FACULTAD DE DERECHO

LA *CIBERDELINCUENCIA* Y LAS ESPECIALIDADES PROCESALES DE LA PRUEBA

Autor: Marina Tornel Estrada
4º E1
Área de Derecho Procesal
Tutora: Cristina Carretero González

Madrid
Marzo 2022

ÍNDICE

Resumen

La ciberdelincuencia es uno de los grandes problemas del siglo XXI con los que el Derecho se está teniendo que enfrentar. El fin de este trabajo es realizar un análisis, no solo del crecimiento de la ciberdelincuencia y sus efectos jurídicos, sino de todos los recursos y mecanismos, a nivel jurídico, con los que el Estado español cuenta para la lucha e investigación de este tipo de delitos. Se trata especialmente la normativa aplicable a día de hoy en esta materia, así como algunas de las aportaciones jurisprudenciales clarificadoras de diversos asuntos relacionados con el objeto del trabajo. A su vez y, basado en la normativa y jurisprudencia mencionada, se estudian detalladamente aquellas cuestiones relacionadas con las pruebas digitales, y en concreto, todas las especialidades que le incumben, incluyendo especialidades en la obtención, en la admisibilidad, en la incorporación al juicio y en su valoración. A través del estudio de dichas peculiaridades junto con la normativa procesal se forman conclusiones acerca de la suficiente o insuficiente adaptación del derecho a esta nueva realidad social.
Palabras clave: ciberdelincuencia, prueba digital, prueba electrónica, investigación, tecnología, especialidades, penal.

Abstract

Cybercrime is one of the great problems of the 21st century with which the Law is having to deal. The aim of this work is to carry out an analysis, not only of the growth of cybercrime and its legal effects, but also of all the legal resources and mechanisms available to the Spanish State for the fight against and investigation of this type of crime. It deals with the regulations currently applicable in this area, as well as some of the clarifying jurisprudential contributions on various issues related to the object of the work. At the same time, and based on the aforementioned regulations and jurisprudence, a detailed study is made of those aspects related to digital evidence, and specifically, all the specialties involved, including specialties in obtaining it, in its admissibility, in its incorporation into the trial and in its assessment. Through the study of these peculiarities together with the procedural law, conclusions are drawn as to whether the law is sufficiently or insufficiently adapted to this new social reality.
Key words: cybercrime, digital evidence, electronic evidence, investigation, technology, specialties, criminal law.

Abreviaturas y acrónimos

Art.	Artículo
BOE	Boletín oficial del Estado
ENISA	Agencia de la Unión Europea para la Ciberseguridad
EE. UU.	Estados Unidos
FFCCSSEE	Fuerzas y Cuerpos de Seguridad del Estado
IMEI	*International Mobile Equipment Identity*
INTERPOL	Organización International de Policía Criminal
INCIBE	Instituto Nacional de Ciberseguridad
IP	*Internet Protocol*
LEC	Ley de Enjuiciamiento Civil
LECRIM	Ley de Enjuiciamiento Criminal
RAE	Real Academia Española
TIC	Tecnologías de la Información
TS	Tribunal Supremo
UE	Unión Europea
UNODC	Oficina de Naciones Unidas contra la droga y el delito

1. INTRODUCCIÓN

1.1. Contexto de los delitos informáticos

La sociedad está sometida a un cambio constante actualmente liderado por el avance tecnológico. Van Dijk[1] define la idea de *Network Society* como "un tipo de sociedad que de forma creciente organiza sus relaciones en redes digitales, gradualmente substituyendo las redes sociales de comunicación cara a cara tradicionales". La comunicación personal es sustituida por la tecnología digital.

La gran consecuencia de esta nueva forma de sociedad es la de que cuestiones que años atrás se realizaban de forma física, desde comunicar, comprar ropa, ingresar dinero, hasta estafar, acosar, amenazar, agredir sexualmente, han pasado a realizarse de forma telemática, aprovechándose así del gran crecimiento tecnológico y de las vías telemáticas que se han creado. En este contexto surge la *ciberdelincuencia*, los *ciberdelincuentes* y las pruebas tecnológicas.

Frente a esta realidad, el derecho es el encargado de adaptarse para constituir recursos eficaces y útiles y poder combatir así los delitos que utilizan las tecnologías de la informática para llevarse a cabo. Surge la necesidad de crear medios especializados para la persecución e investigación de esta nueva delincuencia que sean eficaces y garantistas.

Al mismo tiempo se requieren nuevas normas que precisen cómo se debe obtener, conservar e incorporar la prueba digital al proceso, ya que contiene especialidades, a las que el derecho no se había tenido que enfrentar nunca antes.

[1]Van Dijk, J., 2006. *The network society: Social aspects of new media,* Sage Publications Ltd, London, 2006, p.2.

1.2. Objetivo

El propósito de este trabajo es el de enmarcar el concepto de *ciberdelincuencia* y realizar un análisis, a fondo, de todo aquello que incumbe a la prueba digital en el proceso penal, basado en la normativa vigente y normativa que actualmente se encuentra en fase de aprobación, así como de la jurisprudencia clave que realiza aportaciones relevantes sobre esta materia. Se profundiza en aquellas características que otorgan singularidad a la prueba digital frente a la prueba convencional, para destacar así su especialidad y su complejo tratamiento en un proceso penal.

Todo ello, favorecerá la formación conclusiones acerca de si el actual marco jurídico se encuentra adaptado a esta nueva y especial realidad, o bien, si es necesario seguir actualizándolo para que los sujetos encargados de las investigaciones y enjuiciamientos de los delitos informáticos conozcan perfectamente cómo se tienen que tratar las pruebas digitales.

1.3. Metodología

La metodología llevada a cabo en este trabajo consiste en primer lugar en efectuar un profundo análisis de diferentes fuentes, entre ellas: libros, artículos de revistas, estudios llevados a cabo por diferentes sujetos, así como de datos estadísticos sobre la *ciberdelincuencia*.

En segundo lugar, se ha indagado, desde un punto de vista jurídico, en la normativa esencial en esta materia, tanto nacional como europea. No solo se ha acudido a la que está en vigor, sino también a aquella que ha sido propuesta y está pendiente de ser aprobada por el poder legislativo

Además, se ha acudido a ciertas aportaciones jurisprudenciales consideradas más relevantes del Tribunal Supremo y del Tribunal Constitucional.

Por último, se ha realizado una entrevista con el capitán del Grupo de Ciberterrorismo de la Guardia Civil, con amplia experiencia en el Grupo de Delitos Tecnológicos.

1.4. Estructura

Este trabajo está enfocado en hacer un análisis, no solo del crecimiento de la ciberdelincuencia y sus efectos, sino de todos los recursos y mecanismos, a nivel jurídico, con los que el Estado español cuenta para la lucha e investigación de este tipo de delitos. Para llevar a cabo dichos propósitos, en primer lugar, se explica el concepto de *ciberdelincuencia*, dando paso a continuación a la descripción de los distintos tipos de *ciberdelincuencia* existentes. Posteriormente se mostrarán diferentes datos estadísticos de la evolución de los delitos informáticos en España.

En segundo lugar, se analiza la legislación y jurisprudencia clave en este asunto, tanto a nivel europeo como nacional. A continuación, se expondrán algunos de los sujetos más relevantes encargados de perseguir, de investigar y de obtener las pruebas de los *ciberdelitos*.

Por último, el trabajo se centra en aspectos relevantes y relativos a la prueba digital a lo largo del proceso desde su obtención hasta la valoración en juicio. Se tratan especialmente las singularidades de este tipo de pruebas que no se encuentran en las pruebas convencionales y la forma con la que se tienen que tratar para asegurar las garantías que tienen que imperar en todo proceso penal.

2. LA CIBERDELINCUENCIA

2.1 Concepto

En el código penal español no podemos encontrar una definición de *ciberdelincuencia*; de hecho, no hay una definición única. Por lo tanto, en este trabajo se emplea la definición que acoge la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC)[2], que incluye elementos en común con las definiciones que existen sobre la *ciberdelincuencia*; "la *ciberdelincuencia* es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito".

Uno de los sinónimos mas utilizado es el de: delito informático, definido por la Real Academia Española[3](RAE) como: "Infracción penal cometida utilizando un medio o un instrumento informático".

Como se puede extraer de estas definiciones, nos encontramos ante un concepto muy extenso, de modo abierto y ampliable para recoger futuros delitos que surjan a la luz del creciente mundo de las nuevas tecnologías.

2.2 Tipos de ciberdelincuencia

El concepto de ciberdelincuencia destaca por su generalidad, por ello, ha sido necesario realizar una clasificación en función de los diferentes tipos de ciberdelitos existentes en la actualidad. En el presente trabajo, se explica la diferencia entre la ciberdelincuencia pura y la ciberdelincuencia clásica. Esta clasificación, acogida por VELASCO NÚÑEZ[4], aboga por un concepto amplio del *ciberdelito* al recoger tanto delitos antiguos, como delitos nuevos.

[2]Página web de UNODC:https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html. Consultada el 06/11/2021.
[3]Diccionario de la Real Academia Española, DPEJ, Definición de delito informático, Diccionario de la Real Academia Española, 2021, (disponible en: https://dpej.rae.es/lema/delito-inform%C3%A1tico). Consultada el: 06/11/2021.
[4]*Cfr*., Velasco Núñez, E., *Delitos cometidos a través de Internet. Cuestiones Procesales*, La Ley-Actualidad, Madrid, 2010.

2.2.1 Ciberdelincuencia pura o contra la seguridad

Es definida por la INTERPOL como los "delitos contra ordenadores y sistemas de información en los que el objetivo es acceder sin autorización a un dispositivo o denegar el acceso a un usuario legítimo (típicamente mediante el uso de software malicioso)"[5]. Como se puede extraer de esta definición, son ataques directos contra los dispositivos informáticos.

2.2.2 Ciberdelincuencia clásica

Como su propio nombre indica, aquí nos encontramos con aquellas actividades que se cometen a través de un instrumento digital para llevar a cabo un delito clásico, en los que se atenta contra toda clase de bienes jurídicos, entre ellos destacan: los delitos económico-patrimoniales (estafas, blanqueo de capitales, falsedad documental), delitos contra la intimidad (*hacking*, *sexting*, *ciberbullying*…) y delitos contra la libertad como serían las amenazas y las coacciones[6].

2.3 El estado de la ciberdelincuencia en España

2.3.1 Datos y análisis sobre el incremento de la ciberdelincuencia

Tal y como muestra uno de los estudios más exhaustivo[7] sobre el uso de las redes y de los dispositivos electrónicos realizado por la plataforma Hootsuite, del 2020 al 2021, 93 millones de personas en todo el mundo se han vuelto usuarias de un teléfono propio, de las cuales 323.000 son españolas.

316 millones de personas se han convertido en usuarias de internet en este último año, de las cuales, 144.000 son españolas. Estos datos indican que la digitalización sigue aumentando, sin duda alguna, de forma veloz y exponencial y, a mayor digitalización mayor ciberdelincuencia.

---

[5]Secretaria general INTERPOL, *Resumen: Estrategia mundial contra la ciberdelincuenica*, Lyon, 2017.
[6]*Cfr*., Página web de UNIR, Ciberdelincuencia: *¿Qué es y cuáles son los ciberdelitos más comunes?* Disponible en: https://www.unir.net/derecho/revista/que-es-ciberdelincuencia/. Consultada: 08/11/2021.
[7]Kemp S., "The Global State of Digital 2021; Spain report", *Kepios*, 2021(disponible en https://www.hootsuite.com/es/pages/digital-trends-2021). Consultado 27/10/2021.

Es importante destacar el gran efecto que ha tenido la pandemia ocasionada por la COVID19 en este asunto. En palabras de Jürgen Stock, secretario general de INTERPOL: "Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada por la COVID-19"[8]. El confinamiento ha sido el caldo de cultivo ideal para que los ciberdelincuentes desarrollen su actividad, ya que se hizo un uso mucho más acusado de lo normal de la tecnología, por ser durante meses la vía de comunicación más empleada.

