores jurídicos, Consejo General del Poder Judicial, Fiscalía General del Estado, Consejo General de la Abogacía Española, organismos especializados como CCN-CERT e INCIBE-CERT, Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), representantes del ámbito de la universidad, bancario y organismos y entidades privadas.

6 Ley de Enjuiciamiento Criminal, *Gaceta de Madrid*, núm. 260, España, 17 de septiembre de 1882. https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

7 Cfr. Josefina Quevedo González, *op. cit.*

En el ámbito internacional se creó la figura de la infiltración policial tras la Convención de la onu en la lucha contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas, celebrada en Viena en diciembre de 1988 con la finalidad de mejorar y optimizar los mecanismos utilizados para combatir ese tipo de delincuencia e implementar otros más innovadores y modernos.

Hay diversas medidas de investigación policial en la legislación española, como, la figura de los agentes encubiertos, entrega vigilada, protección de testigos, explotación del arrepentimiento, acciones en altamar,[8] utilización de bienes aprehendidos, transmisión de datos interpoblaciones directos y oficiales de enlace y equipos conjuntos de investigación. Estas circunstancias, bajo el prisma de la seguridad nacional, suponen un gran desafío e implican que el Estado español precise de una especial inversión en recursos de carácter material y personal orientados a la prevención (refuerzo de las fronteras, vigilancia marítima, control portuario, etcétera).[9]

En concreto, la infiltración policial —que se usa como una técnica eficaz para la investigación de delitos como el narcotráfico o el terrorismo en general—, en la *darknet* lleva, en muchas ocasiones, a desvelar y desmantelar actividades delictivas propias de la delincuencia organizada.

La técnica de la infiltración policial es el instrumento utilizado por un miembro de la policía judicial que se adentra y opera en el propio mercado de la *darknet* adoptando la falsa identidad de un comprador o vendedor o de una organización criminal, lo que le permite ganarse la confianza de los ciberdelincuentes y desarrollar tareas principalmente de detección, represión y prevención del delito, además de reunir pruebas y comparecer en las actuaciones judiciales, tras identificar a sus integrantes y recabar información sobre la estructura, funcionamiento, *modus operandi*, ámbito de actuación, tipología delictiva, financiación, etcétera.

Todo ello se trató en la Convención de las Naciones Unidas Contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas del 20 de diciembre de 1988. La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de diciembre de 2000, la consideró como técnica especial con obligación de observancia y respeto de los principios fundamentales de cada ordenamiento jurídico interno.[10]

8 Ley Orgánica 4/2015, de protección de la seguridad ciudadana, *Boletín Oficial del Estado*, núm. 77, España, 30 de marzo de 2015, art. 36.16: se considerará infracción grave "el consumo o la tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas, aunque no estuvieran destinadas al tráfico, en lugares, vías, establecimientos públicos o transportes colectivos, así como el abandono de los instrumentos u otros efectos empleados para ello en los citados lugares".

9 Cfr. Fernando Pérez Álvarez y Laura Zúñiga Rodríguez, *Instrumentos jurídicos y operativos en la lucha contra el tráfico internacional de drogas*, Navarra: Thomson Reuters, 2015, p. 10.

10 Oficina de las Naciones Unidas contra la Droga y el Delito, *Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional y sus protocolos*. Nueva York: Naciones Unidas, 2004, art. 20. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

En el ámbito europeo, el artículo 14 del Convenio de Asistencia Judicial en Materia Penal, de 29 de mayo de 2000, hace referencia a estas técnicas y las denomina como "investigaciones encubiertas", que define como: "investigaciones de actividades delictivas por parte de agentes que actúen infiltrados o con una identidad falsa",[11] y también estipula que la investigación se debe llevar cabo aplicando la ley interna del Estado en cuyo ámbito territorial se desarrolle la investigación.[12]

La figura del agente encubierto en España se encuentra regulada en el artículo 282 bis de la lecrim y fue introducida por la Ley Orgánica 5/1999 del 13 de enero, que modificó la Ley de Enjuiciamiento Criminal, en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves.

El agente encubierto permite que las fuerzas y cuerpos de seguridad del Estado puedan actuar bajo una identidad falsa, como estrategia para poder adentrarse en el seno del ámbito de actuación criminal y revelar la identidad y responsabilidad de los investigados. Tiene un periodo de vigencia inicial de 6 meses, que puede ser prorrogado por autorización judicial, y toda la información y pruebas que obtenga el agente encubierto deberán ponerse disposición de la autoridad judicial a la mayor brevedad posible para que pueda valorarse en un proceso de investigación judicial.

2.2 Medios tecnológicos

La investigación criminal actual cuenta con un gran número de técnicas que benefician su proceso y la lucha contra la ciberdelincuencia y que, además, permiten adoptar medidas preventivas cautelares y restrictivas de derechos en el ámbito de internet, o cualquier tecnología de la información y comunicación, como "la retirada provisional de contenidos ilícitos, interrupción provisional de los servicios que ofrezcan dichos contenidos, bloqueo provisional de ambos cuando radiquen en el extranjero", al amparo del artículo 13 de la Ley de Enjuiciamiento Criminal (LECrim).[13]

11 Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, *Diario Oficial de la Unión Europea*, serie C, núm. 197/01, 12 de julio de 2000, art. 14.

12 En el Informe explicativo de este Convenio se establece que los agentes encubiertos "deberían tener una formación específica, y que puede recurrirse a ellos en particular para que se infiltren en una red delictiva con vistas a obtener información o a ayudar a identificar y detener a los miembros de esa red" (Informe explicativo del Convenio, de 29 de mayo de 2000, relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, *Diario Oficial de la Comunidad Europea*, serie C, núm. 379/7, 29 de diciembre de 2000, art. 14). Se reconoce que el artículo 14 del Convenio se ha redactado en términos generales para que los Estados gocen de "flexibilidad" en las investigaciones encubiertas y se señala que, en todo lo relativo a la preparación y supervisión de la investigación y a la seguridad de los agentes infiltrados, ha de haber una cooperación entre los Estados interesados. Por tanto, deja claro, finalmente, que se aplicará el Derecho nacional del Estado en el que se lleve a cabo la investigación.

13 Se modificó el artículo 13 de la LECrim cuando se le añadió un segundo párrafo mediante la

Las técnicas del raspado, recolección web, extracción de datos web y el análisis de la *darknet* se realizan con herramientas gratuitas que se encuentran en internet. Concretamente, la herramienta del raspado web carga las url que proporcionan los usuarios y, con ello, se extrae toda la información del sitio.

Hay que añadir también la inteligencia artificial IA, software de reconocimiento facial que permite identificar al presunto autor a través de imágenes o videos; el escaneo en 3D, mediante la captura de imágenes que permiten recrear la escena del crimen de forma virtual; el análisis de *big data*, con el que se puede recoger gran cantidad de imágenes e información de distintas fuentes (como redes sociales y bases de datos), y la de ciberseguridad, que se usa frecuentemente en el ámbito de los delitos digitales, como las estafas *online* y el *fishing*. Todas estas herramientas nos permiten conocer y obtener información y análisis específicos sobre patrones delictivos concretos, lo cual mejora la prevención de comisión de delitos.

La Brigada Central de Investigación Tecnológica (BCIT), que es el órgano de la Dirección General de la Policía encargado de la investigación y persecución de los ciberdelitos en el ámbito nacional y trasnacional, tiene como finalidad principal la obtención de pruebas. Los medios que utiliza principalmente la policía son el uso de anzuelos o anclas mediante la navegación por internet, de tal forma que colocan archivos con contenido atractivo e ilícito para los cibernautas, como pornografía infantil, o venta de drogas, que llevan indexado un archivo con la localización; tras su descarga, este permite rastrear la dirección IP del ordenador mediante la línea o cuenta de internet. Después de la localización del ciberdelincuente, con la preceptiva autorización judicial, la Brigada de Delitos Tecnológicos realiza la entrada y registro en la vivienda del usuario e incauta el ordenador, y todos los dispositivos utilizados donde se ubiquen los archivos con contenido delictivo.

Como ejemplo, destaca la operación internacional desarrollada para combatir la pornografía infantil en la *darknet*, en la cual se rastrearon los bitcoins y que condujo a la detención de 338 usuarios que accedían a la página web *Welcome To Video*,[14] en la que existía más de un cuarto de millón de videos con pornografía infantil.

También se puede mencionar el caso Playpen, en el que se desmanteló una red de pedofilia en la *darknet* con la detención de más de 200 personas en todo el mundo por distribución y posesión de abundante material pornográfico infantil. La red fue calificada por el FBI como "el servicio de pornografía infantil oculto más grande del mundo" ;[15] se

disposición final 1.1 de la Ley Orgánica 10/22 de 6 de septiembre, que contempla las medidas cautelares que se pueden adoptar en el curso de una investigación. Cfr. Ley Orgánica10/2022, España, 6 de septiembre de 2025.

14 Raúl Álvarez, "Así es como desmantelaron 'Welcome to Video', una de las webs de pornografía infantil más grandes del mundo en la Dark Web", *Xataka* [en línea], 17 de octubre, 2019. https://www.xataka.com/legislacion-y-derechos/asi-como-desmantelaron-welcome-to-video-webs-pornografia-infantil-grandes-mundo-dark-web

15 La Sexta, "Detenidas 870 personas en una operación mundial contra la pornografía infantil", en *La Sexta*, 5 de mayo, 2017. https://

creó en el año 2014 y cayó a finales de marzo del 2015.

En relación con el tráfico y la venta de drogas, el caso del portal Ruta de la Seda (*Silk Road*) fue un hito mundial y el primero de delincuencia realizada mediante la *darknet*; este se saldó en el año 2015 con una condena de cadena perpetua impuesta por la Corte Federal de Nueva York para su creador, Ross Ulbricht, por la venta de drogas, y productos ilícitos a través de éste, además de otros delitos como blanqueo de dinero e ilícitos informáticos. Su sentencia fue confirmada en 2017, por la desestimación del recurso de apelación.[16]

Finalmente, cabe reseñar la operación internacional Wall Street Market, que se realizó el año 2020 y en la que se detuvo a 179 personas, distribuidas en todo el mundo (Estados Unidos, Alemania, Países Bajos, Reino Unido, Austria y Suecia), al mismo tiempo que se incautaron alrededor de 500 kilogramos de droga, 64 armas de fuego y 6.5 millones de dólares tanto en efectivo como en criptomonedas.

