Victimización sexual y nuevas tecnologías: **desafíos probatorios**

Raquel López Jiménez

VICTIMIZACIÓN SEXUAL Y NUEVAS TECNOLOGÍAS: DESAFÍOS PROBATORIOS

VICTIMIZACIÓN SEXUAL Y NUEVAS TECNOLOGÍAS: DESAFÍOS PROBATORIOS

Raquel López Jiménez
Universidad Carlos III de Madrid
ORCID ID: 0000 0002 5409 3738

DYKINSON
2021

Publicación financiada por la Agencia Estatal de Investigación (AEI) RTI2018-099170-B-I00/AEI/10.13039/501100011033.

Resolución de conflictos, 13
ISSN 2659-952X

Editorial Dykinson
c/ Meléndez Valdés, 61 – 28015 Madrid
Tlf. (+34) 91 544 28 46
E-mail: info@dykinson.com
http://www.dykinson.com

Preimpresión: TallerOnce

ISBN: 978-84-1377-987-4
Depósito legal: M-34764-2021

Versión electrónica disponible en e-Archivo
http://hdl.handle.net/10016/33722

A mis tíos Valentina López y José Cerqueira.
In memoriam.

“Las especies que sobreviven no son las más fuertes ni las más inteligentes, sino aquellas que se adaptan mejor al cambio”.

Charles Darwin

ÍNDICE

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
Art.	Artículo
CE	Constitución Española
CEDH	Convenio Europeo de Derecho Humanos
CIT	Equipo de Inteligencia Cibernética
CP	Código Penal
DNS	Domain Name Systen (nombres de dominio)
EC3	European Cybercrime Centre
ECPA	*Electronic Communications Privacy Act*
ECTEG	Grupo Europeo de Formación y Educación en Ciberdelincuencia
EINSA	European Information Network Security Agency
FTP	File Transer Protocol (Protocolo de transferencia de archivos)
IP	Internet Protocol
ISP	Proveedoras de servicios de Internet
LEC	Ley de Enjuiciamiento Civil
LECrim	Ley de Enjuiciamiento Criminal
LO	Ley Orgánica
LOPJ	Ley Orgánica del Poder Judicial
MAC	Media Acces Code
MMS	Multimedia Messaging System
NTICs	Nuevas tecnologías de la información y comunicación
OSINT	Open Source Intelligent
RAE	Real Academia Española
SIM	Subscriber Identy Module
SMS	Short Message System
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TICs	Tecnologías de la Información y Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea

INTRODUCCIÓN

Cuando comencé a redactar esta obra nunca llegué a pensar que la sociedad actual viviría una pandemia provocada por un virus conocido como Covid-19, ello ha hecho que hayamos cambiado, todavía si cabe más, nuestra forma de relacionarnos y de comunicarnos. Esta "guerra" o "batalla" que libramos contra la Covid-19 marcará, sin duda alguna, nuestra forma de relacionarnos en adelante y, a mi parecer, no sólo durante la cuarentena que estamos pasando mientras escribo estas líneas, sino de por vida o, por lo menos, durante mucho tiempo.

Si ya antes de la pandemia el uso de las nuevas tecnologías era elevado, fundamentalmente entre los adolescentes, el distanciamiento social provocado por el virus ha marcado distancias físicas en nuestros hábitos, no sólo en el trabajo sino también en el resto de ámbitos. La sociedad ha estado mediada por las nuevas tecnologías y el uso de lo virtual ha sido la vía de escape de la mayoría de las personas, haciendo un uso desmesurado durante toda la pandemia. La transformación digital ha llegado a todos los ámbitos y sectores, tanto en las relaciones sociales como laborales, particularmente también en el ámbito de la educación que es donde yo me muevo. La pandemia ha supuesto que hallamos trasladado nuestra vida personal, laboral y social a la esfera de lo virtual. Lo bueno de ello es que ese traslado ha permitido que el mundo siga girando durante la crisis sanitaria, pero sin embargo ha abierto una ventana por la que peligrosamente ha entrado la ciberdelincuencia.

Las estadísticas en la práctica reflejan que el uso de Internet es muy elevado, así en la encuesta a usuarios de Internet (19.973) que llevó a cabo la Asociación para la investigación de medios de comunicación (aimc.es) presentada en marzo de 2020, los datos que exponen de 2019 a personas encuestadas de 14 años o más, es que usan ordenador 23.103 (57,3 %), usan ordenador habitualmente 18.234 (45,3 %), usan Internet último mes 33.811 (83,9%), usan Internet ayer 32.205 (79,9%), conexión Internet en el hogar 34.903 (86,6%).

Esta nueva cultura digital donde cada vez más personas interactúan y comparten información y datos personales a través de Internet facilita a los delincuentes el acceso y la obtención de datos personales y empresariales. La revolución tecnológica ha modificado la manera en la que creamos y gestionamos todas nuestras relaciones, tanto sociales y afectivas y como veremos también sexuales. Es evidente que esta nueva cultura digital supone un reto

para la cultura del Derecho que, aunque últimamente ha avanzado en su regulación, sin embargo, todavía va por detrás.