Según el estudio sobre la *cibercriminalidad* en España llevado a cabo por el Ministerio del Interior[9], hubo un aumento de 69.661 casos de ciberdelincuencia entre 2019 y 2020. El total de este tipo de delitos cometido en 2020 fue de 287.953, de los cuales el 89,6% fueron fraudes informáticos. Respecto a ello el 14% del total fueron esclarecidos en 2020 y, se llevaron a cabo 11.280 detenciones.

Además, a lo largo de la entrevista realizada con el Grupo de ciberterrorismo de la Guardia Civil[10] se formuló la pregunta acerca de si era evidente desde sus puestos de trabajo este incremento mostrado por las estadísticas. La respuesta fue una rotunda afirmación, a lo que se añadió el dato de un incremento del 500% del volumen de casos relacionados con delitos contra menores como, por ejemplo, la explotación sexual infantil durante las primeras semanas[11] de confinamiento debido a la pandemia de la COVID-19. El motivo principal de esta importante subida se produjo debido al aumento en el uso de dispositivos electrónicos por parte de menores sin supervisión parental.

Una vez pasado el periodo de estricto confinamiento, a juicio de la percepción del entrevistado, estas cifras descendieron hasta su normalización.

---

[8]Página web Interpol: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19. Consultado: 27/10/2021.

[9]Dirección general de coordinación y estudios secretaría de estado de seguridad, "Estudio sobre la cibercriminalidad en España", *Ministerio del interior; Secretaría general técnica* , 2020 (disponible en http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3). Consultado: 27/10/2021.

[10]Guardia Civil, entrevista personal con toma de notas, 24 de marzo de 2022.

[11]El confinamiento comienza en España el 15 de marzo de 2020, momento en que entra en vigor el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19.

Como se puede extraer de estas cifras, la persecución es compleja, acarreando con ello una elevada dificultad a la hora de hallar a los delincuentes, siendo uno de los motivos principales de este resultado, las dificultades de investigación y la obtención de pruebas.

Tal y como afirma el Consejo Europeo, esta tendencia seguirá agravándose en el futuro, ya que se espera que 22.300 millones de dispositivos en todo el mundo estén conectados a internet de aquí a 2024[12].

3. NORMATIVA APLICABLE EN MATERIA DE CIBERSEGURIDAD

3.1 Reglamento (UE) 2019/881 del PE y del Consejo de 17 de abril 2019

Este reglamento relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), que tal y como establece el artículo 1 de dicho reglamento, es "un centro de conocimientos técnicos sobre ciberseguridad"[13] es el encargado de regular todo lo que incumbe a dicha agencia. ENISA es un elemento esencial a la hora de enfrentarse a la ciberdelincuencia, por ser una de sus funciones la de asesorar a los Estados miembros, así como a las instituciones, órganos y organismos en esta materia.

En otras palabras, dado que los delitos informáticos constituyen una sección muy técnica, que requiere de un conocimiento amplio de la informática, esta agencia es la que asesora a nivel europeo como especialista informática de la ciberdelincuencia. De hecho, no solo asesora, sino que "fomenta la cooperación, en particular el intercambio de información, y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos"[14], asunto imprescindible para una lucha eficaz contra la ciberdelincuencia.

[12]Consejo Europeo, "Ciberseguridad: cómo combate la UE las amenazas cibernéticas, Consejo Europeo, 2021 (disponible en https://www.consilium.europa.eu/es/policies/cybersecurity/). Consultado 28/10/2021.
[13]Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (DOUE» núm. 151, de 7 de junio de 2019, pág.20).
[14]Reglamento (UE) 2019/881 de 17 de abril de 2019, relativo a ENISA, pág.4.

Si que es cierto, que dicho reglamento contribuye a la ejecución del derecho de la Unión, a la investigación a la cooperación, en cambio, no incluye ningún aspecto de carácter procesal a la hora de enfrentarse a un delito informático. Es decir, que el reglamento y, por ende, la agencia resultan muy útiles para fomentar la seguridad frente a la ciberdelincuencia, pero no para unificar a nivel europeo la forma de afrontar la delincuencia informática y un proceso garantista de obtención de pruebas.

3.2 Directiva UE 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016

En la propia exposición de motivos de la Directiva UE 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 se destaca que "a fin de alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información, cada Estado miembro debe disponer de una estrategia nacional de seguridad de las redes y sistemas de información que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar"[15]. Esto es lo que dicha norma pretende conseguir a través de una serie de pautas que los Estados miembros deben cumplir. Entre ellas, destaca la estrategia nacional de seguridad de las redes y sistemas de información que los Estados deben tener, establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales y, a su vez, crea una red de equipos de respuesta a incidentes de seguridad informática, denominada CSRIT[16]. Por consiguiente, estos requisitos que se exigen a los Estados miembros promueven el aumento de la ciberseguridad, a la vez que facilitan la investigación, detección y el enjuiciamiento de los delitos.

Dicha directiva es traspuesta en España a través del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que preserva la literalidad de la directiva, aunque incluye la novedad de ampliar el ámbito de aplicación a otros sectores que no son contemplados por la Directiva con el objetivo de hacer el real decreto ley más global. Se extiende su aplicación a las entidades que prestan servicios

[15]Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DOUE» núm. 194, de 19 de julio de 2016, pág.5).
[16]Directiva (UE) 2016/1148 de 6 de julio de 2016, pág.12.

esenciales y dependen de las redes y sistemas de información, así como a los proveedores de determinados servicios digitales[17].

Por lo tanto, ambas normas, tanto la Directiva UE 2016/1148 como el Reglamento UE 2019/881, impulsan a nivel europeo y nacional la seguridad de los sistemas informáticos y la investigación en caso de infracción penal, pero no se contempla en ellas ninguna referencia a la forma de investigar o tratar las pruebas de un delito informático. Simplemente son normas cuyo enfoque principal es la ciberseguridad.

4. SUJETOS ENCARGADOS DE INVESTIGAR Y PREVENIR LA *CIBERDELINCUENCIA*

Dentro del proceso de persecución de un delito informático resulta esencial la figura de aquellos sujetos encargados de perseguirlos, no solo para luchar contra ellos, sino para conseguir todas las pruebas pertinentes para el posterior juicio.

Resulta necesario que se trate de sujetos especializados en la materia, debido a las evidentes dificultades que se presentan a la hora de investigar un delito de esta índole, como es la dificultad de descubrimiento del delincuente (por encontrarse protegido por sistemas informáticos complejos y usuarios falsos) lo que conlleva a la dificultad de persecución.

4.1 Ámbito Europeo

4.1.1 Centro Europeo de la Ciberdelincuencia

En 2013, debido a las alarmantes cifras de aumento de la ciberdelincuencia y su previsión de patente crecimiento, la Unión Europea se vio en la necesidad de crear el Centro Europeo de la Ciberdelincuencia. Se trata de una organización perteneciente a la sede de Europol, cuya principal misión es la de prestar apoyo operativo a los países de la UE y aportar conocimientos técnicos, analíticos y de peritaje forense de alto nivel en el marco de investigaciones conjuntas[18].

[17] *Cfr*., Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información («BOE» núm. 218, de 08/09/2018, página 1).
[18] *Cfr*., Página web Comisión Europea, nota de prensa. (Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_13_13). Consultado: 4/11/2021.

Este centro, que, en España coopera mano a mano con el Cuerpo Nacional de Policía, es el punto de coordinación de la persecución de la ciberdelincuencia en la Unión. Este cometido es fundamental debido al carácter transfronterizo de este tipo de delitos.

4.2 A nivel nacional

4.2.1 Instituto Nacional de Ciberseguridad (INCIBE)

INCIBE depende del Ministerio de Asuntos Económicos y Transformación Digital. Su principal actividad consiste en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, sobre todo en aquellos incidentes con operadores críticos[19]. Se podrían comparar sus tareas a la de ENISA, anteriormente citada, por ser la encargada a nivel nacional de asesorar a empresas y particulares sobre la ciberseguridad, combinando estas tareas con las de seguimiento constante de la evolución de la ciberdelincuencia.

De esta forma, se consigue ir adaptando los mecanismos nacionales de detección y persecución a los sucesivos cambios de esta nueva forma de delinquir, consiguiendo así una mayor ciberseguridad a nivel nacional.

4.2.2 Fuerzas y cuerpos de seguridad del Estado

En primer lugar, la Brigada Central de Investigación Tecnológica (BCIT) pertenece a la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía (CNP). Entre sus funciones, cabe destacar para el interés de este trabajo: llevar a cabo las investigaciones de los delitos informáticos más complejos, incluidos aquellos que tengan su origen en países transfronterizos y, por supuesto, la obtención de las pruebas digitales pertinentes para posteriormente, ponerlas a disposición judicial.[20]

[19]Página web INCIBE: https://www.incibe.es/que-es-incibe- Consultada en 4/11/2021.
[20]*Cfr.*, Página web Policía Nacional: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php. Consultada en: 5/11/2021.

En segundo lugar, el Grupo de Delitos Telemáticos (GDT) de la Guardia Civil, que se sitúa dentro de la Unidad Central Operativa de la Guardia Civil. Sus funciones son muy similares a las que realiza el grupo del CNP, como la investigación y la obtención de pruebas. Una de las investigaciones y consecuente detención, de mayor repercusión social mediática, fue llevada a cabo por este grupo: Operación Lupin. En ella se detuvo a uno de los mayores ciberdelincuentes españoles, en el marco de una investigación relativa a la estafa a través de internet[21].

4.2.3 Instrucción N.º 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías.

A nivel judicial, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, concretamente en el Libro I, en el que se regula la extensión de la jurisdicción y la organización de los juzgados y tribunales, no se contempla ningún Juzgado especializado en los delitos informáticos, sino que son los ya contemplados como los Juzgados de lo Penal los encargados de conocer de estos asuntos.

En cambio, la Fiscalía General del Estado sí ha creado Secciones de Criminalidad Informática, ya que, como exponen los propios fundamentos de la instrucción nº 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías: "el área de especialización en criminalidad informática surge como una necesidad constatada en la practica habitual de las Fiscalías al haberse detectado un progresivo aumento en el número de investigaciones criminales vinculadas a la utilización de las nuevas tecnologías y más específicamente de internet, como red de redes"[22].

Entre las funciones que las Secciones Territoriales de Criminalidad Informática desarrollan, cabe destacar que deben cumplir con los criterios de actuación establecidos en materia de criminalidad Informática por la Fiscalía General del Estado, procurar el

[21]López-Fonseca, O., Detenido el mayor ciberestafador de España, El País, 5 de julio de 2019. (Disponible en: https://elpais.com/politica/2019/07/04/actualidad/1562264274_472850.html). Consultada 11/11/2021.
[22]Instrucción nº 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías.

adecuado control estadístico de este tipo de procedimientos judiciales, colaborar con las unidades especializadas de las Fuerzas y Cuerpos de Seguridad del Estado, así como elaborar anualmente un informe sobre los problemas jurídico técnicos detectados en este ámbito[23].

Desde un punto de vista práctico, el capitán del Grupo de ciberterrorismo de la Guardia Civil[24] asegura el importante papel de los fiscales especializados en criminalidad informática, ya que su contribución en los procesos judiciales resulta muy apropiada y valiosa para ampliar los conocimientos de los que podría carecer el juez en materia técnica informática.

5. PRUEBAS ELECTRÓNICAS

5.1 Concepto

En primer lugar, resulta conveniente especificar que en la práctica jurídica y doctrinal se emplean múltiples sinónimos del concepto "prueba electrónica". Destacan, por ser los más empleados, los siguientes: prueba digital, prueba informática y prueba por medios reproductivos.

La primera aproximación normativa relativa al concepto de la prueba electrónica surge en el ámbito civil, concretamente con la Ley 59/2003, de 19 de diciembre, de Firma Electrónica posteriormente derogada por la Ley 56/2007. Tal y como establecía el artículo 3.5 de dicha ley: "Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado"[25].

[23] *Cfr*., Instrucción no 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías, cit.
[24] Guardia Civil, comunicación personal con toma de notas, 24 de marzo de 2022.
[25] Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE núm. 304, de 20/12/2003).