Con dicha operación la policía demostró la capacidad de clausurar algunos servicios y tiendas ilegales dentro de la *deep web*, y localizar a los que dirigen y trabajan en dichas actividades. En la operación se decomisaron varios millones en efectivo, criptomonedas y otros activos, y esta acabó con el cierre de la página. Con más de un millón de usuarios, más de 5 000 proveedores y decenas de miles de artículos, el Wall Street Market era uno de los mayores mercados de productos ilegales, sobre todo, de venta de drogas.[17]

2.3 Uso de navegador de la darknet, *direcciones IP*

La *darknet* es la parte oscura de internet, además de oculta, como la *deep web*; utiliza navegadores como tor o i2p, que albergan un contenido no visible. La más conocida es tor, un explorador de internet, una red de anonimato que contiene su propia *darknet*. Las *darknet* se utilizan para delinquir preservando el anonimato.

Los navegadores que se usan para la *darknet* actualmente son: DuckDuckGo, cuyo motor de búsqueda es como Google; Torch, una combinación de Tor y motor de búsqueda, que es el más antiguo de la red Tor, y Ahmia, Haystak, Not Evil, Candle, Kilos, LibreY.

Hay que mencionar que en la *darknet* se utiliza normalmente el navegador gratuito tor, que elude los mecanismos de control de los ciberdelincuentes. El mecanismo empleado para proteger la información y los datos estriba en que usa nodos de salida y nodos intermedios. De esta forma, tor interpreta las url de la *darknet* compuestas por la combinación de 16 caracteres formados con letras y

www.lasexta.com/noticias/sociedad/detenidas-870-personas-operacion-mundial-pornografia-infantil_20170505590cd0c90cf22906e6b43143.html

16 Sandro Pozzi, "El fundador de Silk Road, condenado a cadena perpetua", *El País*, 29 de mayo de 2015. https://elpais.com/internacional/2015/05/29/actualidad/1432935074_571369.html

17 Cáñamo, "Clausuran uno de los mayores mercados de la deep web", *Cáñamo. La Revista de la cultura del cannabis*, 6 de junio de 2019. https://canamo.net/noticias/mundo/clausuran-uno-de-los-mayores-mercados-de-la-deep-web

dígitos, los cuales comienzan por 2 y finalizan en 7, con terminación en *onion*.

En España no está prohibido legalmente el uso de la red TOR ni el acceso a la *darknet*; lo que se castiga es la comisión delictiva que se realiza a través de este medio. Actualmente, con las herramientas de visibilidad que existen, se consigue detectar a las personas que están accediendo a TOR, por lo que hay que extremar precauciones para acceder a ella, ante la existencia de la peligrosidad de una eventual implicación en hechos delictivos y de la actividad de los *hackers*. Lo más atractivo para los cibernautas es el anonimato y el hecho de que pueden acceder y operar sin ser detectados y con una serie de ventajas:

- Libertad: con TOR, la navegación por internet no tiene censura. Actualmente, los gobiernos, en defensa de la privacidad y de la protección de los ciudadanos, ocultan datos privados, con lo que limitan la consulta en internet.
- Vigilancia: desde una red local doméstica, se accede a toda la información y actividad que se realiza *online*; por el contrario, esto no sucede con la red TOR.
- Bloqueo de rastreadores: normalmente, cuando hacemos búsquedas de un producto o servicio por internet mediante exploradores tradicionales, posteriormente aparece publicidad relacionada con nuestra navegación. Si se utiliza tor, los rastreadores de publicidad no pueden monitorear la búsqueda y enviar información alguna de productos y servicios.
- Seguridad: la red TOR funciona transmitiendo varias veces, mediante los distintos dispositivos de red, el paquete de información recibido y reenviado, en el cual se añaden varias capas de seguridad. El navegador TOR, un buscador de tipo Firefox, ofrece mayor anonimato en la red para poder entrar en la *darknet* a sitios web y contenidos mediante buscadores convencionales.

La conexión a través del navegador TOR se ejecuta mediante un gran número de nodos hasta llegar a la página web seleccionada; esto crea una red superpuesta a lo que sería la internet tradicional.

En definitiva, con la utilización de tor se obtienen muchas capas para ocultar la información que se intercambia (de ahí el nombre tor, *The Onion Router*), por lo que la privacidad se refuerza. Esto es distinto si se accede desde un ordenador a una página web tradicional, como sucede con Chrome, que va a revelar gran información y datos, como la dirección ip, la línea operadora, sistema operativo, el huso horario y mucha información importante para los efectos de identificación.

Cuando se utiliza TOR, la conexión se hace a través de un nodo que va a tener una IP distinta a la real, por lo que oculta la ubicación verdadera; así se navega anónimamente. Su uso es común en los países donde internet no es libre y tienen prohibido o restringido el acceso a determinados contenidos.

Hay que decir que el navegador TOR es legal, seguro y no supone ningún peligro para el equipo informático ni dispositivos tecnológicos, y se puede acceder a todo tipo de sitios web *onion*, incluso a los ilegales. Además, está disponible tanto para sistemas software como Windows, Linux o MacOS, como para dispositivos móviles Android. Es gratis, de código abierto y utilización sencilla; sólo se necesita descargar el programa de la página web de tor e instalarlo en el sistema elegido.

Tras ser conectado, comienza la navegación anónima a través de la red tor, que, como ya se explicó, oculta la dirección ip real y posibilita el acceso a sitios web *onion*, inac-

cesibles a través de buscadores como Google y de la url. Pero esas páginas web no son ilegales, puesto que lo realmente ilícito es una parte del contenido de la *deep web*: la *darknet*, donde existe material prohibido e ilegal, no exento de generar problemas desde el punto de vista penal.

2.4 Identidad virtual. Derecho y protección

La identidad virtual es la representación digital de cualquier individuo, empresa o entidad *online*, y engloba la información personal, empresarial, los intereses, actividades, opiniones, de forma individualizada y singular, en el ámbito virtual; es decir, la manera en que se manifiesta y se visualiza el mundo exterior en el mundo digital. Esta imagen digital y proyección puede afectar la reputación y relaciones en línea, por lo que es de suma importancia el modo en que se hace, si bien hay que indicar que la reputación digital es distinta a la propia identidad digital.

Un ejemplo de reputación digital es la plataforma LinkedIn, la red social profesional más grande del mundo, que permite a cada usuario describir su identidad digital a través de su perfil, donde consta su formación académica y profesional; también, conectar con otros usuarios, compartir contenidos, experiencias, oportunidades, ideas de negocio y ofrecer "recomendaciones" en la red de contactos, con base en el prestigio del titular de la identidad virtual.

Desde la pandemia, el 68 % de la población mundial, que equivale a 5 500 millones de personas, tiene acceso a internet y al mundo digital, y prácticamente casi todos los usuarios poseen una identidad digital con perfiles en redes sociales, blogs, sitios web, canales *online* y cuentas de correo electrónico.

La identidad en el mundo físico comprende, en el ámbito personal, la información relativa al nombre, edad, sexo, localidad, nacionalidad, estado civil, documento identificativo (Número de Identificación Fiscal o nif, Número de Identificación de Extranjero o nie, pasaporte), seguro social, datos biométricos, así como nivel académico, cultural, social, aficiones, deportes, ocupaciones, profesión, etcétera.

En el ámbito empresarial, la identidad está determinada por la razón o denominación social, marca comercial, forma social o tipo de empresa (sociedad limitada, sociedad anónima, sociedad laboral unipersonal, comunidad de bienes, etcétera); es decir, el documento identificativo de la empresa.

En la identidad digital normalmente se utilizan los mismos elementos de identificación que en el mundo físico, a los cuales se suman otros componentes, como correo electrónico, firma digital, nombre de usuario o contraseñas.

Para acreditar la identidad digital del titular real y garantizar la seguridad en los trámites telemáticos, se utilizan distintos mecanismos de identificación (que exigen credenciales del usuario), autentificación (verificación de las credenciales para acreditar que realmente se es quien se dice ser: PIN, SMS, reconocimiento facial, huella digital, firma electrónica) y autorización de las distintas acciones que pueden realizarse.

Existen sectores que exigen una mayor seguridad, como el privado bancario o la administración pública, salud, justicia, hacienda; estos implementan el uso de plataformas digitales para minimizar los riesgos de ataques en la red, sin perjuicio de que, paralelamente, se efectúen mecanismos de autocontrol de los propios usuarios internautas.

A la identidad digital, como deriva y está íntimamente relacionada con la propia iden-

tidad física, se le reconocen los derechos propios de esta, que son fundamentales y protegidos a nivel internacional, como el derecho a la dignidad de la persona, al honor, a la intimidad personal y a la propia imagen. Estos se regulan en la Declaración Universal de los Derechos Humanos (art. 12) y en el Convenio Europeo de Derechos Humanos (art. 8).

En el panorama español, los derechos mencionados se regulan en varios textos legales: en la Constitución Española (arts. 10, 18, 20.4 y 96), en la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y en la Ley Orgánica 3/2018 de protección de datos personales y garantía de los derechos digitales, adaptada al Reglamento General de Protección de Datos de la Unión Europea.

La Ley Orgánica 1/1982, de 5 de mayo, regula la protección civil y protege de la vulneración del derecho al honor, a la intimidad personal y familiar y a la propia imagen cuando existan intromisiones ilegítimas y actos de injerencias no consentidas por el propio titular del derecho, ante lo cual incluso estipula la posibilidad de obtener un resarcimiento del daño en forma de indemnización. Por tanto, el Estado tiene la obligación de proteger a la persona contra esos ataques que se deriven de la actuación de un tercero, de los poderes públicos o de cualquier agente, con imposición de consecuencias jurídicas.

Se reseña, como caso mediático e ilustrativo, la sentencia del 13 de mayo de 2014, "Google Spain y derecho al olvido", del Tribunal de Justicia de la Unión Europea y que dirimió una disputa de Google Spain contra la Agencia Española de Protección de Datos sobre el derecho al olvido.[18] En ella se impuso al buscador Google la eliminación de datos personales de una persona física, que habían sido indexados en los servidores de su empresa y que afectaban a su reputación pública *online*.

La sentencia determina que la responsabilidad, en definitiva, es del prestador de servicios de la sociedad de información, Google, que, al utilizar y distribuir los datos e información personal, debe cumplir con la ley de protección de datos, eliminando la información que pudiera afectar el honor, dignidad y buen nombre del titular de dichos contenidos.

Los conceptos básicos referidos a los datos vienen regulados en el artículo 2 de la Decisión Marco 2008/977/JHA y, en dicho sentido, se expresa el artículo 2, letras *b* y *d* de la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, que regula el tratamiento de datos personales e incluye tanto los identificables como los de contenido sensible, cuando se pone a disposición de los cibernautas la información publicada almacenada para indexarla, en lo que tiene responsabilidad el gestor de la información guardada y obtenida mediante motores de búsqueda.