En el inicio de la redacción de esta obra, con anterioridad a la aparición del virus provocado por la Covid-19 y de vernos limitados en nuestra libertad ambulatoria, ponía de manifiesto en la Introducción de la misma que era sabido por todos que las nuevas tecnologías[1] habían cambiado la sociedad actual en muchos y diferentes aspectos, no sólo en la forma de relacionarnos y comunicarnos entre nosotros, sino también en la forma de cometer nuevos hechos delictivos, no éramos conocedores entonces hasta cuánto iban a cambiar nuestra manera de vivir. En este sentido, las nuevas tecnologías han revolucionado la sociedad desde dos perspectivas distintas; por un lado, favoreciendo la aparición de nuevos delitos[2], ya que el flujo de información incontrolada jurídicamente provoca que aparezcan nuevas formas de criminalidad tecnológica y, por otro lado, facilitando también la persecución de los delitos[3]. En la actualidad, con la pandemia la situación se ha visto agravada, muchos delincuentes están aprovechando estas circunstancias para trasladarse al mundo digital y cometer hechos delictivos. En este sentido, la criminalidad organizada está utilizando el confinamiento para reciclarse y actualizarse en el uso de Internet para seguir delinquiendo[4].

---

1 Se ha decidido aceptar la expresión "NTIC" como "concepto que engloba a un conjunto de herramientas relacionadas con el almacenamiento, procesamiento y transmisión, digitalizados, de información, así como, los procesos y productos derivados de las innovaciones del *hardware* y *software"*. Véase a MARTÍNEZ LÓPEZ-SAEZ, Mónica, *Una revisión del derecho fundamental a la protección de datos de carácter personal*, 2018, Tirant on line, DOCUMENTO TOL6.820.902, quien profundiza en la evolución de las tecnologías pasando de las TIC a las NTIC.

2 Señala AGUILAR CÁRCELES, Marta María, "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido", en *Revista Criminalidad*, 57 (1): 121-135, http://www.scielo.org.co/scielo.php?pid=S1794-31082015000100009&script=sci_arttext, en relación con el concepto de "revolucionario", "*no solo como innovación y avance prosocial, sino también como un hecho transformador y modificador de la vida en sociedad, que ha permitido al delincuente disponer de nuevas formas de actuación e incluso crear tipos delictivos ausentes años atrás*".

3 Como con frecuencia se dice "en la tecnología encontramos tanto la enfermedad como la cura", véase a MARTÍNEZ LÓPEZ-SÁEZ, Mónica, *Una revisión del derecho…*, op. cit.

4 Véase el trabajo de VALLS PRIETO, Javier, "Nuevas formas de combatir el crimen en internet y sus riesgos", en *Revista Electrónica de Ciencia Penal y Criminología,* RECPC 18-22 (2016), 36 págs.

Recientemente, junio de 2020, Europol ha manifestado en el Informe que emite en el ámbito de la *Evaluación de amenazas contra la delincuencia organizada en Internet* (IOCTA), que la explotación sexual infantil en línea es un fenómeno en constante evolución y está condicionado por los avances tecnológicos. La conectividad móvil, la creciente cobertura de Internet en los países en desarrollo y el desarrollo de soluciones de transmisión de pago por uso, que brindan un alto grado de anonimato al espectador, están promoviendo la tendencia en la transmisión comercial en vivo de abuso sexual infantil[5].

Además, la inexistencia de fronteras tanto físicas como espaciales unido a la rapidez en las comunicaciones ha supuesto que la sociedad de la información opere en esas dos direcciones; por un lado, fomentando la comisión de hechos delictivos y, por otro, favoreciendo la investigación de dichos delitos, si bien, hay que tener en cuenta que el anonimato de los autores de los delitos está presente en la forma de comisión de los mismos. Por lo tanto, si bien las nuevas tecnologías van a ayudar a investigar y facilitar el enjuiciamiento de nuevos delitos puesto que las nuevas tecnologías proporcionan valiosas herramientas de investigación[6], por otro lado, el acceso a las tecnologías desde cualquier ámbito sin ningún límite ni temporal ni material dificulta considerablemente el descubrimiento de los autores delictivos. Es evidente que las nuevas tecnologías, en concreto, las características propias de Internet[7] favorecen y propician las posibilidades de comisión de ciertos delitos y, en definitiva, fomentan las posibilidades al alcance de los delincuentes permi-

5 Véase https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation.

6 Señala FERNÁNDEZ MARTÍNEZ, Juan Carlos, "Especialidades de la prueba cuando, esta, es tecnológica", en *Nuevas tecnologías 2020*, Tirant lo Blanch, 2020, pág. 325, que "a nivel europeo observamos que, según datos publicados por el Consejo de Europa, se hace mención a que más del 85% de las investigaciones penales en la Unión Europea (UE) utilizan algún tipo de dato electrónico y de los cuales, en más de la mitad, son necesarios el requerimiento por la autoridad de información a un prestador de servicios".