En cambio, en la normativa correspondiente al Derecho Procesal difícilmente se puede encontrar una definición clara y específica de prueba electrónica. Por ello, a efectos de este trabajo, se va a emplear la definición llevada a cabo por DELGADO MARTÍN[26]: "toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio", junto con la de CRESPO SANCHIS[27]: "a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto ateniendo a una norma legal". La unión de estas dos definiciones muestra una visión completa del concepto de prueba electrónica.

Como se puede extraer de esta definición se trata de cualquier tipo de información (vídeos, mensajes de texto, mensajes de voz, fotografías), incluida o transferida a través de cualquier medio, electrónico, definido por el DPEJ de la RAE[28] como: "Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía fija y móvil u otras". Más ejemplos de ello serían: el teléfono, ordenador, pantallas de coche, relojes inteligentes, redes sociales, etc. Es decir que las pruebas digitales son la consecuencia directa de que exista la ciberdelincuencia.

5.2 Acceso transfronterizo

Existen dos problemas principales que incumben a las pruebas digitales. La primera, consiste en la facilidad existente de poder falsificar o manipular estas pruebas debido a los medios en los que se crean, almacenan y envían. En ciertos casos las pruebas se encuentran en perfiles personales de redes sociales o en otro tipo de aplicaciones cuya accesibilidad es fácil y su contenido sencillo de manipular. Por otro lado, hay ocasiones en las que las pruebas digitales no se encuentran almacenadas en España, sino que se hallan en los centros de datos de las empresas situados en otras jurisdicciones. Como

[26]Delgado Martín, J., *La prueba digital. Concepto, clases y aportación al proceso*, Diario La Ley, Nº 6, Sección Ciberderecho, Editorial Wolters Kluwer, 11 de abril de 2017, p.1.
[27]Sanchis Crespo, C., Las Tecnologíass de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio, Thomson Reuters Aranzadi, Navarra, 2012, p.713.
[28]Diccionario de la Real Academia Española, DPEJ, Definición de medio electrónico, Diccionario de la Real Academia Española, 2021. (Disponible en: https://dpej.rae.es/lema/medio-electr%C3%B3nico) Consultada: 18/11/2021.

ejemplo práctico, los servidores de WhatsApp se encuentran en Dublín[29] mientras que los de Apple se encuentran en Estados Unidos[30].

La consecuencia directa de ello es la abundante lentitud y complejidad del proceso de obtención de las pruebas digitales. Además, sin unos procedimientos reglados de obtención y conservación de pruebas electrónicas, se crea el riesgo de que surjan muchas situaciones de inseguridad jurídica. La seguridad jurídica no es solo un derecho fundamental sino un principio del Estado de Derecho y, por ende, del proceso judicial. Asenta el Tribunal Constitucional[31] que "*implica que el legislador debe perseguir la claridad y no la confusión normativa, debe procurar que acerca de la materia sobre la que legisle sepan los operadores jurídicos y los ciudadanos a qué atenerse, y debe huir de provocar situaciones objetivamente confusas (...)*".

Por ello, es necesaria una regulación clara y coordinada, que indique el proceso de obtención y conservación de las pruebas digitales, por ser estas de naturaleza completamente distinta a las pruebas tradicionales que forman habitualmente parte del proceso penal.

Con una regulación de esta índole, se asegura que los derechos de las partes del proceso no están siendo vulnerados, como, por ejemplo, la protección de datos personales y, a su vez que las pruebas se están integrando en el proceso con las garantías de que no han sido falsificadas, manipuladas o viciadas.

Por otro lado, al existir normas internacionales y claras en esta materia, los proveedores de servicios sabrían a qué consecuencias se atienen en caso de incumplirlas, y los procedimientos que deben de llevar a cabo para tratar y remitir las pruebas a las autoridades competentes.

---

[29] *Cfr.*, Página web: Cliatec 360 Data Center. (Disponible en https://cliatec.com/whatsapp-y-centro-de-datos-infraestructuras-boton-enviar/). Consultada: 18/11/2021.

[30] *Cfr.*, Apple, Outside US Legal Process Guidelines. (Disponible en https://images.apple.com/legal/privacy/law-enforcement-guidelines-outside-us-es.pdf). Consultada:18/11/2021.

[31] Sentencia del Tribunal Constitucional de 15 de marzo 46/1990, La Ley 1458-TC/1990, FJ 5.

5.2.1 Normas propuestas y en fase de aprobación en la UE

La Unión Europea parece ser consciente del problema que acarrea el acceso transfronterizo al haber propuesto a nivel europeo una serie de normativas con el objetivo de paliar las consecuencias de que las pruebas digitales se encuentren en distintos Estados Miembros, promoviendo así la agilización y sencillez del proceso. Dichas propuestas van a ser presentadas a continuación.

5.2.1.1 Directiva DEL PARLAMENTO EUROPEO Y DEL CONSEJO por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales 2018/0107 (COD)

La propuesta de la Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, resulta de vital importancia para la evolución y adaptación del derecho a la realidad social. De su propio título se puede extraer la creación de la nueva figura del representante legal de los proveedores de servicios.

La razón de ser de la Directiva es la de crear una mayor libertad, seguridad y justicia[32]. Reflejan los fundamentos de la Directiva propuesta la incertidumbre que existe por parte de las autoridades de los Estados Miembros, a la hora de tener que solicitar una prueba digital, debido a que, en numerosas ocasiones, no se sabe a quien se debe dirigir la orden. Este problema cesa con la figura del representante, ya que seria el encargado de "recibir, cumplir y hacer cumplir las decisiones dirigidas a recabar pruebas emitidas por las autoridades nacionales competentes en procesos penales"[33].

Será la obligación de los proveedores de servicios de la UE, la de designar a su representante legal en la UE, entendiendo por proveedor de servicio en este contexto "proveedores de servicios de comunicaciones electrónicas; proveedores de servicios de la sociedad de la información que almacenen datos como parte del servicio prestado al

[32] *Cfr.*, Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales COM/2018/226 final - 2018/0107 (COD) (EURLEX documento 52018PC0226, pág. 4).
[33] Propuesta de Directiva por la que se establecen normas armonizadas … COM/2018/226 final - 2018/0107 (COD), pág. 4.

usuario, incluidas las redes sociales, los mercados en línea y otros proveedores de servicios de alojamiento de datos; y proveedores de servicios de asignación de nombres y números en internet"[34].

El incumplimiento de la obligación implicará la imposición de una sanción al Proveedor de Servicios correspondiente.

Las principales tareas que los representantes deberán de llevar a cabo serán las de acatar los requerimientos de los jueces o fiscales, aportar los datos que se le soliciten en el marco del proceso penal y la adopción de medidas para la conservación de los datos en el proceso penal[35].

En el momento en que esta Directiva entre en vigor en los Estados miembros será de gran utilidad para los procesos penales relacionados con delitos informáticos. El hecho de obligar a los proveedores de servicios a contar con un representante legal en la UE facilitará enormemente la persecución y enjuiciamiento de estos delitos, permitiendo que las pruebas puedan ser recabadas en un tiempo inferior al que se necesita actualmente. Además, existirá una seguridad jurídica mayor, ya que las partes y las autoridades conocerán exactamente los pasos que se tienen que llevar a cabo para recabar las pruebas con todas las garantías pertinentes.

En cambio, el proceso legislativo se está extendiendo excesivamente en el tiempo, ya que la propuesta fue impulsada por la Comisión Europea el 18 de abril de 2018 y el último avance que se realizó fue el 12 de marzo de 2019 cuando la propuesta fue discutida en el Consejo de la Unión Europea[36]. Es decir, que la propuesta se encuentra paralizada desde hace tres años.

[34]Propuesta de Directiva por la que se establecen normas armonizadas … COM/2018/226 final - 2018/0107 (COD), pág. 8.
[35]*Cfr*., Propuesta de Directiva por la que se establecen normas armonizadas … COM/2018/226 final - 2018/0107 (COD), pág. 8.
[36]*Cfr*., Página web de Eur-Lex. Disponible en: https://eur-lex.europa.eu/procedure/EN/2018_107. Consultada en: 25/02/2022.

5.2.1.2 Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal 2018/0108 (COD)

Estrechamente vinculado con la Directiva (2018/0107/COD), surge la propuesta del Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal. La razón de ser de esta norma coincide con la de la Directiva, ya que ambas buscan el mismo objetivo, consistente en la agilización de la obtención de la prueba digital, asegurando a su vez que no se vulnere ninguna de las garantías procesales.

Una de las facilidades que surgen en este Reglamento, consiste en evitar que una autoridad del estado en el que esté establecido el destinatario de la orden tenga que intervenir en la ejecución y notificación de la misma[37], por el contrario, la orden, cuya emisión deberá ser supervisada por una autoridad judicial[38], será directamente dirigida al proveedor de servicio, o en su caso al representante del mismo.

Como se puede extraer de lo anterior, el propio Reglamento hace expresa mención de la figura del representante de proveedores de servicios, por lo que la Directiva y el Reglamento propuestos son regulaciones que claramente se complementan. Con ambos instrumentos normativos se consigue una mayor cooperación europea en el ámbito de los procesos penales, cuyo impacto directo es la mayor facilidad y eficacia en la persecución de delitos informáticos, así como un incremento en la seguridad jurídica para todas las partes del proceso judicial.

En el artículo 9 del Reglamento, se fijan unos plazos para que se cumpla la orden de entrega. El plazo normal será de 10 días, aunque en situaciones de urgencia, definidas como "situaciones en las que exista una amenaza inminente para la vida o la integridad

[37] *Cfr.*, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, COM/2018/225 final - 2018/0108 (COD), (EURLEX documento 52018PC0225, pág. 6).

[38] *Cfr.*, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega..., art. 55, pág. 38.

física de una persona o para una infraestructura crítica, el plazo será de 6 horas"[39]. Las disposiciones del reglamento están enfocadas a diseñar una estructura completa de las ordenes de entrega y conservación, determinando tanto el contendido mínimo, el proceso de elaboración y de ejecución como las consecuencias en caso de incumplimiento. Cabe destacar que estas órdenes solo son susceptibles de ser emitidas para obtener datos que ya se encuentran almacenados y en investigaciones o procesos penales para infracciones específicas[40]. Estas son las "infracciones penales punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años, o para delitos específicos a que se refiere la propuesta y cuando exista un vínculo específico con herramientas electrónicas y delitos cubiertos por la Directiva sobre terrorismo (UE) 2017/54"[41].

Esta regla engloba muchos de nuestros delitos, que a su vez son punibles con las penas nombradas en otros estados. En cambio, no todos los delitos tipificados son los mismos y con las mismas penas en los 27 Estados que forman la UE, por lo tanto, se sigue corriendo el riesgo de que haya investigaciones penales que no se puedan llevar al cabo de la forma más completa posible por no ser posible solicitar las pruebas digitales.

Para homogeneizar el proceso en todos los Estados Miembros y que sea más sencillo gestionar las órdenes de entrega y conservación de pruebas electrónicas, se unen al Reglamento tres modelos normalizados diferentes: un certificado de orden europea de entrega, un certificado de orden europea de conservación y un documento sobre la imposibilidad de ejecutar alguna de las órdenes anteriores.

En cambio, este Reglamento, que fue propuesto el 18 de abril de 2018 por la Comisión Europea, sigue sin haber llegado a la fase de primera lectura en el Parlamento de la UE[42]. Es decir, al igual que con la Directiva 2018/0108, el procedimiento legislativo se está extendiendo de forma prolongada en el tiempo.

---

[39]Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas ..., art. 9, pág. 9.
[40]*Cfr.*, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas ..., art. 24, pág. 32.
[41] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación..., pág. 5.
[42]Página web de Eur-Lex. Disponible en: https://eur-lex.europa.eu/legal-content/ES/HIS/?uri=COM:2018:0225:FIN. Consultada en: 25/02/2022.

Tras la entrevista llevada a cabo con el Grupo de ciberterrorismo de la Guardia Civil[43], se destaca la lentitud del proceso actual de órdenes de entrega y conservación de las pruebas digitales. El entrevistado se refiere a la necesaria rapidez en la vía judicial para este tipo de delitos en los que en abundantes ocasiones se está atentando contra la integridad de un menor. Es decir, que actualmente se requiere de mecanismos más rápidos para solventar esto cuanto antes. Actualmente se requieren de muchos pasos intermedios que complican la situación y, por ello resulta mucho más práctica y eficaz la cooperación policial internacional que la judicial. Además, en esta entrevista se nos informa de la duración aproximada de las comisiones rogatorias. El entrevistado aporta el dato acerca de la duración de las comisiones rogatorias internacionales para la obtención de datos, las cuales tardan aproximadamente un periodo de seis a veinticuatro meses.