Sin embargo, con la evolución de la tecnología, el concepto de *datos* ha evolucionado, por lo cual entró en vigor en 2018 la Directiva 2016/680 del Parlamento Europeo y del Consejo del 27 de abril de 2016, en la cual se definen como:

18 Cfr. Cecilia Álvarez, "Sentencia Google Spain y derecho al olvido", *Actualidad Jurídica Uría Menéndez*, pp. 110-118. https://es.scribd.com/document/444020931/Sentencia-Google-Spain-y-Derecho-Al-Olvido-Uria-Menendez

> [...] toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.[19]

El derecho al olvido (*right to be forgotten*) se recoge igualmente en el Reglamento General de Protección de Datos de la Unión Europea (rgpd) (*European General Data Protection Regulation*, GDPR), que se aplica tras su entrada en vigor el 25 de mayo de 2018.

La sentencia del Tribunal Constitucional 139/1995, del 26 de septiembre de 1995, se pronuncia precisamente sobre el derecho al honor, reputación e identidad *online* de las personas jurídicas y dice literalmente:

> Resulta evidente, pues, que, a través de los fines para los que cada persona jurídica privada ha sido creada, puede establecerse un ámbito de protección de su propia identidad y en dos sentidos distintos: tanto para proteger su identidad cuando desarrolla sus fines como para proteger las condiciones de ejercicio de su identidad, bajo las que recaería el derecho al honor. En tanto que ello es así, la persona jurídica también puede ver lesionado su derecho al honor a través de la divulgación de hechos concernientes a su entidad, cuando la difame o la haga desmerecer en la consideración ajena.[20]

3. Medios analógicos

Los medios analógicos empleados para luchar contra los delitos realizados mediante internet no son más que el producto del compromiso y voluntad de los Estados y gobiernos a nivel internacional para, por un lado, poder perseguir y castigar los delitos cometidos mediante esta vía y, por otro lado, reforzar la seguridad global en internet.

Para ello se han creado equipos contra la ciberdelincuencia y los ciberataques informáticos con mecanismos de actuación ágiles y directos en caso de situación de urgencia, concretamente el CERT (*Computer Emergency Response Team*). En España se cuenta con el Instituto Nacional de Tecnologías de la Comunicación (INTECO), INTECO-CERT, el Cuerpo Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y el CCN-CERT,[21] que es el equipo de respuesta a incidentes de seguridad de la información del Centro Criptológico Nacional (CCN),[22] nacido a finales del año 2006, como el CERT gubernamental y nacional. Sus funciones se establecen en la Ley 11/2002 reguladora del Centro Nacio-

19 Cfr. Directiva (UE) 2016/680, Parlamento Europeo y del Consejo de la Unión Europea, *Diario Oficial de la Unión Europea*, 27 de abril de 2016, art. 3. https://www.boe.es/doue/2016/119/L00089-00131.pdf

20 Cfr. Sentencia recaída al Recurso de Amparo 83/1994, Sala Primera del Tribunal Constitucional, ponente: presidente Álvaro Rodríguez, 14 de octubre de 1995. https://www.boe.es/diario_boe/txt.php?id=BOE-T-1995-22479

21 Cfr. CN-CERT, Centro Criptológico Nacional [en línea]. www.ccn-cert.cni.es

22 Cfr. *Idem*.

nal de Inteligencia (CNI); en el Real Decreto 421/2004 de regulación del CCN, y en el Real Decreto 3/2010, del 8 de enero, regulador del Esquema Nacional de Seguridad.

El CCN-CERT actúa en los ciberataques que se realicen sobre sistemas clasificados y de la administración y de empresas pertenecientes a ámbitos considerados estratégicos, que merecen un máximo de seguridad. De esta forma, el equipo CCN-CERT se presenta como el paradigma para favorecer y reforzar la ciberseguridad española, concretamente en las administraciones públicas y empresas estratégicas, al ser el centro de alerta y respuesta nacional ante toda forma de ataque o amenaza en el ciberespacio. Para ello dispone de mecanismos, herramientas y servicios como:

1. Soporte y coordinación para el tratamiento de vulnerabilidades y resolución de incidentes.
2. Investigación y divulgación de mejores prácticas (Guías CCN-STIC).
3. Formación al personal de la administración especialista en ciberseguridad.
4. Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas sobre los sistemas de información.

Los CERT (*Computer Emergency Response Team*) o CSIRT (*Computer Security and Incident Response Team*) son fundamentales para proteger la seguridad nacional y mundial y están destinados a garantizar que la gestión de sistemas de información se realiza de forma adecuada para resistir los ataques en sistemas interconectados, limitar el daño y asegurar la continuidad de los servicios críticos a pesar de ataques exitosos, accidentes o fallos, por lo que su finalidad es proteger, detectar y responder. El primer CERT nació en 1988 para combatir "el gusano Morris", que afectó a un 10 % de los sistemas de internet.

Existe una pluralidad de CSIRT en distintos ámbitos de competencia: académico, comercial, interno, información y comunicaciones, pequeña y mediana empresa (pyme), de soporte, infraestructuras críticas, militar, gubernamental, nacional. En España, el CERT gubernamental, CCN-CERT, apareció en 2004 por Real Decreto 421/2004,[23] junto con la creación del Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia.

En octubre de 2012, el Ministerio del Interior y el Ministerio de Industria, Energía y Turismo firmaron un convenio de colaboración para combatir la ciberdelincuencia y el ciberterrorismo y, al mismo tiempo, reforzar el CNPIC, las Fuerzas y Cuerpos de Seguridad del Estado y el INTECO.

Actualmente, aunque existen convenios y compromisos en dicho sentido, no se ha alcanzado la armonización legislativa internacional, puesto que ello requiere una actuación conjunta entre países, en lugar de aislada por cada nación en concreto.

En el Convenio sobre Cibercriminalidad de 2001 se hizo patente la necesidad de que los gobiernos nacionales e internacionales trabajen en conjunto para firmar acuerdos internacionales, con el fin de garantizar la efectividad e intervención de los cuerpos y fuerzas de seguridad de los Estados en su objetivo de mantener la seguridad de los ciudadanos y de las entidades públicas y privadas, y de sancionar y perseguir la ciberdelincuencia sin limitación fronteriza y en un marco normativo común.

23 Cfr. CCN-CERT, "El Papel de un CERT gubernamental", *Perspectiva de las AA.PP.*, núm. 14, septiembre de 2007, pp. 50-52.

El ciberespacio es un medio que, por sus propias características, es fácil de atacar para los ciberdelincuentes, de tal suerte que las propias comunicaciones y el uso de los sistemas tecnológicos se vuelven inseguros y peligrosos, por lo que deben adoptarse unas mínimas precauciones y medidas de seguridad para protegerse de las prácticas de dicha criminalidad del ciberespacio.

Por ello, como sostienen los profesores José Antonio Gómez Hernández y María Concepción Rayón Ballesteros, fue necesario crear una política penal común, que sirviera como modelo a todos los países que se adhirieran o ratificaran el Convenio, de forma que cada uno, con posterioridad, desarrollase una legislación propia, de carácter nacional, pero "manteniendo una política de cooperación internacional".[24]

Es digno de destacar que, a fin de otorgar seguridad y amparo en los sistemas de red, existen muchas y diversas soluciones para combatir la ciberdelincuencia, tanto domésticas como a nivel empresarial o institucional.

Los sistemas de seguridad perimetral tienen como finalidad proteger la accesibilidad, la integridad, el contenido, la propia seguridad en la transmisión y la confidencialidad de los sistemas de información y las infraestructuras lógicas de una red, a través de los medios que se detallan a continuación:

1. Sistemas *antimalware*: comúnmente denominados *antivirus*, son un tipo de software que detecta y elimina todo tipo de programas maliciosos registrados que pueden infectar y afectar el sistema informático e, incluso, las distintas amenazas no registradas, como los virus, los troyanos, *spyware*, *rasomware*, entre otras.
2. Sistemas de control de acceso: se basan en una tecnología de ingreso de personas o recursos digitales que utilizan distintos protocolos de seguridad con base en elementos de identificación concretos, para impedir o facilitar su entrada, como huellas dactilares, PIN, tarjetas, reconocimiento facial, etc.
3. Sistemas *firewall*: es el llamado coloquialmente *cortafuegos*. Es la primera barrera lógica de entrada y salida de una red con internet. Controla la seguridad del tráfico de red frente a amenazas externas y accesos no autorizados, monitorizando el tráfico y determinando el permitido, para bloquear, con base en medidas de seguridad definidas, los paquetes de datos que se ponderen necesarios.

a. LAN: *Local Area Network* (Zona de Área Local). Es una red ubicada en una pequeña zona geográfica; conecta un router con dispositivos cercanos o internos y con servidores para compartir y trasmitir datos e información.

b. WAN: *Wide Area Network* (Red de Área Extensa). Red que conecta redes locales (LAN) a mayor distancia, por cable, o de manera inalámbrica o remota.

c. DMZ: *Demilitarized Zone* (zona desmilitarizada). Permite separar los servidores de acceso público que están expuestos (emails, páginas web) del resto, por lo que se protegen las redes internas (LAN) y se controla e impide el acceso a estas.

24 Cfr. José Antonio Gómez Hernández y María Concepción Rayón Ballesteros, "Cibercrimen: particularidades en su investigación y enjuiciamiento", *Anuario Jurídico y Económico Escurialense*, núm. 47, marzo, 2014, p. 212. https://publicaciones.rcumariacristina.net/AJEE/article/view/189

d. Sistemas *antispam*: el filtrado *antispam* es un sistema de identificación y bloqueo de contenido indeseado y se aplica en todo tipo de comunicación e información en la que usuarios de un listado reciben, de forma masiva, mensajes, correos electrónicos o SMS sin haberlo solicitado; las comunicaciones se remiten mediante *spammers* (con robo de datos, virus informáticos…), con una finalidad publicitaria y pueden servir para llevar a cabo una suplantación de identidad o envío de *malware*.

e. Sistemas IDS (*Intrusion Detection System*) (sistemas de detección de intrusiones). Son programas y herramientas de seguridad de detección de acceso no permitido a un dispositivo digital o red, que alerta de las actividades maliciosas o infracciones de políticas de seguridad, respondiendo a las amenazas sin afectar al tráfico de datos, al trabajar con una captura y copia del tráfico intruso.