5.2.2 Negociaciones internacionales sobre el acceso transfronterizo de las pruebas electrónicas

Los dos instrumentos expuestos en los subapartados directamente anteriores han sido diseñados para ser aplicados dentro de la UE. Sí que es cierto, que para aquellos servidores de almacenamiento de información que, a pesar de no tener un establecimiento en la Unión, les serán de aplicación ambas normativas en el momento que tengan un vínculo sustancial, es decir cuando tengan un número significativo de usuarios en uno o más estados miembros[44]. A pesar de que en la Directiva y en el Reglamento, no se exprese de forma clara cuantos usuarios son "un número significativo", se amplía mucho el rango de aplicación de la misma. En cambio, puede surgir el caso en el cual se tenga que obtener una prueba digital de unos servidores que no se encuentren localizados en la UE, es decir, que no exista ninguna representación de los mismos a la que acudir para solicitar datos, por encontrarse fuera de las fronteras de la misma.

Para afrontar casos de esta naturaleza, se están intentando diseñar dos nuevos instrumentos jurídicos: El Acuerdo UE-EE. UU sobre el acceso transfronterizo de las pruebas electrónicas y el segundo protocolo adicional al Convenio de Budapest sobre Ciberdelincuencia.

[43]Guardia Civil, comunicación personal con toma de notas, 24 de marzo de 2022.
[44]Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación ..., pág. 9.

5.2.2.1 Acuerdo UE-EE. UU sobre el acceso transfronterizo de las pruebas electrónicas

El 27 de mayo de 2019, el Consejo de la Unión Europea publicó una Decisión por la cual se habilitó a la Comisión Europea para llevar a cabo negociaciones con Estados Unidos (EE. UU), y desarrollar así un Acuerdo entre la Unión Europea y los EE. UU sobre el acceso transfronterizo a pruebas electrónicas para la cooperación judicial en materia penal[45].

Dichas negociaciones siguen en proceso[46] y por ello, actualmente, no se ha logrado formalizar el Acuerdo. En la Decisión por la que se autoriza la negociación, se deja una amplia libertad a la hora de realizar las negociaciones, ya que no se establece una guía compleja acerca de cómo llevarlas a cabo. Únicamente se establece el objetivo principal del Acuerdo, ya expresado en su propio título. La parte más extensa del documento muestra la preocupación por parte de la Unión de que, en todo caso, el futuro Acuerdo sea conforme a la Carta de Derechos Fundamentales de la Unión Europea, haciendo especial hincapié al derecho a la intimidad y a la protección de datos personales[47].

5.2.2.2 Propuesta del Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas.

El Convenio sobre la ciberdelincuencia aprobado en Budapest el 23 de noviembre de 2001, conocido como el Convenio de Budapest, introdujo, por primera vez, la idea de cooperar internacionalmente para la persecución de los delitos cometidos a través de los medios informáticos[48]. Actualmente el Convenio ya ha sido ratificado por 66 Estados, entre ellos se encuentran España desde 2010 y Estados Unidos desde 2006[49]. Para estos

[45] *Cfr.*, Recomendación de Decisión del Consejo por la que se autoriza la apertura de negociaciones para un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en materia penal COM/2019/70 final (EURLEX, documento 52019PC0070, pág.1).
[46] *Cfr.*, Página web Consejo de la UE. (Disponible en: https://www.consilium.europa.eu/es/policies/e-evidence/). Consultada en: 25/02/2022.
[47] Recomendación de Decisión del Consejo por la que se autoriza la apertura de negociaciones …, pág.3.
[48] *Cfr.*, Instrumento de ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, (BOE, núm. 226, de 17 de septiembre de 2010, pág. 2).
[49] *Cfr.*, Página web del Consejo de Europa, (disponible en: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185). Consultado el 28 de noviembre de 2021.

países, el Convenio ha servido como una guía fundamental a la hora de adaptar la legislación nacional a la lucha contra la ciberdelincuencia.

A través del Convenio, se establecen múltiples medidas, entre ellas, sobre derecho material para la tipificación de nuevos delitos, sobre sanciones y sobre derecho procesal. Concretamente, sobre el tema que nos concierne, en el artículo 23 se establece que:

"Las Partes cooperarán entre sí en la mayor medida posible, (...), en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos"[50].

Debido a que dicho Convenio empezaba a resultar insuficiente dado el actual auge de la ciberdelincuencia, el 21 de mayo de 2019 se decidió por parte del Consejo de la Unión Europea autorizar a la Comisión Europea a participar en nombre de la UE en las negociaciones sobre un Segundo Protocolo adicional al Convenio de Budapest. En el mismo se propuso incluir disposiciones "*que permitan la cooperación directa con los proveedores de servicios en otras jurisdicciones con respecto a las solicitudes de información de los abonados, de conservación y de los procedimientos de urgencia*"[51].

[50]Instrumento de ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, pág. 13.
[51]*Cfr*., Recomendación de Decisión del Consejo por la que se autoriza la participación en las negociaciones sobre un Segundo Protocolo adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia (STE n.º 185), COM/2019/71 final (Eurlex documento 52019PC0071, pág. 2).

El objetivo es el mismo que para los otros instrumentos ya expuestos, conseguir una mayor cooperación en materia penal, no solo entre los Estados, sino también con el sector privado, agilizar el proceso de obtención de las pruebas digitales, es decir, mejorar todo el aspecto procesal de los procedimientos, aportando una mayor seguridad jurídica al sistema, constituyendo este un ámbito esencial de un Estado de Derecho. Además, se especifica la primacía que tienen los acuerdos ya establecidos entre los Estados Miembros y la normativa europea frente a este futuro protocolo. Es decir, que estos aplicarán las futuras nuevas disposiciones del protocolo adicional en ausencia de normativa existente sobre la materia[52]. Es decir, que resulta aplicable como una segunda fuente de Derecho.

Dentro de la propia propuesta del Protocolo, se establecen dos procedimientos diferentes en función de la cooperación necesaria en cada caso.

El primero de ellos, recogido en la sección 2 del capítulo II[53], va dirigido a la comunicación con proveedores de servicios. En la mencionada sección, se expone la libertad de los Estados para adoptar las medidas legislativas que crean pertinentes para autorizar a sus propias autoridades la emisión de solicitudes a los servidores, así como para aceptar dichas solicitudes. En cambio, se establece de forma específica aquella información que las solicitudes deben contener, como, por ejemplo, la fecha de solicitud, una lista detallada de información la solicitada, la necesidad de la información sobre un procedimiento penal específico, etc.

El segundo de los procedimientos se encuentra en la sección 3ª del mismo capítulo[54] por el cual se establece un procedimiento para mejorar la cooperación entre las autoridades. Tal y como está definido en el proyecto del Protocolo, se refleja esta definición "una autoridad judicial, administrativa u otra autoridad encargada de hacer cumplir la ley que esté facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de medidas en virtud del presente Protocolo con el fin de obtener o presentar pruebas en

[52] *Cfr.*, ADENDA de la Recomendación de Decisión del Consejo por la que se autoriza a la Comisión Europea a participar, en nombre de la Unión Europea, en las negociaciones sobre un Segundo Protocolo adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia (STCE n.º 185), 9296/19, Bruselas, 2019, disponible en (https://data.consilium.europa.eu/doc/document/ST-9664-2019-INIT/es/pdf%20). (Consultado: 29 de noviembre de 2021).
[53] *Cfr.*, Preparación de un Segundo Protocolo adicional al Convenio de Budapest sobre la Ciberdelincuencia, Proyecto de Protocolo, versión 2, pág. 8, art. 6.3, Consejo de Europa, Francia, 2021, disponible en (https://rm.coe.int/0900001680a27dbe). (Consultado: 29 de noviembre de 2021).
[54] *Cfr.*, Preparación de un Segundo Protocolo adicional al Convenio de Budapest, Sección 3ª, pág. 11.

relación con investigaciones o procedimientos penales específicos"[55]. En este caso, se sigue dejando libertad a los estados para adoptar las medidas legislativas pertinentes, no obstante, se añade que además de la información mínima que la orden debe contener, se debe incluir información de apoyo para ayudar a la Parte requerida (autoridad del estado al que se requiere) a dar efecto a la orden. Esta información de apoyo, en ningún caso, será transmitida al proveedor de servicios[56].

A diferencia del primer procedimiento, en el segundo no se coopera directamente entre la autoridad de un Estado y el proveedor de servicios, sino que la cooperación en un proceso penal concreto oscila entre la autoridad de un estado requirente con la autoridad del estado requerido. Para garantizar que el proceso siga haciéndose en un plazo de tiempo razonado y cumplir así el objetivo de agilizar la obtención de pruebas transfronterizas, en el proyecto de Protocolo se establece un plazo de 45 días para que la parte requerida notifique al proveedor de servicios la orden de obtención de los datos de tráfico. El proveedor de servicios dispondrá de un plazo de otros 45 días para remitirlos.

Cabe destacar que, para este último caso, se contempla en el proyecto de Protocolo un procedimiento para los casos de emergencia. En parte, esto ya venía recogido en el Convenio de Budapest, concretamente en el artículo 35: "Cada parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, como objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones (…)"[57]. Pues bien, el procedimiento de solicitud y emisión es muy similar al anterior, con la salvedad de que es preceptivo razonar la emergencia.

Se puede extraer de lo anterior que, desde una perspectiva internacional, se está trabajando de forma eficiente en formar un sistema completo, eficaz y global que establezca un claro proceso de obtención de pruebas digitales garantizando la protección de los derechos fundamentales. En cambio, según la información aportada por el capitán del Grupo de ciberterrorismo de la Guardia Civil[58], actualmente los procedimientos de

[55]Preparación de un Segundo Protocolo adicional al Convenio de Budapest, art. 3.2b., pág. 6.
[56]*Cfr*., Preparación de un Segundo Protocolo adicional al Convenio de Budapest, pág. 12, art. 8.3b.
[57]Instrumento de ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, pág.7.
[58]Guardia Civil, comunicación personal con toma de notas, 24 de marzo de 2022.

cooperación judicial internacional siguen siendo demasiado complejos, largos y exigentes, por lo que resultan ineficientes.

5.3 Técnicas de investigación específica para la obtención de pruebas electrónicas

Como toda prueba que vaya a formar parte de un proceso judicial, antes de ser incorporada al proceso debe de obtenerse de manera lícita. Tras la obtención de la prueba electrónica, esta debe incorporarse al proceso judicial donde se llevará a cabo su valoración[59].

Como ya ha sido mencionado, las pruebas electrónicas, en función del delito cometido, se pueden constituir en diferentes fuentes de distinta naturaleza. Por ello, en función de la circunstancia en la que la prueba se halle, se tendrá que emplear un medio de obtención u otro.

Por ello, en este apartado del trabajo se explican aquellos mecanismos de obtención de las pruebas digitales que resultan distintos y peculiares en comparación con los mecanismos de obtención de pruebas no digitales. Así, se va a poder observar las especialidades procesales de estos mecanismos de investigación.

5.3.1 Obtención de la dirección de *Internet Protocol* y del número de *International Mobile Equipment Identity*

Los artículos 588 ter. k y ter. l del Real Decreto de 14 de septiembre de 1882 por el que se aprueba la LECrim[60], contemplan la posibilidad de que los agentes de la Policía Judicial tengan acceso a una dirección IP o IMEI.

En primer lugar, una dirección IP "es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa "protocolo de Internet", que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local"[61]. Es

[59] *Cfr*. Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer, Madrid, 2018, p.43.
[60] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (BOE 31/03/2015).
[61] Página web de Kaspersky, (disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address). Consultada: 20/12/2021.

decir, que cada teléfono y cada ordenador poseen su número de identificación propio, siendo esto de gran utilidad para las investigaciones policiales en el marco de un delito concreto. Para ponerlo en contexto, y, a efectos prácticos, si se parte de una situación en la que, por ejemplo, a través de un perfil falso de cualquier red social, supuestamente se ha producido un delito de enaltecimiento del terrorismo recogido en el artículo 578 del Código Penal, sería de vital importancia para dar con el supuesto autor, averiguar desde qué dispositivo o red se ha realizado la comunicación. En este punto entra en juego la dirección IP, ya que proporciona la información sobre el dispositivo o red.

Uno de los rasgos a destacar de la obtención de una dirección IP es la innecesaridad de contar con autorización judicial para recabar la prueba. Defiende el TS en la sentencia del 17 de noviembre de 2011 que la IP es un dato público, siendo consciente el usuario de que al navegar por internet dicha información queda registrada. "*No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada queda registrada siempre y ello lo sabe el interesado*[62] *".* En esta misma sentencia se establece que una vez las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSSEE) han obtenido la IP, sí necesitan de autorización judicial para averiguar los datos de la persona usuaria del dispositivo o red a través de la cual se ha cometido el delito. Esta información se averigua a través de los operadores de internet (i.e. Vodafone, Jazztel, Pepephone, etc.).

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[63] establece cuáles son los datos relacionados con las comunicaciones telefónicas o realizadas a través de internet que los operadores deben conservan. Uno de los objetivos de esta medida es garantizar que las investigaciones de delitos graves puedan llevarse a cabo de forma favorable, esto es gracias a que no se hayan eliminado los datos relativos a los titulares de las redes, así como las fechas y horarios de conexión a diferentes servicios de internet.

[62]Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 17 de noviembre de 2011, 1299/2011, La Ley 246234/2011, ECLI: ES:TS:2011:8595, FJ:5.
[63]Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE 19/10/2007).

En su artículo primero ya se menciona la obligatoriedad de una autorización judicial previa para poder ceder estos datos a las personas encargadas de la investigación[64].

En cambio, tras la entrevista llevada a cabo con la Guardia Civil[65], se puede extraer que en este asunto también es necesario una regulación común y única entre estados, ya que existen ciertas diferencias muy relevantes. Por ejemplo, En Alemania el periodo de conservación de datos asociados a las comunicaciones es de 10 semanas[66], mientras que en España es de 12 meses[67].

A pesar de que este método resulte de gran utilidad para la obtención de pruebas electrónicas, resulta necesario tener en cuenta que *"un atacante malicioso puede aprovechar aquella vulnerabilidad para utilizar el equipo ajeno quedando su uso registrado como si fuera el auténtico titular el que utiliza la IP en esa manipulación del equipo, sin más condición que la de que el equipo del titular verdadero se encuentre encendido. Y ello sin que este titular pueda ni siquiera percatarse de ese uso malicioso y ajeno de su equipo"*[68]. Es en esta sentencia del 3 de diciembre del 2012 en la que se establece la insuficiencia probatoria de una dirección IP para establecer la autoría de un delito.

Es por ello por lo que la dirección IP a pesar de resultar muy útil a la hora de llevar a cabo una investigación penal, no es prueba suficiente para acusar a una persona. Por tanto, resulta necesario complementarla con otro tipo de pruebas para llegar a conclusiones veraces sobre la autoría del delito, como podría ser la aprehensión del dispositivo para examinar su contenido.

[64]Ley 25/2007, de 18 de octubre, de conservación de datos (BOE 19/10/2007), art.1.
[65]Guardia Civil, comunicación personal, 24 de marzo de 2022.
[66]Sánchez R., Alemania almacenará datos telefónicos sistemáticamente durante diez semanas, El Mundo, 27 de mayo de 2015. (Disponible en: https://www.elmundo.es/internacional/2015/05/27/5565ec4ae2704ebc738b4590.html). Consultado: 24/03/2022.
[67]Ley 25/2007, de 18 de octubre, de conservación de datos (BOE 19/10/2007), art 5.
[68]Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 3 de diciembre de 2012, 987/2012, La Ley 195398/2012, ECLI: ES:TS:2012:8316, FJ:3.

En segundo lugar, el número IMEI "sirve para identificar un teléfono móvil que se utiliza en GSM (*Global System for Mobile Communications*) de red"[69]. Se puede observar que es muy parecido a la dirección IP, pero, en este caso, en dispositivos móviles. Así pues, la jurisprudencia[70] ha establecido los mismos requisitos que para obtener la dirección IP, es decir, que para su obtención no se requiere de autorización judicial, por considerarse este número de acceso público y, lo mismo ocurre con el resto de los medios técnicos que sean válidos para identificar el equipo empleado para acceder a la red de telecomunicaciones.

5.3.2 Agente encubierto informático

La figura del agente encubierto informático viene recogida en el articulo 282 bis.6 de la LECrim. En este mismo artículo se detallan las actividades que exclusivamente los funcionarios de la Policía Judicial podrán realizar con la autorización del juez de instrucción. Entre las mismas se incluye "intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido"[71].

A través de este método de investigación *"funcionarios de policía actúan en la clandestinidad, con identidad supuesta y con la finalidad de reprimir o prevenir el delito"*[72]. En cambio, el agente encubierto informático, a diferencia de un agente encubierto que no tenga la especialidad de informático, solo puede ser autorizado por el Juez de Instrucción, nunca por el Ministerio Fiscal.

Para obtener una definición y explicación más precisa y extensa de la que realiza el propio artículo que regula esta figura, resulta esencial traer a colación la sentencia del TS de 29 de diciembre de 2010 en la que se especifica que:

[69]Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 20 de octubre de 2009, 921/2009, La Ley 200570/2009, ECLI: ES:TS:2009:6307, FJ:5.
[70]*Cfr*. Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 22 de junio de 2016, 551/2016, La Ley 74791/2016, ECLI: ES:TS:2016:3062, FJ:2.
[71]LECrim, art. 282 bis. 6.
[72]Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 29 de diciembre de 2010, 1140/2010, LA LEY 226907/2010, ECLI: ES:TS:2010:718, FJ:6.

> *"Agente encubierto, en nuestro ordenamiento será el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operandi, así como obtener pruebas sobre la ejecución de hechos delictivos, debiéndose aclarar que es preciso diferenciar esta figura del funcionario policial que de forma esporádica y aislada y ante un acto delictivo concreto oculta su condición policial para descubrir un delito ya cometido"*[73].

Una de las notas más características de la definición es la limitación del empleo de este método de investigación ya que, solo se permite su uso de forma excepcional y, como indica el artículo 286 bis. 6 de la LECrim, solo para esclarecer algunos delitos concretos recogidos en el apartado 4 del mismo artículo o en el articulo 588 ter a[74]. Entre ellos se encuentran delitos de terrorismo, delitos relativos a la propiedad intelectual e industrial, delitos relativos a la prostitución, etc.

Otro elemento relevante a destacar consiste en que el agente encubierto informático únicamente podrá actuar en canales cerrados de comunicación[75] con la previa autorización judicial. Una de las notas más características de estos canales consiste en que se intercambia información entre personas determinadas o determinables y, por ello, las comunicaciones realizadas se encuentran afectadas por el secreto de las comunicaciones[76].

En cambio, para los canales abiertos y/o públicos, los miembros de las FFCCSSEE cuentan con el respaldo del artículo 11 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad[77] por el que, para la prevención de la comisión de actos delictivos, así como para su investigación, los funcionarios podrán realizar mediante el

[73]Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 29 de diciembre de 2010, FJ:6, cit.
[74]LECrim, art. 282 bis. 6.
[75]LECrim, art. 282 bis. 6.
[76]*Cfr*. Delgado Martín, J., "*Derecho a la intimidad*", *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer España, Madrid, 2018.
[77]Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, art. 11, (BOE 14/03/1986).

uso de cuentas ficticias las actividades pertinentes para la consecución de dichos fines, sin necesidad de autorización judicial[78]. Un ejemplo de ello sería la venta de droga en redes sociales o a través de un foro, que por ser estos canales abiertos no estarían protegidos por el derecho fundamental del secreto de las comunicaciones del articulo 18.2 de la Constitución Española[79].

La figura del agente encubierto informático puede llegar a confundirse o a colisionar con lo que se conoce como delito provocado. La jurisprudencia[80] ha ido enmarcando el concepto de delito provocado estableciendo que se da en aquellos casos en los que alguien delinque como consecuencia de una actividad previa llevada a cabo por un funcionario de los Cuerpos o Fuerzas de Seguridad. La actividad previa consiste en una actuación engañosa que provoca que la persona, a la cual tenían intención de detener, cometa un delito sin que haya surgido de su propia voluntad y libre decisión y que no hubiese cometido si los agentes no hubiesen actuado.

Esta actividad choca directamente con los principios de un Estado de Democrático y de Derecho por ir en contra de la dignidad de la persona y del libre desarrollo de su personalidad.

Lo cierto es que, aunque ambas figuras puedan parecer semejantes o cercanas, no lo son. Existe jurisprudencia en la que se afirma que la ley no ampara el delito provocado. Es en la misma sentencia de 19 de noviembre de 2009, en la que se establecen los elementos que se deben dar para estar ante un delito provocado:

> *"La provocación delictiva es una inducción engañosa, es decir, supone injertar en otra persona el dolo de delinquir, y cuando esto se hace con la colaboración policial, se produce el efecto perverso de que la policía lejos de prevenir el delito, instiga a su comisión -elemento subjetivo- bien que sin poner en riesgo ningún*

[78] *Cfr*. Quevedo González, J., *Investigación y pruebas del delito*, Programa de Doctorado en Derecho y Ciencia Política, Línea de investigación: Derecho Procesal, Universidad de Barcelona, 2017, pág. 272. (Disponible en https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y). Fecha de consulta: 03/01/2022.
[79] Constitución Española, art. 18.2, (BOE 29/12/1978).
[80] *Cfr*., Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 19 de noviembre de 2009, 1166/2009, LA LEY 237364/2009, ECLI: ES:TS:2009:7467, FJ:3.

bien jurídico, pues en la medida que lo apetecido es la detención del provocado - elemento objetivo-, toda la operación está bajo el control policial por lo que no hay tipicidad ni culpabilidad, ya que los agentes de la autoridad tienen un control absoluto sobre los hechos y sus eventuales consecuencias - elemento material-, siendo estos tres elementos los que vertebran y arman la construcción del delito provocado, figura que como también se ha dicho por esta Sala es distinta a la actividad del agente encubierto o provocador, figura regulada en el art. 282 bis LECrim, que tiende exclusivamente a hacer aflorar a la superficie, la actividad delictiva de quien por su propia voluntad y sin instigación ajena, está dedicado a una actividad delictiva, o como se dice, entre otras STS 1114/2002 , "....cuando los agentes de la autoridad sospechan o conocen la existencia de una actividad delictiva y se infiltran entre los que la llevan a cabo en busca de información o pruebas que permitan impedir a sancionar el delito...."[81].

Por lo tanto, tal y como se puede extraer del párrafo anterior, la realización de esta actividad desembocaría en la impunidad del acusado, por no darse todos los elementos necesarios para considerar la concurrencia de delito.

En cambio, es importante mencionar que, respecto a la provocación del delito, la legislación y los límites entre provocación y agente encubierto son muy desiguales en función de la jurisdicción. Señala en la entrevista realizada y mencionada la Guardia Civil[82], por citar un supuesto concreto que, en EE. UU el límite es amplísimo. En este país es viable que, por ejemplo, agentes de la policía se hagan pasar por niñas incitando al delincuente a ir a una casa donde posteriormente se procede a su detención.

Como se aprecia, la diferente normativa propicia que en un Estado se usen unos métodos y en otro otros. La confrontación normativa surge en el momento en el que, para conseguir información de una persona que se encuentra en España las autoridades de EE. UU emplean un método parecido al ejemplo mencionado. Por ello, consideramos que sería deseable de una normativa global, internacional, que regulara unitariamente los medios de investigación de los delitos informáticos con el fin de que las diferentes jurisdicciones tengan los mismos fines y herramientas.

[81]Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 19 de noviembre de 2009, FJ:9, cit.
[82]Guardia Civil, comunicación personal con toma de notas, 24 de marzo de 2022.