La tecnología que se utiliza puede ser de los siguientes tipos:

– *Host-Based*: el análisis del tráfico y la búsqueda de actividad maliciosa se realiza sobre un solo *host*, dispositivo individual o servidor de red.
– *Network-Based*: se realiza sobre una determinada parte de la red, automatiza procesos a gran escala y procesa el tráfico de dicho segmento.
– *Knowledge-Based*: se utiliza el conocimiento almacenado en bases de datos compartidas.
– *Behavior-Based*: estudia el tráfico mediante la observación en los patrones de comportamiento habituales en cada tipo de comunicación, detectando las similitudes o diferencias.

f. Sistemas IPS: Sistemas de Prevención de Intrusiones (*Intrusion Prevention System)*. Se distinguen de los sistemas IDS al supervisar el tráfico de red en busca de amenazas potenciales y bloquearlas directamente con alertas al propio dispositivo, por lo que no permiten la entrada del tráfico intruso o malicioso en la red.

g. Sistemas proxy: es la puerta de enlace o acceso entre el usuario e internet, de manera que se facilitan los datos de IP al servidor proxy, que es como un ordenador en la red que ofrece protección mediante filtros web y *firewalls*, contra posibles amenazas.

h. Sistemas balanceadores de carga: con ellos se distribuye el flujo y tráfico de red entre una gran cantidad de servidores de internet que están en conexión entre sí, lo que favorece el óptimo tráfico en momentos de alta afluencia.

i. Equipos UTM (*Unified Threat Management* o gestión unificada de amenazas): los múltiples servicios de seguridad y protección mediante *antispam*, antivirus, filtrados de emails, etcétera, se ofrecen en un solo dispositivo.

j. Sistemas contra ataques DDOS (*Distributed Denial of Service* o ataques de denegación de servicio distribuido): se colapsa y ataca un servidor de internet para evitar y bloquear el acceso de los internautas a los servicios y sitios *online*.

4. Instrumentos de cooperación internacional

El 24 de diciembre de 2024, la Asamblea General de las Naciones Unidas (onu) aprobó el primer tratado internacional sobre crimen, la Convención de las Naciones Unidas contra la Ciberdelincuencia, que fue propuesta en 2019.

En materia de cooperación internacional, hay un firme propósito y voluntad para trabajar en la lucha contra la ciberdelincuencia. En concreto, tras su adhesión el 14 de mayo de 2008, España participa y forma parte del Centro de Excelencia de Ciberdefensa Cooperativa (*Cooperative Cyber Defence Centre of Excellence*, CCDCOE), que la OTAN instauró en Tallín, Estonia.

El CCDCOE es una organización internacional que recoge la capacidad de ciberdefensa de la OTAN, y pretende unir los esfuerzos de los países participantes, con la posibilidad de firmar convenios con organizaciones e instituciones públicas y privadas externas, como universidades, empresas, centros, etcétera.

En el ámbito de la Unión Europea (UE), el 11 de enero de 2013 entró en funcionamiento el Centro Europeo de Cibercrimen (EC3), dependiente de la Europol, ubicado en La Haya, Países Bajos. Su objetivo es coordinar las actividades policiales transfronterizas contra la ciberdelincuencia y proteger a las empresas y a los ciudadanos europeos de la ciberdelincuencia y del ciberterrorismo, al mismo tiempo que defender la existencia de una internet libre, abierta y segura, mediante la prevención de la criminalidad en la red.

Está diseñado para aportar soporte a todos los países de la UE e intercambiar sus conocimientos, operando como centro de fusión de la información y de apoyo operativo, forense y de investigación; también, para movilizar todos los recursos en los Estados miembros de la UE y, de esta manera, minimizar la amenaza de los delincuentes con independencia del lugar de comisión delictiva.[25]

La actividad del Centro Europeo de Ciberdelincuencia (EC3) se centra en las actividades ilegales en línea de las bandas de delincuencia organizada, especialmente en los ataques dirigidos contra las operaciones bancarias y actividades financieras; en la explotación sexual infantil *online*, y en los delitos que afectan las estructuras críticas y los sistemas de información de la UE.[26]

Como señala el profesor Leyre Hernández Díaz:

> […] la difusión de ordenadores en el mundo empresarial supuso que la gran parte de delincuencia informática tuviese relación con la delincuencia económica […]. Hasta el punto de que estas nuevas modalidades de delincuencia económica integraban el concepto de delito informático; o, al menos, […] las principales manifestaciones del mismo. [27]

Por ello, el EC3 prioriza la persecución, los delitos de defraudación económica, los ataques informáticos a empresas o infraestructuras críticas y los relativos a la explotación sexual infantil.

Para dicho propósito se recopila una gran cantidad y variedad de información de origen diverso, del ámbito público y privado, que determina una base de datos policiales para intercambiar con los países miembros en el marco de la cooperación internacional. Es así como la ue, en materia de ciberdefensa,

25 Cfr. Comisión Europea, "El Centro Europeo de Ciberdelincuencia (EC3) se inaugura el 11 de enero", *Comisión Europea* [en línea], 9 de enero de 2013. https://ec.europa.eu/commission/presscorner/detail/es/ip_13_13

26 Cfr. *Idem*.

27 Leyre Hernández Díaz, "El delito informático", *Eguzkilore*, núm. 23, diciembre de 2009, p. 229.

el 12 de diciembre de 2006,[28] creó un Programa Europeo para la Protección de las Infraestructuras Críticas (pepic) y posteriormente adoptó una propuesta de Directiva de identificación de estructuras críticas europeas para reforzar y optimizar la protección de éstas.

Dicho programa[29] diseña un plan de acción y medidas estratégicas de protección de las infraestructuras críticas de la Unión Europea, que se articula sobre la base de una red de alerta de nombre *Critical Infraestructure Warninig Information Network*, CIWIN; también, de la creación de un grupo de expertos de protección, la ayuda a los Estados y planes de intervención, planes estratégicos, medidas financieras y programas de prevención, entre ellos, uno específico de prevención, preparación y gestión de las consecuencias del terrorismo y de otros riesgos en materia de seguridad, así como mejora legal de la protección de los sistemas de información, que conduce a la implementación del marco legislativo de los países de la Unión Europea.

En el marco normativo europeo se cuenta con la Directiva 2002/58/CE, del 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas;[30] esta autoriza a los Estados miembros a que regulen por ley la obligación, a cargo de los prestadores de servicios, de conservar los datos electrónicos de tráfico de sus clientes, por razones de seguridad nacional, defensa, seguridad pública y lucha contra la criminalidad, durante un tiempo limitado y determinado libremente por cada Estado miembro.[31]

Después se aprobó el Reglamento de 2004 del Parlamento Europeo y del Consejo, en virtud del cual se crea la Agencia Europea de Seguridad de las Redes y la Información para:

> […] garantizar un nivel efectivo y elevado de seguridad de la red y de la información en la Comunidad y con el fin de desarrollar una cultura de la seguridad de las redes de información en beneficio de los ciudadanos, los consumidores, las empresas y las organizaciones del sector público de la Unión Europea, lo que contribuirá al correcto funcionamiento del Mercado Interior.[32]

28 Cfr. Unión Europea, *Diario Oficial de la Unión Europea*, serie C, núm. 126, 7 de junio de 2007. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2007:126:FULL&from=-FR

29 Cfr. Comisión Europea, Programa Europeo para la Protección de Infraestructuras Críticas, 7 de junio de 2007. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=legissum:l33260

30 Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), Parlamento Europeo y del Consejo de la Unión Europea, *Diario Oficial de las Comunidades Europeas*, 12 de julio de 2002. https://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81371

31 Cfr. Norberto Javier de la Mata Barranco, "Ilícitos vinculados al ámbito informático: la respuesta penal", en José Luis de la Cuesta Arzamendi (dir.), *Derecho Penal Informático*, Madrid: Civitas, 2010, pp. 15-30.

32 Reglamento (CE) 460/2004, del Parlamento Europeo y del Consejo de la Unión Europea, *Diario Oficial de la Unión Europea*, núm. 77, capítulo 1, art. 1.1, 13 de marzo de 2004. https://www.boe.es/buscar/doc.php?id=-DOUE-L-2004-80487

También cabe resaltar la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005,[33] relativa a los ataques contra los sistemas de información, para combatir la delincuencia informática y fomentar y desarrollar la seguridad de la información, reforzando la cooperación entre las autoridades judiciales, policiales y otras con competencia para la lucha contra la delincuencia informática, que se manifiesta en ataques informáticos.[34]

Por otra parte, está la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE,[35] que se centra en el uso de las comunicaciones digitales y las medidas por adoptar para la prevención, investigación, persecución e imputación, con mayor énfasis en el ámbito de la delincuencia organizada.

Por su parte, España, como país miembro de la Unión Europea y con una situación geográfica ventajosa para luchar y combatir esta ciberdelincuencia, creó la Estrategia de Seguridad Nacional española en 2011, revisada posteriormente en 2013,[36] cuyos principios y directrices fundamentales son: la unidad de acción, anticipación y prevención, eficiencia y sostenibilidad en el uso de los recursos, y resiliencia o capacidad de resistencia y recuperación.

La Estrategia de Ciberseguridad española de 2013 diseña ocho líneas de acción llevadas a cabo por el Consejo de Seguridad Nacional 2013, entre las que destaca: aumentar la prevención, detección, investigación y respuesta ante las ciberamenazas; garantizar y fortalecer la seguridad de los sistemas de información, redes e infraestructuras críticas; potenciar las capacidades para investigar y perseguir las actividades terroristas, e intensificar la colaboración internacional.

Los ámbitos de actuación son: defensa nacional, lucha contra el terrorismo, ciberseguridad, lucha contra el crimen organizado, seguridad económica y financiera, seguridad energética, no proliferación de armas de destrucción masiva, ordenación de flujos migratorios, contrainteligencia y protección ante emergencias y catástrofes. [37]

En concreto, para combatir la lucha contra el terrorismo, establece diferentes líneas de acción: prevención, protección, persecución y resiliencia.

33 Decisión Marco 2005/222/JAI, Consejo de la Unión Europea, *Diario Oficial de la Unión Europea*, 24 de febrero de 2005. https://www.boe.es/buscar/doc.php?id=DOUE-L-2005-80503

34 Cfr. Cristos Velasco San Martin, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e Internet*, Valencia: Tirant lo Blanc (Monografías, 807), 2012.