En definitiva, un agente encubierto informático se encuentra amparado por la ley. Su objetivo principal es el de recabar pruebas y perseguir un delito que ya está realizando el delincuente por su propia voluntad y decisión sin que haya sido impulsado por la Policía Judicial.

Como se ha ido tratando a lo largo de este trabajo, la persecución e investigación de la *ciberdelincuencia* resulta compleja no solo por el sofisticado empleo que se hace de las nuevas tecnologías para dificultar las líneas de investigación, sino también, por el ocultamiento de los autores a través de perfiles falsos o cuentas con difícil acceso. Por ello, este mecanismo de investigación puede resultar muy útil a la hora de averiguar el *iter criminis* del delito, las personas implicadas y, sobre todo, para recabar las pruebas suficientes sobre todas las actividades ilegales llevadas a cabo.

5.3.3 Registros remotos de equipos informáticos

En ocasiones, se puede dar la circunstancia en la cual los agentes encargados de la investigación de un delito concreto tengan localizado el dispositivo desde el que se está llevando a cabo el hecho ilícito. Ante estos supuestos, el artículo 588 septies a de la LECrim contempla la posibilidad, por medio de la correspondiente autorización judicial, de que se pueda llevar a cabo un examen remoto, es decir a distancia y sin conocimiento del propietario, del contenido de los dispositivos localizados[83]. Con una primera lectura del artículo mencionado, se podría llegar a la conclusión de que el mismo tan solo permite el uso de este método de investigación y de obtención de pruebas para ciertos delitos, es decir que sería de aplicación *númerus clausus*. En cambio, es el apartado e) del mismo artículo el que permite la aplicación de esta técnica a *"delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación"*[84]. Tal y como se puede extraer de lo anterior y de la propia literalidad del artículo, dicha técnica se podría aplicar a cualquier delito informático o *ciberdelito,* pero para la investigación de un delito concreto.

Una de las grandes ventajas que tiene esta técnica es la de permitir a los agentes aprehender de forma remota toda la información hallada, incluyéndose aquí cualquier

[83] *Cfr.*, LECrim, art. 588 septies 1.a.
[84] LECrim, art. 588 septies 1.e.

dato relevante para ser aportado como prueba electrónica de cara al juicio[85]. Esto garantizaría que las pruebas se han quedado guardadas a pesar de que posteriormente el presunto autor intente eliminarlas de su dispositivo. Es labor del juez la de determinar en la propia autorización aquellas medidas que se deberán de llevar a cabo para preservar la integridad de los datos extraídos[86], es decir las medidas necesarias para garantizar la cadena de custodia. En cambio, no se puede observar en la misma ley algún apartado que establezca las pautas para llevar a cabo de forma satisfactoria la debida cadena de custodia de este tipo de pruebas, quedando totalmente en manos de la jurisprudencia y de los jueces el procedimiento que se deba llevar a cabo para ello.

Es la sentencia del TS de 27 de enero de 2010[87] la que proporciona información general, pero muy relevante sobre la cadena de custodia. Según esta, la función principal de la cadena de custodia es la de garantizar que los vestigios relacionados con un delito no son alterados de ninguna forma hasta que llegan a concretarse como pruebas en el momento del juicio. Es decir que se garantiza que la prueba es la misma a lo largo de todo el proceso judicial, ya que desde un primer momento puede parecer impensable que la prueba pueda ser alterada, pero hay que tener en cuenta que los objetos intervenidos deben pasar por distintos lugares para llevar a cabo diferentes exámenes sobre ellos. Por ello, en todo momento se debe garantizar que lo que se está trasladando y analizando no está siendo alterado y es exactamente lo mismo en todo momento, desde su obtención hasta su análisis.

Tal y como señala Gómez Sierra[88], la LECrim no específica tampoco qué instrumento o qué *software* deben emplear las FFCCSSEE para llevar a cabo el registro remoto de un dispositivo. Esto crea cierta inseguridad jurídica de la medida además de crear el riesgo de que las pruebas no sean consideradas válidas por no ajustarse a derecho.

[85]LECrim, art. 588 septies 2.b.
[86]LECrim, art. 588 septies 2.e.
[87]*Cfr*., Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 27 de enero de 2010, 6/2010, LA LEY 2383/2010, ECLI: ES:TS:2010:54, FJ:2.
[88]*Cfr*. Gómez Sierra, P., Medidas especiales de lucha contra el crimen organizado. La monitorización silenciosa de equipos informáticos, LA LEY, Nº 7, Sección Ciberseguridad, Wolters Kluwer Primer trimestre de 2021.

En conclusión, se puede observar en la regulación de este método de investigación que existen diversas carencias normativas sobre todo en lo que respecta a la forma en la que se debe de llevar a cabo el registro remoto. A pesar de ello, los registros remotos son una relevante fuente de prueba del delito, siendo de grandísima utilidad en aquellos supuestos en los que es necesaria una actuación ágil y rápida[89].

5.3.4 Aprehensión y volcado del disco duro

El volcado de disco duro es un proceso más físico que los explicados anteriormente. Esta técnica se lleva a cabo una vez que se han conseguido obtener de forma física aquellos dispositivos que pueden contener las pruebas del delito. Por ejemplo, un supuesto ficticio a través del cual un agente encubierto informático ha conseguido acceder al canal cerrado en el que se está cometiendo un delito de venta de pornografía infantil, se ha rastreado la dirección IP y, mediante la correspondiente autorización judicial, a través del operador de internet se han obtenido los datos correspondientes al titular de la red, incluido aquí el domicilio. Con una nueva autorización judicial se accede al domicilio del supuesto autor en el que se encuentran varios ordenadores y discos duros. Sería en este punto de la investigación en el que se aplicaría la técnica de volcado del disco duro.

En primer lugar, cabe recordar que la información que se encuentra almacenada dentro de los dispositivos electrónicos, incluyendo aquí los discos duros, es de contenido personal y por lo tanto protegida por diversos derechos fundamentales, como sería el derecho a la intimidad personal recogido en el artículo 18.1 CE, el secreto a las comunicaciones del artículo 18.3 CE e incluso a la protección de datos personales amparada en el art 18.4 CE[90].

Por ello, la autorización judicial para entrar en un domicilio no sería suficiente y, por lo tanto, no daría cobertura legal al hecho de aprehender dichos dispositivos y acceder a toda su información. Por el contrario, tal y como establece el artículo 588 sexies a. de la LECrim[91], se requiere de una autorización judicial específica para la aprehensión de los

[89]*Cfr.* Delgado Martín, J., "*Registro de dispositivos y registros remotos*", *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer España, Madrid, 2018, pág. 408, óp. cit.
[90]Delgado Martín, J., "*Registro de dispositivos y registros remotos*", *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer España, Madrid, 2018, Cfr, op. cit. pág. 386.
[91]LECrim, art. 588 sexies a.

distintos aparatos (esto es: ordenadores, teléfonos, discos duros, etc.), tampoco siendo esta suficiente para amparar el registro de los mismos. Es el párrafo segundo de este mismo artículo el que establece que será necesaria una autorización judicial adicional para proceder al registro del contenido de los aparatos.

El Tribunal Supremo en la sentencia del 17 de abril de 2013[92] establece la necesidad de obtener una autorización judicial que habilite a los agentes a intervenir un ordenador para acceder a su contenido, fundándose esta necesidad en el derecho de exclusión del propio entorno virtual y en las garantías constitucionales de inviolabilidad de las comunicaciones e intimidad. Es esta misma sentencia la que destaca que la autorización judicial previa para acceder al domicilio no habilita para acceder a los dispositivos que se hallen en él.

> *"De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías"*[93].

Así mismo, la ley prevé a su vez un procedimiento para los casos de urgencia. Es el artículo 588 sexies c. de la LECrim[94] el que habilita a la Policía Judicial, para aquellos casos en los que se aprecie un interés constitucional legítimo para examinar de forma directa los datos almacenados en los dispositivos hallados. Los agentes deberán comunicar dicha actuación al juez en un plazo máximo de veinticuatro horas con el objetivo de que sea revocado o confirmado. Tal y como afirma el Tribunal Constitucional en la sentencia del 24 de septiembre de 2007[95] la revocación de la actuación por el hecho de no haberse dado el presupuesto habilitante o la falta de proporcionalidad tendría efectos procesales en cuanto a la ilicitud de las pruebas obtenidas, ya que esta se habría hallado a través de la vulneración de derechos fundamentales.

---

[92]*Cfr.*, Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 17 de abril de 2013, 343/2013, FJ:8.
[93]Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 17 de abril de 2013, 343/2013, FJ:8, cit.
[94]LECrim, art. 588 sexies c.
[95]Cfr., Sentencia del Tribunal Constitucional de 24 de septiembre 2007, 206/2007, ECLI:ES:TC:2007:206, FJ 6.

En segundo lugar, una de las partes fundamentales al obtener las pruebas para su posterior incorporación al proceso es la de asegurar las pruebas obtenidas con el cumplimiento de todas las garantías. Reza el artículo 588 sexies c de la LECrim que "*la resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial"*[96].

Se puede extraer de la literalidad del artículo la posibilidad que se tiene de realizar un volcado, es decir, una copia clon de los datos obtenidos. En cambio, son varios los autores que se muestran críticos con la legislación, ya que no existen disposiciones que regulen cómo se deben realizar estas copias ni cómo se debe actuar con las pruebas para que se conserve la cadena de custodia, sino que se recae en la jurisprudencia la responsabilidad de dar respuesta a estas preguntas[97].

La información almacenada en dispositivos electrónicos es fácilmente manipulable y eliminable no solo por manipulación humana, sino por fallo del propio dispositivo, por ello, realizar un clonado del contenido resulta imprescindible para garantizar que esto no se produzca. Cuando se realiza un volcado de disco duro se produce un número denominado *hash,* conocido también como huella digital, el cual varía inmediatamente en el momento que haya un mínimo cambio en el contenido[98].

Es en este momento en el que Letrado de la Administración de Justicia debe dar fe sobre el numero *hash* creado anotándolo así en el acta levantada[99]. Existe jurisprudencia[*100*] que señala que no resulta necesario que el Letrado de la Administración de Justicia esté presente mientras se realiza el volcado, ya que por la complejidad técnica que dicho

[96]LECrim, art. 588 sexies c.
[97]*Cfr*. Rubio Alamillo, J., *Conservación de la cadena de custodia de una evidencia informática*, Diario La Ley, nº8859, Wolters Kluwer, 2016.
[98]Rubio Alamillo, J., *Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales*, Diario La Ley, nº9300, Wolters Kluwer, 2018.
[99]Delgado Martín, J., "*Registro de dispositivos y registros remotos*", *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer España, Madrid, 2018, *cfr.*, óp. cit. pág. 420.
[100]Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 22 de mayo de 2009, 480/2009, VLEX, ECLI: ES:TS:2009:3057, FJ:3.

proceso tiene, su presencia no garantizaría la legalidad de este. Es decir, que su presencia es innecesaria.

> *"En definitiva, la presencia del fedatario judicial en el acto del volcado de datos no actúa como presupuesto de validez de su práctica. Lo decisivo es que, ya sea mediante la intervención de aquél durante el desarrollo de la diligencia de entrada y aprehensión de los ordenadores, ya mediante cualquier otro medio de prueba, queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto de intervención y la que se obtiene mediante el volcado"*[101].

En definitiva, esta técnica de investigación y de obtención de pruebas resulta muy útil para la persecución de los delitos informáticos. En cambio, concurren dos hechos que el derecho debe tener muy presentes; Por un lado, la complejidad técnica es muy elevada y requiere la presencia de expertos que conozcan a la perfección como se deben manipular los aparatos sin que el contenido del interior sea alterado. Por otro lado, toda la información almacenada está amparada por el derecho a la intimidad. Ello requiere que el acceso sea restrictivo y quede sujeto a la autorización y supervisión judicial.

5.4 Incorporación de las pruebas informáticas al proceso

Una vez que se ha superado la fase de instrucción de un proceso penal en la que se han localizado y conservado las diligencias de investigación, y la fase intermedia, el proceso continuo a través de la tercera fase, la del juicio oral. En esta se practican las pruebas para cumplir así con lo exigido en el artículo 24.2 de la CE[102] tanto por la exigencia del carácter público del proceso, como el derecho a la defensa. De esta forma se cumple con los principios de oralidad, publicidad, inmediación y contradicción. Tal y como afirma Jaén Vallejo "*es en el juicio oral en donde hay que practicar las pruebas, porque solo lo que ha sido oralmente debatido en el juicio puede ser fundamento legítimo de la sentencia*"[103].

[101]Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 17 de abril de 2013, 342/2013, VLEX, ECLI: ES:TS:2013:2222, FJ:8.
[102]Constitución Española, art. 24.2.
[103]Jaén Vallejo, M. *Los principios de la prueba en el proceso penal español,* Universidad de las Palmas de Gran Canaria, pág. 2. Disponible en: https://escuela.fgr.gob.sv/wp-content/uploads/Leyes/Leyes-2/prueba-de-referencia-y-prueba-en-general-en-espa%C3%B1a.pdf (Fecha de consulta 10/01/2022).

En este punto del trabajo resulta relevante destacar la diferencia entre fuente de prueba y medio de prueba. Por un lado, la fuente de prueba es un concepto de naturaleza material y extraprocesal, ya que se refiere a aquellos elementos, lugares o personas que contienen la información relevante para el proceso, como por ejemplo el ordenador en el que se encuentra todo el plan de un atentado terrorista. Por otro lado, el concepto de medio de prueba sí es jurídico-procesal, por tratarse de la actividad a través de la que la información contenida en la fuente de prueba se incorpora al proceso, realizándose ante los miembros del órgano jurisdiccional y ante la parte contraria[104]. Siguiendo con el ejemplo, el plan en el que se describe el atentado encontrado en el ordenador se presentaría de forma documental ante el juez.

Como se ha ido exponiendo a lo largo del trabajo, las pruebas electrónicas, desde el momento de su obtención, se encuentran rodeadas de peculiaridades que las hacen diferentes de las pruebas convencionales. A pesar de ello, la ley no recoge ninguna especialidad acerca de la incorporación al juicio de la prueba digital, sino que tal y como defiende Delgado Martín, los datos electrónicos pueden incorporarse al proceso a través de cualquier medio probatorio previsto por la LECrim[105].

Es el capitulo III del título III de la LECrim[106] el que recoge los medios de prueba, entre los que destacan el interrogatorio de parte o del imputado, el examen de los testigos, la inspección ocular, el informe pericial y la prueba documental. En función de los datos que sean relevantes para el proceso, se introducirán de una forma u otra, ya que pueden ser de naturaleza muy diferente.

Respecto a la prueba documental la LECrim tan solo nombra el documento en soporte papel, a diferencia de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (LEC) que recoge expresamente en su artículo 384[107] la posibilidad de que los documentos que sean relevantes para el proceso puedan ser aportados de forma electrónica. Esta posibilidad es

[104]Enciclopedia Jurídica, Concepto de Fuente de prueba, Disponible en: http://www.enciclopedia-juridica.com/d/fuente-de-prueba/fuente-de-prueba.htm. (Fecha de consulta 10/01/2022).
[105]*Cfr*. Delgado Martín, J., "*Teoría general de la prueba digital: concepto, modalidades y fases en todos los procesos judiciales*", *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer España, Madrid, 2018, op. cit. pág. 51.
[106]Ley de Enjuiciamiento Criminal.
[107]Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, art.384, (BOE 08/01/2000).

aplicable y, de hecho, se aplica al derecho penal y, por ende, a los procesos penales a través de la analogía, tal y como establece el artículo 4 de la LEC[108].

Un claro ejemplo de ello es la sentencia del TS de 30 de diciembre de 2009[109], a través de la cual se admite como prueba válida la aportación de diferentes DVDs sobre los que se han volcado grabaciones de discos duros añadiendo además que estas gozan de presunción de veracidad salvo prueba en contrario. En esta misma sentencia se establece que las grabaciones o cualquier otra información puede ser incorporada al proceso a través de distintos medios, ya que la sociedad tecnológica va avanzando y pueden crearse medios nuevos que ni siquiera a día de hoy imaginemos que pudiesen existir. Se señala que lo relevante es la autenticación de las grabaciones y que las mismas puedan ser reproducidas en un soporte.

Tal y como señala Delgado Martín[110], los medios aportados siempre deben cumplir dos requisitos para que puedan presentarse en el juicio oral. El primero consiste en que los mismos puedan ser examinados por el órgano jurisdiccional con pleno respeto a las garantías del debido proceso y el segundo consistente en que el juzgado o tribunal cuente con los medios técnicos para poder acceder a la información, es decir a practicar la prueba. Estos dos requisitos resultan trascendentes, ya que sin su consideración las pruebas no podrían ser practicadas poniendo así en jaque el fallo judicial.

Asimismo, y en estrecha relación con lo mencionado en el párrafo anterior, el artículo 230 de la Ley Orgánica 4/2018, de 28 de diciembre, del Poder Judicial[111] establece que los Juzgados, Tribunales y las Fiscalías están obligados a utilizar cualesquiera medios técnicos e informáticos que se encuentren a su disposición para el desarrollo de su actividad y de sus funciones. Establece a su vez que los documentos entregados por los medios anteriores gozarán de la validez y eficacia de un documento original, siempre que se hayan cumplido las obligaciones establecidas por las leyes procesales.

---

[108]LEC, art.4.
[109]*Cfr*., Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 30 de diciembre de 2009, 1215/2009, La Ley 273447/2009, ECLI:ES:TS:2009:8417, FJ:1.
[110]*Cfr*., Delgado Martín, J., "*Teoría general de la prueba digital: concepto, modalidades y fases en todos los procesos judiciales*", *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer España, Madrid, 2018, Op. cit. pág. 54.
[111]*Cfr*., Ley Orgánica 4/2018, de 28 de diciembre, de reforma de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, art. 230, (BOE 29 de diciembre de 2018).

Como ha sido mencionado, no existe un único medio probatorio por el que los datos informáticos tengan que incorporarse al proceso, por ello se podría emplear cualquiera de los establecidos en la ley. En cambio, estos medios "tradicionales" deben adaptarse a las especialidades de las pruebas digitales y esto es lo que ocurre con la prueba pericial. Con la evolución tecnológica y su impacto en los procesos judiciales ha surgido doctrinal y jurisprudencialmente lo que se conoce como prueba pericial informática.

No se puede observar en las disposiciones de la LECrim referencia alguna a la prueba pericial informática, a diferencia de lo que ocurre con otras pruebas periciales[112] como por ejemplo la tasación pericial de objetos, los informes periciales sobre muestras de ADN o informes periciales del médico forense.

Tal y como define Pintor Palacios[113], un informe pericial consiste en un "medio de prueba a través del cual una persona emite una declaración de conocimiento sobre unos hechos, circunstancias o condiciones para lo que se requiere unos conocimientos científicos técnicos o prácticos". Para llevar a cabo los informes periciales, se emplea la informática forense consistente en la aplicación de técnicas científicas y analíticas con el objetivo de obtener, conservar y analizar información que sea válida dentro de un proceso judicial[114].

Por ello, se podrá hacer uso de este medio de prueba cuando las circunstancias lo requieran por la elevada complejidad técnica o bien para acreditar la autenticidad e integridad de las pruebas aportadas. Esta herramienta puede ser de gran utilidad para las partes involucradas en el proceso, así como para la autoridad judicial cuyos conocimientos técnicos sean limitados.

[112]LECrim, arts.363, 365, 375.
[113]Pintor Palacios, F., *La prueba pericial informática*, Diario la Ley nº5, LA LEY 3614/2017, Wolters Kluwer, 2017. (disponible en: https://acortar.link/bgy16z).
[114]*Cfr*., Pintor Palacios, F., *La prueba pericial informática*, cit. (online).

5.5 Valoración de las pruebas informáticas

La valoración de la prueba consiste en "*determinar qué es lo que nos quiere decir una prueba y en otorgar o no credibilidad a dicha prueba en orden a fijar como probados los hechos controvertidos*"[115].

Las pruebas practicadas en la fase de juicio oral deben ser valoradas por el juez conforme a su sana crítica y "*según su conciencia*"[116]. Por ello, no se encuentra una regulación acerca de cómo se deben valorar las pruebas o qué pautas se deben seguir para ello, ya que esto sería contrario a derecho.

Antes de proceder a analizar la eficacia probatoria de cada medio de prueba, el juez debe realizar lo que doctrinalmente se conoce como "test de admisibilidad"[117]. Como ha sido mencionado a lo largo del presente trabajo, las pruebas electrónicas son muy fácilmente manipulables, por ello el test de admisibilidad es un paso esencial para garantizar la seguridad jurídica de las partes y la legalidad del proceso. En el test se debe comprobar la integridad de las pruebas, la autenticidad y la licitud.

Tal y como afirma Urbano Castrillo[118], las pruebas electrónicas poseen ciertas especificidades que requieren de una atención diferente a las pruebas clásicas, sobre todo a la hora de llevar a cabo el "test de admisibilidad". Por ello, "*reclama de un mínimo normativo que ayude a clarificar un tema sobre el que escasea la doctrina y que contiene elementos propios bastantes, para justificar la solicitud*"[119].

Para llegar a una valoración completa de las pruebas electrónicas, es necesario examinar el estado de tres elementos, el *hardware* ("conjunto de elementos físicos que constituyen una computadora o un sistema informático"[120]), el software ("conjunto de programas,

---

[115]Vallespín Perez, D., El doble sistema de valoración de la prueba en interrogatorio de parte en el proceso civil, LA LEY 3314/2015, Wolters Kluwer, 2015. (Disponible en: https://acortar.link/XxPdPq).
[116]LECrim, art. 741.
[117]Urbano Castrillo, E., *La regulación legal de la prueba electrónica: una necesidad pendiente*, La Ley penal nº82, LA LEY 7393/2011, Wolters Kluwer, 2011. (Disponible en: https://bit.ly/3u5b7vz).
[118]Urbano Castrillo, E., *La regulación legal de la prueba electrónica: una necesidad pendiente* ..., cit. (online).
[119]Urbano Castrillo, E., *La regulación legal de la prueba electrónica: una necesidad pendiente*..., cit. (online).
[120]Diccionario de la Real Academia Española, DPEJ, Definición de hardware, Diccionario de la Real Academia Española, 2021, (disponible en: https://dpej.rae.es/lema/hardware). Consultada el:21/01/2022.

instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora"[121]) y el contenido digital alojado en el interior (ej. grabaciones de video, fotografías, documentos, etc.). El hecho de tener que analizar el hardware y el software dota a la valoración de la prueba electrónica de una especialidad ausente en el resto de las pruebas.

Como se puede extraer de lo anterior, la complejidad técnica de la valoración de las pruebas digitales es elevada. Por ello, las pruebas periciales llevadas a cabo por peritos informáticos expertos en la materia podrían tener un papel muy relevante en este ámbito judicial, ya que ayudarían al juez a la comprensión técnica del estado del software y hardware, evitando así que la valoración final de la prueba digital haya sido realizada conforme al conocimiento personal del juez sobre la tecnología.

Por ultimo, una vez realizado el "test de admisibilidad" y valoradas de forma libre las pruebas digitales, la resolución debe realizarse de forma motivada por el juez. "*Pruebas que, además, tienen que haber sido valoradas con arreglo a las máximas de la experiencia y a las reglas de la lógica, constando siempre en la resolución debidamente motivado el resultado de esa valoración"*[122]. Pero, como se ha mencionado anteriormente, la valoración de las pruebas digitales puede llegar a ser una ardua tarea para los jueces debido a la complejidad técnica de las mismas y a la carente experiencia en el ámbito digital.

[121]Diccionario de la Real Academia Española, DPEJ, Definición de software, Diccionario de la Real Academia Española, 2021, (disponible en: https://dpej.rae.es/lema/software). Consultada el:21/01/2022.
[122]Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 10 de julio de 2014, 439/2014, La Ley 82909/2014, ECLI: ES:TS:2014:2815, FJ:1.