35 Directiva 2006/24/CE, Parlamento Europeo y del Consejo de la Unión Europea, *Diario Oficial de la Unión Europea*, núm. 105, 15 de marzo de 2006. https://www.boe.es/buscar/doc.php?id=DOUE-L-2006-80647

36 Departamento de Seguridad Nacional, *Estrategia de Seguridad Nacional. Un proyecto compartido*, Madrid: Gobierno de España, mayo, 2013. https://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

37 Cfr. *Idem*.

4.1 Asistencia judicial

El desarrollo de la tecnología informática, la aparición de nuevas tecnologías y su constante evolución han originado un medio nuevo de actuación, un gran cambio en la sociedad y una nueva forma de delincuencia, la ciberdelincuencia, desarrollada en el seno de la sociedad de la información y la telecomunicación; en consecuencia, a través de la tecnología se permite y posibilita cometer delitos tradicionales de forma no tradicional, desde cualquier parte del mundo y en cualquier momento.[38]

Sieber destacó que, desde mediados del siglo XX, surgieron tres etapas importantes que marcaron la evolución de la sociedad industrial a la sociedad de la información, lo que generó la aparición de la revolución informática, la sociedad de riesgos y, por último, una sociedad global/internacional que adquiere mayor protagonismo ante las sociedades nacionales.[39]

De esta forma, el desarrollo de la sociedad industrial hacia la sociedad de la información, en la que la tecnología facilita la creación, uso e intercambio de la información, es un proceso en evolución constante y dinámico y que afecta a toda la sociedad en general, la cual en la segunda etapa, se puede calificar concretamente como "una sociedad en la que los ciudadanos sean capaces de hacer uso de diversos servicios de telecomunicaciones avanzados para mejorar los distintos aspectos de su vida cotidiana". [40]

El *Diccionario* de la Real Academia Española dice que la información es, entre otras acepciones: "comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada".[41]

El concepto de sociedad de la información surgió en Japón en los años setenta, con la obra de Yoneji Masuda titulada: *Una introducción a la sociedad de la información en 1984*.

La información, en el mundo actual, tiene un papel fundamental en las relaciones personales, sociales, económicas, políticas y culturales, toda vez que, con el desarrollo de las tecnologías, el mundo y la sociedad están completamente digitalizados; por ello, cobra especial protagonismo, a pesar de que, como contrapartida, puede suponer un peligro individual y colectivo, lo que ha motivado y acelerado los procesos de protección frente a las nuevas formas de delincuencia que se valen de la información y la comunicación para perpetrar los distintos delitos que, como medio comisivo, usan la tecnología y la red.

Las organizaciones criminales internacionales, europeas y nacionales, haciendo

38 Cfr. Benjamín Blanco Blanco, "Revista núm. 151. El crimen organizado y las nuevas tecnologías", *El Fisco*, s. f. http://elfisco.com/articulos/revista-no-151-el-crimen-organizado-y-las-nuevas-tecnologias

39 Cfr. Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos*, Granada: Comares, 2002.

40 Cfr. miguel López Coronado, evaristo Abril Domingo y Rafael Mompó Gómez, "La necesidad de indicadores sociales y económicos para el estudio de la evolución de la sociedad de localización", *Revista de Investigación Económica y Social de Castilla y León*, núm. 1, 1999, pp. 73-86. https://dialnet.unirioja.es/servlet/articulo?codigo=1219319

41 Real Academia Española, "Información", en *Diccionario de la Lengua Española*. https://dle.rae.es/informaci%C3%B3n

uso de la información obtenida de la sociedad y de las nuevas tecnologías, actúan, en muchas ocasiones, con total impunidad, centrando su principal actividad en la comercialización de información financiera *online*, que reporta grandes beneficios económicos ilícitos, y en la perpetración de delitos informáticos, como estafas, fraudes informáticos, violación del derecho a la intimidad, acoso, extorsiones, pornografía infantil, tráfico de drogas, entre otros.

Como afirma José López Yepes, la Unión Europea ha sido de los principales promotores de la sociedad de la información desde los años 90, incluso adoptó un plan de actuación denominado "Europa en marcha hacia la Sociedad de la Información", que contenía el informe Bangemann de 1994. En 1996 se elaboró otro documento llamado "Europa a la vanguardia de la Sociedad de la Información. Plan de actuación móvil".[42]

Como dice Javier Fernández Teruelo:

> […] 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.[43]

En el marco de la Unión Europea, tenemos un informe de la Europol, "Internet Organised Crime Threat Assessment" (IOCTA), que pretende adoptar mejores decisiones y establecer prioridades en el ámbito de la lucha contra los delitos informáticos, la explotación sexual infantil a través de internet, los fraudes de pagos en la red y otros tipos de delitos.[44]

La lucha y persecución de la delincuencia informática se lleva a cabo en el espacio común de libertad, seguridad y justicia, y concretamente en el de justicia, con instrumentos cuyo objetivo es asegurar el establecimiento de una cooperación judicial penal.

Europol es el órgano que trabaja conjuntamente con los Estados miembros, instituciones, organismos y entidades para la lucha contra la delincuencia internacional.

La Comisión Europea, desde hace muchos años y actualmente, trabaja con gran esfuerzo, ante la proliferación de la ciberdelincuencia, para reprimirla y proteger a Europa; esta apunta que:

> Una respuesta eficaz ante los incidentes y crisis de ciberseguridad a gran escala a nivel de la UE requiere una cooperación rápida

42 José López Yepes, "La política de la Sociedad de la Información en España", *Documentación de las Ciencias de la Información*, núm. 24, octubre, 2001, pp. 14-15. https://revistas.ucm.es/index.php/DCIN/article/download/DCIN0101110011A/19491/20434

43 Javier Gustavo Fernández Teruelo, *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, Valladolid: Lex Nova, 2011.

44 Cfr. European Union Agency for Law Enforcement Cooperation (Europol), *Europol Review. General Report on Europol Activities 2015*, La Haya: European Police Office, 2016.

> y eficaz entre todas las partes interesadas pertinentes y se basa en la preparación y en las capacidades de cada uno de los Estados miembros, así como en una acción común coordinada apoyada en las capacidades de la Unión.[45]

En España, el ordenamiento jurídico en materia de ciberdelincuencia, el artículo 276 de la Ley Orgánica del Poder Judicial, 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",[46] por lo que hay una remisión directa a los convenios internacionales de los que España es integrante y que, a nivel europeo, son:

- Convenio Europeo de Asistencia Judicial en Materia Penal, aprobado en Estrasburgo el 20 de abril de 1959.[47]
- Convenio de Aplicación del Acuerdo de Schengen de 19 junio de 1990.[48]
- Convenio Europeo relativo a la Asistencia Judicial en Materia Penal entre los Estados Miembros de la Unión, aprobado en Bruselas el 29 de mayo de 2001.[49]

Al amparo del artículo 277 de la LOPJ, más allá del ámbito europeo, tendremos que aplicar los convenios existentes o el reconocimiento legislativo y judicial entre países por reciprocidad.

45 Recomendación (UE), 2017/1584, Comisión Europea, *Diario Oficial de la Unión Europea*, 13 de septiembre de 2017, párr. 5. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017H1584

46 Ley Orgánica del Poder Judicial (LOPJ), *Boletín Oficial del Estado*, núm. 157, 2 de julio de 1985 (última reforma publicada en el *Boletín Oficial del Estado* el 17 de febrero de 2025), art. 276. https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666

47 Ratificado por España el 14 de julio de 1982. Cfr. Instrumento de Ratificación de 14 de julio de 1982 del Convenio Europeo de Asistencia Judicial en Materia Penal, hecho en Estrasburgo el 20 de abril de 1959, *Boletín Oficial del Estado*, núm. 223, 17 de septiembre de 1982. https://www.boe.es/buscar/doc.php?id=BOE-A-1982-23564

48 Ratificado por España el 5 de abril de 1994. Cfr. Instrumento de ratificación del Acuerdo de Adhesión del Reino de España al Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, al cual se adhirió la República Italiana por el Acuerdo firmado en París el 27 de noviembre de 1990, hecho el 25 de junio de 1991, *Boletín Oficial del Estado*, núm. 81, de 5 de abril de 1994. https://www.boe.es/buscar/doc.php?id=BOE-A-1994-7586

49 Ratificado por España el 28 de octubre de 2005. Cfr. Entrada en vigor del Convenio celebrado por el Consejo, de conformidad con el artículo 34 del Tratado de la Unión Europea, relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, hecho en Bruselas el 29 de mayo de 2000, cuya aplicación provisional fue publicada en el 'Boletín Oficial del Estado' número 247, de 15 de octubre de 2003, *Boletín Oficial del Estado*, núm. 258, 28 de octubre de 2005. https://www.boe.es/eli/es/res/2000/05/29/(4)

El artículo 82.1 del Tratado de Funcionamiento de la Unión Europea (TFUE) —derivado del Tratado de Lisboa que se elaboró tras el Tratado Constitutivo de la Comunidad Europea, según estableció el Tratado de Maastricht—,[50] establece "[...] el principio de reconocimiento mutuo de las sentencias y resoluciones judiciales" y "la aproximación de las disposiciones legales y reglamentarias de los Estados miembros en los ámbitos mencionados en el apartado 2 y en el artículo 83", esto es, en materia penal y procesal penal.[51]

El principio de reconocimiento mutuo en la cooperación judicial europea se abordó en el Consejo Europeo de Tampere de 1999, en el Programa de la Haya de 2005 y en el de Estocolmo en 2010 y 2014.

En cualquier caso, hay que destacar que la Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la Orden Europea de Investigación (OEI) en materia penal, responde a la necesidad de solucionar los problemas de fragmentación y complejidad del marco existente para la obtención de pruebas de investigación penal establecidas por las Decisiones Marco 2003/577/JAI y 2008 /978/JAI.

La Orden Europea de Investigación (OEI) diseña un régimen único en la investigación de los delitos telemáticos para la obtención de pruebas en los casos de aplicación internacional, simplificando y acelerando sus procesos.[52]

En consecuencia, para dar cumplimiento y eficacia a la cooperación judicial penal, basada en el principio de reconocimiento mutuo de las resoluciones judiciales, el Parlamento Europeo y el Consejo prevén la posibilidad de adoptar criterios normativos conforme al procedimiento legislativo ordinario, con observancia de los ordenamientos jurídicos internos de los propios Estados miembros, de manera que se refuerce la confianza mutua y recíproca en orden a establecer normas y criterios penales y procesales que faciliten, fomenten y unifiquen la cooperación judicial.

Con todo ello, la finalidad esencial es reprimir la delincuencia tradicional, como, por ejemplo, fraudes, estafas, falsificación, suplantación de identidad, la pornografía infantil, delitos contra sistemas informáticos, delitos de odio, tráfico de drogas, por medio de las tecnologías y redes de internet y sistemas de comunicación e información digitales.