6. CONCLUSIONES

I. Tras la investigación llevada a cabo, la primera conclusión que se obtiene consiste en que tanto la UE como el propio Estado español son conscientes del imparable crecimiento de la *ciberdelincuencia*, así como de la necesidad de crear normas específicas e internacionales adaptadas a esta realidad, ya que solo con ellas se podrá combatir contra los delitos informáticos. En cambio, no se encuentra una definición unitaria de la *ciberdelincuencia* y de las pruebas digitales en el ordenamiento jurídico español.

II. Desde ambos niveles territoriales (UE y España) se trabaja en la implementación de la ciberseguridad a través de la creación de diferentes agencias y organismos que funcionan como una primera barrera para la evitación de delitos informáticos.

III. Se ha podido observar que la persecución de la ciberdelincuencia es una ardua tarea debido a diferentes factores como el acceso transfronterizo, la complejidad técnica, la volatilidad de las pruebas etc. Por ello, entendemos que surge la necesidad de adaptar el derecho a esta realidad social con el fin de que todas estas cuestiones se resuelvan y de actualizar las herramientas existentes para que las autoridades encargadas de la persecución de los delitos informáticos puedan llevar a cabo su trabajo de forma eficaz y cumpliendo con todas las garantías legales. En cierto modo, la UE ha mostrado su implicación en esta cuestión a través de diferentes propuestas normativas que resuelven diversos problemas planteados. Esto muestra el claro interés en formar un sistema completo y eficaz que establezca un claro proceso de obtención de pruebas digitales garantizando la protección de los derechos fundamentales. En cambio, esta elaboración normativa lleva paralizada 4 años, hasta la fecha, provocando una carencia normativa al respecto.

IV. Por otro lado, la UE también ha iniciado los procesos para establecer acuerdos internacionales en la materia, pero estos también se encuentran paralizados. La consecuencia directa de la escasez normativa es la lentitud y falta de seguridad en los procesos judiciales en materia de ciberdelincuencia. La seguridad jurídica no

es solo un derecho fundamental, sino un principio del Estado de Derecho y, por ende, del proceso judicial.

V. Resulta urgente y necesaria una normativa internacional completa que armonice la legislación en la materia y que agilice la cooperación judicial internacional.

VI. Por otro lado, desde el punto de vista nacional, la LECrim sí ha introducido algunos elementos referentes a la investigación de los delitos informáticos. En ella podemos encontrar la regulación de algunos medios de investigación específicos, que además son de gran utilidad para las FFCCSSEE. Incluso la norma opera de una forma flexible al permitir que las pruebas digitales sean incorporadas al proceso judicial a través de cualquier medio. En cambio, tal y como ha sido mencionado, esto no resulta suficiente.

VII. La LECrim no desarrolla de forma detallada cómo se deben de obtener las pruebas digitales. La consecuencia directa es el riesgo para la necesaria seguridad jurídica, ya que la información que se maneja es de carácter personal. Además, una de las carencias normativas más palpables es acerca del modo en el que se deberían de custodiar las pruebas digitales obtenidas durante la investigación, asunto que se ha dejado en manos de la jurisprudencia. La custodia de las pruebas digitales en un asunto delicado que precisa de una regulación única y completa para evitar que situaciones en las que la veracidad de las pruebas y la justicia del juicio se pueda ver afectada.

VIII. En definitiva, queda mucho trabajo por hacer para llegar a una situación en la que se regulen de forma coherente, unitaria y completa los aspectos que envuelven a la ciberdelincuencia y, en especial, lo relacionado con las pruebas digitales a lo largo de todo el proceso, ya que estas tienen unas características muy peculiares a las que la norma no se había tenido que enfrentar nunca antes y, por ello se requiere su actualización.

7. REFERENCIAS BIBLIOGRÁFICAS

7.1 NORMATIVA (normas y otros instrumentos de regulación)

Derecho nacional

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (BOE 31/03/2015).

Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE núm. 304, de 20/12/2003).

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE 19/10/2007).

Instrucción nº 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías.

Derecho comunitario

Instrumento de ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, (BOE, núm. 226, de 17 de septiembre de 2010, pág. 2).

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DOUE» núm. 194, de 19 de julio de 2016, pág.5).

Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales COM/2018/226 final - 2018/0107 (COD) (EURLEX documento 52018PC0226, pág. 4).

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, COM/2018/225 final - 2018/0108 (COD), (EURLEX documento 52018PC0225, pág. 6).

Recomendación de Decisión del Consejo por la que se autoriza la apertura de negociaciones para un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en materia penal COM/2019/70 final (EURLEX, documento 52019PC0070, pág.1).

Recomendación de Decisión del Consejo por la que se autoriza la participación en las negociaciones sobre un Segundo Protocolo adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia (STE n.º 185), COM/2019/71 final (Eurlex documento 52019PC0071, pág. 2).

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (DOUE» núm. 151, de 7 de junio de 2019, pág. 20).

Preparación de un Segundo Protocolo adicional al Convenio de Budapest sobre la Ciberdelincuencia, Proyecto de Protocolo, versión 2, pág. 8, art. 6.3, Consejo de Europa, Francia, 2021, disponible en (https://rm.coe.int/0900001680a27dbe). (Consultado: 29 de noviembre de 2021).

7.2 JURISPRUDENCIA

Sentencia del Tribunal Constitucional de 15 de marzo 46/1990, La Ley 1458-TC/1990, FJ 5.

Sentencia del Tribunal Constitucional de 24 de septiembre 2007, 206/2007, ECLI:ES:TC:2007:206, FJ 6.

Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 10 de julio de 2014, 439/2014, La Ley 82909/2014, ECLI: ES:TS:2014:2815, FJ:1.

Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 17 de noviembre de 2011, 1299/2011, La Ley 246234/2011, ECLI: ES:TS:2011:8595, FJ:5.

Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 17 de abril de 2013, 342/2013, VLEX, ECLI: ES:TS:2013:2222, FJ:8.

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 19 de noviembre de 2009, 1166/2009, LA LEY 237364/2009, ECLI: ES:TS:2009:7467, FJ:3.

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 20 de octubre de 2009, 921/2009, La Ley 200570/2009, ECLI: ES:TS:2009:6307, FJ:5.

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 22 de junio de 2016, 551/2016, La Ley 74791/2016, ECLI: ES:TS:2016:3062, FJ:2.

Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 22 de mayo de 2009, 480/2009, VLEX, ECLI: ES:TS:2009:3057, FJ:3.

Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 27 de enero de 2010, 6/2010, LA LEY 2383/2010, ECLI: ES:TS:2010:54, FJ:2.

Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 29 de diciembre de 2010, 1140/2010, LA LEY 226907/2010, ECLI: ES:TS:2010:718, FJ:6.

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal de 3 de diciembre de 2012, 987/2012, La Ley 195398/2012, ECLI: ES:TS:2012:8316, FJ:3.

Sentencia del Tribunal Supremo, Sala Segunda, de lo penal de 30 de diciembre de 2009, 1215/2009, La Ley 273447/2009, ECLI:ES:TS:2009:8417, FJ:1.

7.3 OBRAS DOCTRINALES

Delgado Martín, J., "*Derecho a la intimidad*", *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer España, Madrid, 2018.

Delgado Martín, J*., Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer, Madrid, 2018, p. 43.

Delgado Martín, J., *La prueba digital. Concepto, clases y aportación al proceso*, Diario La Ley, Nº 6, Sección Ciberderecho, Editorial Wolters Kluwer, 11 de abril de 2017, p. 1.

Gómez Sierra, P., Medidas especiales de lucha contra el crimen organizado. La monitorización silenciosa de equipos informáticos, LA LEY, Nº 7, Sección Ciberseguridad, Wolters Kluwer Primer trimestre de 2021.

Jaén Vallejo, M. *Los principios de la prueba en el proceso penal español,* Universidad de las Palmas de Gran Canaria, pág. 2. Disponible en: https://escuela.fgr.gob.sv/wp-content/uploads/Leyes/Leyes-2/prueba-de-referencia-y-prueba-en-general-en-espa%C3%B1a.pdf (Fecha de consulta 10/01/2022).

Pintor Palacios, F., *La prueba pericial informática*, Diario la Ley nº5, LA LEY 3614/2017, Wolters Kluwer, 2017, (disponible en: https://acortar.link/bgy16z).

Quevedo González, J., *Investigación y pruebas del delito*, Programa de Doctorado en Derecho y Ciencia Política, Línea de investigación: Derecho Procesal, Universidad de Barcelona, 2017, pág. 272. (Disponible en https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y). Fecha de consulta: 03/01/2022.

Rubio Alamillo, J., *Conservación de la cadena de custodia de una evidencia informática*, Diario La Ley, nº8859, Wolters Kluwer, 2016.

Sanchis Crespo, C., *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*, Thomson Reuters Aranzadi, Navarra, 2012, p.713.

Urbano Castrillo, E., *La regulación legal de la prueba electrónica: una necesidad pendiente*, La Ley penal nº82, LA LEY 7393/2011, Wolters Kluwer, 2011. (Disponible en: https://bit.ly/3u5b7vz).

Vallespín Pérez, D., El doble sistema de valoración de la prueba en interrogatorio de parte en el proceso civil, LA LEY 3314/2015, Wolters Kluwer, 2015. (Disponible en: https://acortar.link/XxPdPq).

Van Dijk, J., 2006. *The network society: Social aspects of new media,* Sage Publications Ltd, London, 2006, p.2.

Velasco Núñez, E., *Delitos cometidos a través de Internet. Cuestiones Procesales*, La Ley-Actualidad, Madrid, 2010.

7.4 RECURSOS DE INTERNET

Apple, Outside US Legal Process Guidelines. (Disponible en https://images.apple.com/legal/privacy/law-enforcement-guidelines-outside-us-es.pdf). Consultada:18/11/2021.

Consejo Europeo, "Ciberseguridad: cómo combate la UE las amenazas cibernéticas, Consejo Europeo, 2021 (disponible en https://www.consilium.europa.eu/es/policies/cybersecurity/). Consultado 28/10/2021.

Dirección general de coordinación y estudios secretaría de estado de seguridad, "Estudio sobre la cibercriminalidad en España", *Ministerio del interior; Secretaría general técnica*, 2020 (disponible en http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3). Consultado: 27/10/2021.

Kemp S., "The Global State of Digital 2021; Spain report", *Kepios*, 2021(disponible en https://www.hootsuite.com/es/pages/digital-trends-2021). Consultado 27/10/2021.

López-Fonseca, O., "Detenido el mayor ciberestafador de España", *El País*, 5 de julio de 2019. (Disponible en: https://elpais.com/politica/2019/07/04/actualidad/1562264274_472850.html). Consultado 11/11/2021.

Página web Comisión Europea, nota de prensa: https://ec.europa.eu/commission/presscorner/detail/es/IP_13_13. Consultado: 4/11/2021.

Página web Consejo de la UE. (Disponible en: https://www.consilium.europa.eu/es/policies/e-evidence/). Consultado en: 25/02/2022.

Página web de Eur-Lex. Disponible en: https://eur-lex.europa.eu/procedure/EN/2018_107. Consultado en: 25/02/2022.

Página web de UNIR, Ciberdelincuencia: *¿Qué es y cuáles son los ciberdelitos más comunes?* Disponible en: https://www.unir.net/derecho/revista/que-es-ciberdelincuencia/. Consultado: 08/11/2021.

Página web de UNODC:https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html. Consultado el 06/11/2021.

Página web INCIBE: https://www.incibe.es/que-es-incibe- Consultado en 4/11/2021.

Página web Interpol: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19. Consultado: 27/10/2021.

Página web Policía Nacional: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php. Consultado en: 5/11/2021.

Página web: Cliatec 360 Data Center. (Disponible en https://cliatec.com/whatsapp-y-centro-de-datos-infraestructuras-boton-enviar/). Consultado: 18/11/2021.

Página web de Kaspersky, (disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address). Consultada: 20/12/2021.

Sánchez R., “Alemania almacenará datos telefónicos sistemáticamente durante diez semanas”, *El Mundo*, 27 de mayo de 2015. (Disponible en: https://www.elmundo.es/internacional/2015/05/27/5565ec4ae2704ebc738b4590.html). Consultado: 24/03/2022.

7.5 DICCIONARIOS

Diccionario de la Real Academia Española, DPEJ.

Enciclopedia Jurídica.