50 El tratado de la Comunidad Europea se basó en el Tratado de la Comunidad Económica Europea (TCEE) firmado en Roma el 25 de marzo de 1957. La creación de la Unión Europea por medio del Tratado de Maastricht, el 7 de febrero de 1992, supuso el paso a la unificación política de Europa. Cfr. Tratado de Funcionamiento de la Unión Europea, *Diario Oficial de la Unión Europea*, serie C, núm. 202/01, 7 de junio de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=legissum:4301854

51 *Idem*, art. 82.1.

52 La OEI se ejecutará en cada Estado miembro sobre la base del principio de reconocimiento mutuo y se regirá por el derecho del estado de ejecución. Cfr. Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, *Diario Oficial de la Unión Europea*, serie L, núm. 130/1, 1 de mayo de 2025. http://data.europa.eu/eli/dir/2014/41/oj

El problema de estos delitos estriba en que su comisión despliega sus efectos de forma trasnacional, lo que genera graves problemas en la instrucción de la causa, investigación, obtención de pruebas, recopilación e incriminación posterior y, como refiere la Oficina contra la Droga y el Delito de Naciones Unidas (UNOCD), "la mayoría de los datos probatorios son intangibles y transitorios".[53] En relación con los delitos informáticos, además, sostiene que estos son conductas proscritas:

> [...] por la legislación y/o la jurisprudencia, que implican la utilización de las tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos.[54]

En 2008 nace, en la Unión Europea, la Estrategia de Ciberseguridad, con especial protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad.

Y, con posterioridad, se aprobó y publicó la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.[55]

El art. 1 de la Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, señala las siguientes medidas:

a. establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;
b. crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;
c. crea una red de equipos de respuesta a incidentes de seguridad informática, llamado CSIRT (*Computer Security Incident Response Teams*) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;
d. establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;
e. establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.[56]

La Comunicación de 2016 sobre "Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguri-

53 Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Delitos informáticos*, 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, hoja informativa 6, 18 a 25 abril de 2005, Bangkok, Tailandia, p. 2.

54 *Ibidem*, p. 1.

55 Cfr. Directiva (UE) 2016/1148, Parlamento Europeo y del Consejo de la Unión Europea, *Diario Oficial de la Unión Europea*, serie L, núm. 194/1, 6 de julio de 2016. https://www.boe.es/doue/2016/194/L00001-00030.pdf

56 *Ibidem*, párr. 2.

dad competitiva e innovadora"[57] instó a los Estados miembros a aplicar la Directiva (UE) 2016/1148, en materia de seguridad de las redes y sistemas de información (Directiva SRI).

La finalidad no es otra que reforzar la cooperación transfronteriza para combatir la comisión reincidente de gran expansión. Asimismo, estableció que se obtendrían mejores resultados si se creaba un enfoque coordinado de la cooperación ante las crisis entre los diferentes elementos del ecosistema cibernético, que se debería plasmar en un "plan director" de la Comisión Europea.[58]

En las Conclusiones del Consejo Europeo del 22 y 23 de junio de 2017, se reconoció que la Unión Europea "ha dedicado su atención al fortalecimiento de Europa y a la protección de los ciudadanos mediante medidas eficaces destinadas a luchar contra el terrorismo y a desarrollar su seguridad y defensa comunes [...]".[59] Asimismo, en relación con el desarrollo de la Europa digital, en ese mismo Consejo Europeo se debatió y se establecieron planteamientos que se abordarían en la cumbre digital celebrada en Tallin el 29 de septiembre de 2017. También el Consejo Europeo recalcó la necesidad de trabajar en la ciberseguridad en Europa y remarcó el objetivo de la Comisión Europea de revisar la Estrategia de Ciberseguridad en septiembre de 2017 y de proponer y recabar más objetivos antes de la finalización del año.[60]

Por tanto, los objetivos de la CE, en aras de implementar la estrategia general de la Unión Europea, son proponer y supervisar las leyes, así como su aplicación y las políticas de la UE; garantizar el cumplimiento del ordenamiento jurídico de la UE y gestionar el presupuesto de la UE, además de velar por el desarrollo internacional y humanitario. Desde la Comisión Europea se adoptó la implantación de medidas de diferentes tipos,[61] como las siguientes:

- Fortalecimiento de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea en (ENISA).
- Creación de un mercado único de la seguridad en internet.
- Aplicación de la Directiva relativa a la seguridad de las redes y sistemas de información.
- Mecanismos de solución rápida de emergencia, con un plan director que contribuya a dar una respuesta directa en el ámbito de la Unión de los Estados

57 Cfr. Comisión Europea (CE), COM/2016/0410 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Bruselas, 5 de julio de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016DC0410

58 Cfr. Recomendación (UE) 2017/1584, Comisión Europea, *Diario Oficial de la Unión Europea*, serie C, núm. 6100, 13 de septiembre de 2017. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017H1584

59 Consejo Europeo, Conclusiones de la reunión del Consejo Europeo, Bruselas, 23 de junio de 2017, p. 1. https://www.consilium.europa.eu/media/23969/22-23-euco-final-conclusions-es.pdf

60 Cfr. *Idem*.

61 Cfr. Comisión Europea (CE), JOIN/2017/0450 Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la Ciberseguridad de la UE, Bruselas, 13 de septiembre de 2017. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52017JC0450

miembros ante un riesgo cibernético o ataque.
- Creación de una red de competencia en ciberseguridad con un Centro Europeo de competencia e investigación.
- Creación de una base sólida de competencias cibernéticas de la Unión Europea, promoción de la ciberhigiene y ciberconcienciación.
- Fomento de la ciberhigiene y la ciberconcienciación en orden a prevenir la ciberdelincuencia, con participación de las instituciones públicas y privadas, empresas y de los ciudadanos.

La Comisión Europea, con la finalidad de proteger y asegurar la ciberseguridad, adopta distintas acciones:

- Detectar a los ciberdelincuentes respecto de los ciberataques.
- Reforzar el sistema policial entre países con un protocolo y sistema procesal que permita la obtención y custodia de pruebas digitales.
- Colaboración del ámbito público y privado en la lucha contra la ciberdelincuencia.
- Aumentar la respuesta política con la colaboración de la diplomacia para luchar contra la ciberdelincuencia.
- Mejorar la defensa de los Estados miembros como un mecanismo disuasorio ante un eventual ataque de ciberseguridad.
- Optimizar y desarrollar la cooperación internacional en el ámbito de la ciberseguridad.

Los Estados miembros y la Unión Europea, desde hace muchos años, han trabajado conjuntamente en la lucha contra la ciberdelincuencia de forma preventiva, para lo cual han adoptado medidas, propuestas, normas y acciones políticas para combatirla.

Entre las prerrogativas que tiene la Unión Europea para luchar contra la ciberdelincuencia podemos señalar las siguientes:

1. La persecución de delitos informáticos

Presenta grandes problemas y dificultades por el específico medio comisivo digitalizado, esto es, internet y la estructura y funcionamiento intrínsecos y dinámica de ésta, pues conecta a los internautas y a los ciberdelincuentes, que actúan bajo el anonimato de forma trasnacional, en un espacio intangible y en distintos lugares, con normativa legal propia y, en ocasiones, sin regulación alguna o con lagunas legales, a veces, de gran escala. En este sentido, como afirma el profesor Bueno Arús, la delincuencia informática:

> [...] presenta dificultades especiales para su persecución en relación con la delincuencia tradicional, dada la rapidez de su comisión, que puede tener lugar a distancia, y atendida la complejidad de la fijación de la autoría, así como la facilidad para encubrir el hecho y borrar las pruebas que habrían permitido enjuiciarlo. [62]

2. La especialización de las autoridades judiciales y policiales

Es fundamental contar con una adecuada capacitación específica de la policía y de los operadores jurídicos, jueces y tribunales de justicia, y dotarlos de los medios técnicos necesarios, de nuevos instrumentos de inves-

62 Bueno Arús citado en Enrique Rovira del Canto, *op. cit.*

tigación y de una normativa que regule los medios de prueba tecnológicos válidos en un proceso penal. Es necesario, para ello, reforzar e implementar la coordinación legislativa internacional. Como dice el profesor Juan Carlos Ortiz Pradillo:

> La armonización normativa internacional sobre la ilicitud de los hechos delictivos, así como una mayor cooperación entre las distintas autoridades de los Estados miembros para la puesta a disposición y traslado de pruebas son propuestas a llevar a cabo para combatir el fenómeno de la ciberdelincuencia.[63]

Por tanto, la cooperación europea e internacional entre cuerpos policiales de los Estados miembros, la creación de fiscalías especializadas, el desarrollo de instrumentos procesales, la mejora de procedimientos de investigación y práctica forense en orden a detectar interceptación de comunicaciones informáticas, datos de navegación o rastreo de contenidos delictivos, son necesarios y de vital importancia para la lucha contra el cibercrimen, ya que ayudan a establecer estrategias de trabajo conjunto y medidas para combatirlo, para lo cual se capacita a los distintos operadores jurídicos y a los miembros de las fuerzas y cuerpos de seguridad y policiales nacionales e internacionales.

Cada vez es mayor la perfección en la ejecución del acto delictivo por parte de los ciberdelincuentes, que incluso actúan como auténticos profesionales y mercenarios de prestación de servicios y compraventa de productos en un mercado clandestino diverso, donde se puede obtener un amplio abanico de productos y servicios, desde drogas, hasta armas, asesinos a sueldo, pornografía infantil, terrorismo, fraudes, blanqueo de dinero, estafas, entre otros, que se llevan a cabo en el ámbito de internet y, más concretamente, de la *darknet*.

Finalmente, cabe señalar que el instrumento internacional por antonomasia en la lucha contra la ciberdelincuencia en general, y los delitos en la *darknet*, no es otro que el Convenio de Budapest de 23 de noviembre de 2001,[64] ratificado por España el 17 de septiembre de 2010.

4.2 Reconocimiento mutuo

La Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, establece en su artículo 2.1 que el principio de reconocimiento mutuo se entiende como "aquella orden europea o resolución emitida por la autoridad competente de un Estado miembro de la Unión europea que se trasmite a otro Estado miembro para su reconocimiento, y ejecución en el

63 Cfr. Juan Carlos Ortiz Pradillo, *Problemas procesales de la ciberdelincuencia*, Madrid: Colex, 2013.

64 Cfr. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, *Boletín Oficial del Estado*, núm. 226, 17 de septiembre de 2010. https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-S-2010-226.pdf

mismo".[65] Además, en su art. 2.2, define los instrumentos de reconocimiento mutuo:

a. La orden europea de detención y entrega.
b. La resolución por la que se impone una pena o medida privativa de libertad.
c. La resolución de libertad vigilada.
d. La resolución sobre medidas de vigilancia de la libertad provisional.
e. La orden europea de protección.
f. La resolución de embargo preventivo de bienes o de aseguramiento de pruebas.
g. La resolución de decomiso.
h. La resolución por la que se imponen sanciones pecuniarias.
i. La orden europea de investigación.[66]

El principio de reconocimiento mutuo y la aproximación de legislaciones en materia penal y procesal penal se regula también en el artículo 82.1 del Tratado de Funcionamiento de la Unión Europea. Cabe resaltar que, como sostiene Mar Jimeno Bulnes, estos principios no fueron nuevos del Tratado de Lisboa, puesto que se habían previsto con anterioridad en el Consejo Europeo de Tampere de 1999, en el Programa de la Haya de 2005 y en el Programa de Estocolmo en los años 2010 y 2014.[67]

Para poder cumplir con la finalidad de la cooperación penal, sobre la base del principio de reconocimiento mutuo de las resoluciones judiciales, a nivel europeo, tanto el Parlamento como el Consejo Europeo tienen competencia para elaborar normas con criterios penales y procesales comunes, para lo cual es necesaria la confianza recíproca entre los Estados miembros, como apunta María Ángeles Pérez Marín.[68]

El principio de reconocimiento mutuo se formuló en el Consejo Europeo de Tampere y se convirtió en la base fundamental de la cooperación judicial penal y también civil en la Unión Europea; funciona como paradigma de cooperación, puesto que cualquier resolución emitida por una autoridad judicial de un Estado miembro, con aplicación de dicho principio, debe ser reconocida, respetada y ejecutada en otro Estado miembro, excepto en aquellos casos en que concurran motivos o causas de denegación justificada que amparen dicha excepción.

65 Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, *Boletín Oficial del Estado*, núm. 282, 21 de noviembre de 2014 (última reforma publicada en el Boletín Oficial del Estado el 3 de enero de 2025), art. 2.1. https://www.boe.es/eli/es/l/2014/11/20/23/con

66 Véase Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, para regular la Orden Europea de Investigación, *Boletín Oficial del Estado*, núm. 142, 12 de junio de 2018. https://www.boe.es/eli/es/l/2018/06/11/3, solo en lo referido a "la orden europea de investigación", artículo único 1.

67 Cfr. Mar Jimeno Bulnes, "Las implicaciones del Tratado de Lisboa en la cooperación judicial europea en materia penal", en Coral Arangüena Fanego (dir.), *Espacio Europeo de Libertad, Seguridad y Justicia: últimos avances en cooperación judicial penal*, Valladolid: Lex Nova, 2010, pp. 30-70.

68 Cfr. María Ángeles Pérez Marín, *La lucha contra la criminalidad en la Unión Europea. El camino hacia una jurisdicción penal común*, Barcelona: Atelier, 2013.

La regulación, como hemos apuntado anteriormente, se encuentra en la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea; la Ley 3/2018, de 11 de junio, que modifica a la anterior sólo en el art. 1 respecto a la "orden europea de investigación", y la Ley Orgánica 6/2014, de 29 de octubre, complementaria de la ley 23/2014 de 20 de noviembre, por la que se modifica la LOPJ.[69]

Como instrumento jurídico principal,

69 Esta ley incorpora a nuestro ordenamiento jurídico:
- La Decisión Marco 2008/909/JAI, de 27 de noviembre de 2008, relativa a la aplicación del principio de reconocimiento mutuo de sentencias en materia penal por las que se imponen penas u otras medidas privativas de libertad a efectos de su ejecución en la Unión Europea.
- La Decisión Marco 2008/947/JAI, de 27 de noviembre de 2008, relativa a la aplicación del principio de reconocimiento mutuo de sentencias y resoluciones de libertad vigilada con miras a la vigilancia de las medidas de libertad vigilada y las penas sustitutivas.
- La Decisión Marco 2008/978/JAI, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal.
- La Decisión Marco 2009/299/JAI, de 26 de febrero de 2009, por la que se modifican las Decisiones Marco 2002/584/JAI, 2005/214/JAI, 2006/783/JAI, 2008/909/JAI y 2008/947/JAI, destinada a reforzar los derechos procesales de las personas y a propiciar la aplicación del principio de reconocimiento mutuo de las resoluciones dictadas a raíz de juicios celebrados sin comparecencia del imputado;
- La Decisión Marco 2009/829/JAI, de 23 de octubre de 2009, relativa a la aplicación, entre Estados miembros de la Unión Europea, del principio de reconocimiento mutuo a las resoluciones sobre medidas de vigilancia como sustitución de la prisión provisional;
- La Directiva 2011/99/UE, de 13 de diciembre de 2011, sobre la orden europea de protección.
- La Decisión Marco 2002/584/JAI, relativa a la orden europea y a los procedimientos de entrega entre Estados miembros, incorporada inicialmente al Derecho español a través de la Ley 3/2003, de 14 de marzo, sobre la orden europea de detención y entrega y la Ley Orgánica 2/2003, de 14 de marzo, complementaria de la anterior.
- La Decisión Marco 2003/577/JAI, de 22 de julio de 2003, relativa a la ejecución en la Unión Europea de las resoluciones de embargo preventivo de bienes y aseguramiento de pruebas, incorporada inicialmente al Derecho español a través de la Ley 18/2006, de 5 de junio, para la eficacia en la Unión Europea de las resoluciones de embargo y aseguramiento de pruebas en procedimientos penales y la Ley Orgánica 5/2006, de 5 de junio, complementaria de la anterior, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
- La Decisión Marco 2005/214/JAI, de 24 de febrero de 2005, relativa a la aplicación del principio de reconocimiento mutuo de sanciones pecuniarias, transpuesta anteriormente en España mediante la Ley 1/2008, de 4 de diciembre, para la ejecución en la Unión Europea de resoluciones que impongan sanciones pecuniarias y la Ley Orgánica 2/2008, de 4 de diciembre, de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, complementaria de la anterior.
- La Decisión Marco 2006/783/JAI, de 6 de octubre de 2006, relativa a la aplicación del principio de reconocimiento mutuo

está la Orden Europea de Detención y Entrega y Protección, y el Título X relativo a la diligencia de exhorto europeo de obtención de pruebas, que ha sido derogado y sustituido por la Directiva 2014/41/UE del Parlamento Europeo y del Consejo, relativa a la Orden Europea de Investigación (OEI).

Hay que reseñar que la Orden Europea de Detención y Entrega (oede) y el resto de instrumentos de reconocimiento mutuo no han sido muy utilizados por las autoridades judiciales españolas.

4.3 Entrega y extradición

El marco normativo de entrega y orden de detención entre Estados miembros se encuentra en la Decisión Marco del Consejo 2002/584/JAI, de 13 de junio de 2002, que "es la primera concreción en el ámbito del Derecho penal del principio del reconocimiento mutuo que el Consejo Europeo ha calificado como 'piedra angular' de la cooperación judicial";[70] también, está en la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.[71]

Podemos decir que la extradición es la entrega de un investigado o culpable de un delito, de un Estado a otro para poder ser enjuiciado en el país que solicite la extradición o que cumpla la condena en el que lo solicita. Esta práctica es una clara y directa manifestación de la cooperación jurídica internacional y una herramienta útil en orden a la lucha contra la delincuencia trasnacional y la ciberdelincuencia.

En el ordenamiento jurídico español, nos encontramos con la regulación de la extradición en el artículo 13.3 de la Constitución Española (CE), que dice: "la extradición sólo se concederá en cumplimiento de un tratado o de la ley, atendiendo al principio de reciprocidad. Quedan excluidos de la extradición los delitos políticos, no considerándose como tales los actos de terrorismo".[72]

Concretamente, en España, se contempla este procedimiento en la Ley 4/1985, de 21 de marzo, de extradición pasiva, que establece en su artículo 2 que:

> [...] se podrá conceder la extradición por aquellos hechos para los que las Leyes españolas y las de la parte requirente señalen una pena o medida de seguridad cuya duración no sea inferior a un año de privación de libertad en su grado máximo o a una pena más grave; o cuando la reclamación tuviere por objeto el cumplimiento de condena a una pena o medida de seguridad no inferior a cuatro meses de privación de libertad por

de resoluciones de decomiso, transpuesta anteriormente en nuestro país, a través de la Ley 4/2010, de 10 de marzo, para la ejecución en la Unión Europea de resoluciones judiciales de decomiso y la Ley Orgánica 3/2010, de 10 de marzo, de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y complementaria de la anterior.

70 Decisión Marco 2002/584/JAI, Consejo de la Unión Europea, *Diario Oficial de las Comunidades Europeas*, núm. 190, 13 de junio de 2002. https://www.boe.es/buscar/doc.php?id=-DOUE-L-2002-81377

71 Cfr. Ley 23/2014, *op. cit.*

72 Constitución Española, *Boletín Oficial del Estado*, 29 de diciembre de 1978. https://app.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=13&tipo=2

hechos también tipificados en la legislación española.[73]

El Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa de 23 de noviembre de 2001, en su artículo 24, define los principios generales relativos a la extradición en materia de ciberdelincuencia:

a. El presente artículo se aplicará a la extradición entre las Partes por los delitos establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.

b. Cuando deba aplicarse una pena mínima diferente en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE n.º 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.[74]

También establece, en el apartado 5 del referido artículo 24, que "la extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición".[75]

Los distintos y numerosos tratados de extradición suscritos por España regulan los delitos en concreto por los que debe acordarse la extradición. La competencia jurisdiccional en España para el conocimiento de la Orden Europea de Detención y Entrega (OEDE) y para ventilar los procesos de extradiciones la tienen los Juzgados Centrales de Instrucción y el Ministerio de Justicia.

La tramitación procesal de la OEDE o extradición es homogénea en todos los delitos que puedan ser objeto de esta; no existen diferencias entre sí por la propia tipología delictiva. Como medida cautelar, en el curso de tramitación de la OEDE se puede adoptar la prisión provisional mientras se sustancia el procedimiento principal de entrega, con el propósito preservar el cumplimiento efectivo del expediente de entrega[76] y evitar posibles fugas y la frustración de la extradición.

La adopción de prisión preventiva como medida cautelar se sustancia por el mismo procedimiento que en un supuesto de investigación nacional donde se adopte dicha medida y se aplican las mismas reglas y condiciones. En un procedimiento de extradición pasiva, de igual forma y conforme a la ley de

73 Ley 4/1985, de 21 de marzo, de extradición pasiva, *Boletín Oficial del Estado*, núm. 73, 26 de marzo de 1985. https://www.boe.es/eli/es/l/1985/03/21/4

74 Instrumento de Ratificación del Convenio de Budapest sobre Ciberdelincuencia, Consejo de Europa, *Boletín Oficial del Estado*, núm. 226, 23 de noviembre de 2001, art. 24. https://www.boe.es/eli/es/ai/2001/11/23/(1)

75 *Idem*.

76 Al formalizar la Orden Europea de Detención y Entrega, en la práctica, en vez de acordarse Auto de Detención, que genera mayores problemas, se suele dictar Auto de Prisión del artículo 539 lecrim, estableciendo la celebración de la comparecencia prevista en el art. 505 LECrim en las 48 horas siguientes a su detención.

extradición, se puede acordar la prisión provisional si el Estado reclamante así lo solicita; esta prisión provisional deberá dejarse sin efecto si, a los 40 días de haberse acordado, el Estado reclamante no ha presentado en forma la reclamación extradicional.77

5. Referencias

Álvarez, Cecilia, "Sentencia Google Spain y derecho al olvido", *Actualidad Jurídica Uría Menéndez*, pp. 110-118. https://es.scribd.com/document/444020931/Sentencia-Google-Spain-y-Derecho-Al-Olvido-Uria-Menendez

Álvarez, Raúl, "Así es como desmantelaron 'Welcome to Video', una de las webs de pornografía infantil más grandes del mundo en la Dark Web", *Xataka* [en línea], 17 de octubre de 2019. https://www.xataka.com/legislacion-y-derechos/asi-como-desmantelaron-welcome-to-video-webs-pornografia-infantil-grandes-mundo-dark-web

Blanco Blanco, Benjamín, "Revista núm. 151. El crimen organizado y las nuevas tecnologías", *El Fisco*, s. f. http://elfisco.com/articulos/revista-no-151-el-crimen-organizado-y-las-nuevas-tecnologias

Cáñamo, "Clausuran uno de los mayores mercados de la deep web", *Cáñamo. La Revista de la cultura del cannabis*, 6 de junio de 2019. https://canamo.net/noticias/mundo/clausuran-uno-de-los-mayores-mercados-de-la-deep-web

CCN-CERT, "El Papel de un cert gubernamental", *Perspectiva de las aa.pp.*, núm. 14, septiembre de 2007, pp. 50-52

CN-CERT, Centro Criptológico Nacional [en línea]. www.ccn-cert.cni.es

Comisión Europea (CE), JOIN/2017/0450 Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la Ciberseguridad de la UE, Bruselas, 13 de septiembre de 2017. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:-52017JC0450

CE, COM/2016/0410Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Bruselas, 5 de julio de 2016.https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A-52016DC0410

CE, "El Centro Europeo de Ciberdelincuencia (EC3) se inaugura el 11 de enero", *Comisión Europea* [en línea], 9 de enero de 2013. https://ec.europa.eu/commission/presscorner/detail/es/ip_13_13

Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, *Diario Oficial de la Unión Europea*, serie C, núm. 197/01, 12 de julio de 2000.

Decisión Marco 2002/584/JAI, Consejo de la Unión Europea, *Diario Oficial de las Comunidades Europeas*, núm. 190, 13 de junio de 2002. https://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81377

Directiva (UE) 2016/1148, Parlamento Europeo y del Consejo de la Unión Europea, *Diaro Oficial de la Unión Europea*, serie L, núm. 194/1, 6 de julio de 2016.https://www.boe.es/doue/2016/194/L00001-00030.pdf

77 Los tratados bilaterales suscritos por España contienen también normativa específica en relación con la prisión provisional, que regula y especifica cuestiones concretas como los plazos de presentación de documentación que puede variar dependiendo del tratado de aplicación preferente.

Directiva (UE) 2016/680, Parlamento Europeo y del Consejo de la Unión Europea, *Diario Oficial de la Unión Europea*, 27 de abril de 2016. https://www.boe.es/doue/2016/119/L00089-00131.pdf

Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, *Diario Oficial de la Unión Europea*, serie L, núm. 130/1, 1 de mayo de 2025. http://data.europa.eu/eli/dir/2014/41/oj

Entrada en vigor del Convenio celebrado por el Consejo, de conformidad con el artículo 34 del Tratado de la Unión Europea, relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, hecho en Bruselas el 29 de mayo de 2000, cuya aplicación provisional fue publicada en el 'Boletín Oficial del Estado' número 247, de 15 de octubre de 2003, *Boletín Oficial del Estado*, núm. 258, 28 de octubre de 2005. https://www.boe.es/eli/es/res/2000/05/29/(4)

Espinosa Sánchez, Jesús Francisco, "Ciberdelincuencia. Aproximación criminológica de los delitos en la red", *La Razón Histórica*, núm. 44, septiembre-diciembre, 2019, pp. 153-173.

European Union Agency for Law Enforcement Cooperation (Europol), *Europol Review. General Report on Europol Activities 2015*, La Haya:European Police Office, 2016.

Fernández Teruelo, Javier Gustavo, *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, Valladolid: Lex Nova, 2011.

Gómez Hernández, José Antonio y María Concepción Rayón Ballesteros, "Cibercrimen: particularidades en su investigación y enjuiciamiento", *Anuario Jurídico y Económico Escurialense*, núm. 47, marzo, 2014. https://publicaciones.rcumariacristina.net/AJEE/article/view/189

Hernández Díaz, Leyre, "El delito informático", *Eguzkilore*, núm. 23, diciembre de 2009, pp. 227-243.

Informe explicativo del Convenio, de 29 de mayo de 2000, relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, *Diario Oficial de la Comunidad Europea*, serie C, núm. 379/7, 29 de diciembre de 2000.

Instrumento de Ratificación de 14 de julio de 1982 del Convenio Europeo de Asistencia Judicial en Materia Penal, hecho en Estrasburgo el 20 de abril de 1959, *Boletín Oficial del Estado*, núm. 223, 17 de septiembre de 1982. https://www.boe.es/buscar/doc.php?id=BOE-A-1982-23564

Instrumento de ratificación del Acuerdo de Adhesión del Reino de España al Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, al cual se adhirió la República Italiana por el Acuerdo firmado en París el 27 de noviembre de 1990, hecho el 25 de junio de 1991, *Boletín Oficial del Estado*, núm. 81, de 5 de abril de 1994. https://www.boe.es/buscar/doc.php?id=BOE-A-1994-7586

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, *Boletín Oficial del Estado*, núm. 226, 17 de septiembre de 2010. https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-S-2010-226.pdf

La Sexta, "Detenidas 870 personas en una operación mundial contra la pornografía infantil", en *La Sexta*, 5 de mayo, 2017. https://www.lasexta.com/noticias/sociedad/detenidas-870-personas-operacion-mundial-pornografia-infantil_20170505590cd0c90cf22906e6b43143.html

Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, *Boletín Oficial del Estado*, núm. 282, 21 de noviembre de 2014 (última reforma publicada en el *Boletín Oficial del Estado* el 3 de enero de 2025). https://www.boe.es/eli/es/l/2014/11/20/23/con

Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, para regular la Orden Europea de Investigación, *Boletín Oficial del Estado*, núm. 142, 12 de junio de 2018. https://www.boe.es/eli/es/l/2018/06/11/3

Ley de Enjuiciamiento Criminal, *Gaceta de Madrid*, núm. 260, 17 de septiembre de 1882. https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

Ley Orgánica 4/2015, de protección de la seguridad ciudadana, *Boletín Oficial del Estado*, núm. 77, España, 30 de marzo de 2015. https://www.boe.es/buscar/act.php?id=BOE-A-2015-3442

Ley Orgánica del Poder Judicial (LOPJ), *Boletín Oficial del Estado*, núm. 157, 2 de julio de 1985 (última reforma publicada en el Boletín Oficial del Estado el 17 de febrero de 2025). https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666

López Coronado, Miguel Evaristo, Abril Domingo y Rafael Mompó Gómez, "La necesidad de indicadores sociales y económicos para el estudio de la evolución de la sociedad de localización", *Revista de Investigación Económica y Social de Castilla y León*, núm. 1, 1999, pp. 73-86. https://dialnet.unirioja.es/servlet/articulo?codigo=1219319

López Yepes, José, "La política de la Sociedad de la Información en España", *Documentación de las Ciencias de la Información*, núm. 24, octubre, 2001, pp. 14-15. https://revistas.ucm.es/index.php/DCIN/article/download/DCIN-No101110011A/19491/20434

Miró Llinares, Fernando, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid: Marcial Pons, 2013, pp. 37-38.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Delitos informáticos*, 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, hoja informativa 6, 18 a 25 abril de 2005, Bangkok, Tailandia.

Oficina de las Naciones Unidas contra la Droga y el Delito, *Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional y sus protocolos*. Nueva York: Naciones Unidas, 2004.

Ortiz Pradillo, Juan Carlos, *Problemas procesales de la ciberdelincuencia*, Madrid: Colex, 2013.

Pérez Álvarez, Fernando y Laura Zúñiga Rodríguez, *Instrumentos jurídicos y operativos en la lucha contra el tráfico internacional de drogas*, Navarra: Thomson Reuters, 2015.

Pérez Marín, María Ángeles, *La lucha contra la criminalidad en la Unión Europea. El camino hacia una jurisdicción penal común*, Barcelona: Atelier, 2013.

Quevedo González, Josefina, *Investigación y prueba del ciberdelito* (tesis doctoral), Barcelona: Universidad de Barcelona, 2017.

Real Academia Española, "Información", en *Diccionario de la Lengua Española*. https://dle.rae.es/informaci%C3%B3n

Recomendación (UE), 2017/1584, Comisión Europea, *Diario Oficial de la Unión Europea*, 13 de septiembre de 2017. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017H1584

Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos*, Granada: Comares, 2002.

Sentencia recaída al Recurso de Amparo 83/1994, Sala Primera del Tribunal Constitucional, ponente: presidente Álvaro Rodríguez, 14 de octubre de 1995. https://www.boe.es/diario_boe/txt.php?id=BOE-T-1995-22479

Tratado de Funcionamiento de la Unión Europea, *Diario Oficial de la Unión Europea*, serie C, núm. 202/01, 7 de junio de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=legissum:4301854

Unión Europea, *Diario Oficial de la Unión Europea*, serie C, núm. 126, 7 de junio de 2007. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2007:126:FULL&from=FR

URBANO CASTRILLO, Eduardo de, "Los delitos informáticos tras la reforma del cp de 2010", *Revista Aranzadi Doctrinal*, núm. 6, octubre, 2011, pp. 163-176.

VELASCO NÚÑEZ, Eloy, *Delitos cometidos a través de Internet: cuestiones procesales*, Madrid: La Ley, 2011.

RPM

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

ESTADOS UNIDOS MEXICANOS

FGR
FISCALÍA GENERAL
DE LA REPÚBLICA