7 Entre estas características técnicas destaca QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, Tesis Doctoral dirigida por ORTEGO PÉREZ, Fr., y tutorizada por VALLESPÍN PÉREZ, D., defendida en la Universidad de Barcelona, Facultad de Derecho, 2017, en disposit.ub.edu, págs. 39-45, se encontrarían: a) Conmutación de paquetes; b) Adressing and routing; c) Protocolos de comunicación; d) Número de Puerto, dirección IP, dirección MAC; e) Gestor de las direcciones IP y Puerto de Dominio; entre los componentes técnicos destacan: a) Routers; b) Redes de acceso; c) Redes de Área Local; d) Servidores Hosts.

tiendo generalmente su anonimato como pasaré a exponer. Existen determinadas conductas delictivas que se han visto favorecidas precisamente por las ventajas que ofrece el uso de las nuevas tecnologías.

Es en este ámbito o contexto donde se vienen materializando muchas conductas delictivas caracterizadas por el uso de las nuevas tecnologías digitales como vía o medio de comisión de un delito. Tanto es así, que recientemente estamos asistiendo a la aparición de nuevas figuras delictivas cuya comisión se lleva a cabo precisamente a través de los medios informáticos o tecnológicos en las que una de las características principales es la dificultad que existe para sancionar la conducta delictiva de los culpables puesto que aun cuando se produce una situación de indefensión la misma no queda amparada por la práctica probatoria procesal penal. Los delincuentes están aprovechándose de las posibilidades que ofrece Internet y los delitos que se comenten están cada día más en alza. Sin entrar ahora en profundidad en las características técnicas de Internet quisiera apuntar que las mismas hacen que sea mucho más fácil para los delincuentes la comisión de determinados delitos. Estas técnicas están en constante desarrollo dado el avance de las tecnologías y ello hace muy difícil tanto su averiguación como su persecución y enjuiciamiento.

Es así, que la aparición de Internet y de las redes telemáticas han supuesto la creación de un nuevo concepto de delito denominado desde el Convenio de Budapest sobre Ciberdelincuencia de 2001[8] como *ciberdelito* para referirse a "aquel delito, ya sea tradicional o característico de la sociedad de la información, propiciado por las nuevas tecnologías"[9]. Si bien, aunque existen diferentes concepciones del *ciberdelito,* se pueden agrupar en dos. La doctrina habla a este respecto, por un lado, de una interpretación estricta y por otro lado de una amplia. En relación con la primera, se incluirían todos los delitos en los que las TICs se utilizan tanto como medio y como objetivo del delito, ejemplos

8 Este Convenio tenía como objetivo principal la armonización de las legislaciones nacionales tanto en materia sustantiva como procedimental, definiendo las conductas que deben ser sancionadas, así como asegurando la existencia de instrumentos legales que posibiliten la investigación del ciberdelito y en general los delitos cometidos a través de sistemas informáticos o cuya prueba pueda obtenerse en formato electrónico, creando a su vez mecanismos de cooperación urgentes y efectivos para que unos Estados y otros puedan prestarse diversas formas de asistencia específicamente diseñadas por razón de la materia.

9 En la actualidad existen muchos calificativos para referirse a los delitos cometidos a través de Internet o haciendo uso de las nuevas tecnologías, ya sean delitos informáticos, delitos cometidos en red, en línea, digital, delitos on line, ciberdelitos, etc. Véase a QUEVEDO GONZÁLEZ, Josefina, *Investigación y prueba del ciberdelito*, op. cit., pág. 55.

de ello son la piratería informática o la propagación de virus informáticos. Por otro lado, la interpretación amplia incluye aquellos delitos donde las TICs son esenciales para la ejecución, pero no son el objetivo[10].

Como ha sido definido, Internet es considerada "una red mundial con conexiones instantáneas y con una estructura descentralizada que se basa en la representación digital de la información y que permite las conexiones en tiempo real entre las personas independientemente de su ubicación"[11].

Como señala FERNÁNDEZ DOYAGUE, "las redes sociales virtuales han transformado la forma en que hombres y mujeres se relacionan e interactúan entre sí. Las nuevas tecnologías de la información y comunicación (TICs), son espacios donde se realiza una exposición de la vida personal, que suponen nuevas formas de violencia y control sobre las mujeres y nuevas formas de relaciones afectivas y sexuales"[12]. Las denominadas nuevas tecnologías se pueden agrupar en tres áreas relacionadas entre sí: la informática, el video y la telecomunicación. La aparición de las mimas ha supuesto en el ámbito del derecho la aparición de nuevas fuentes de prueba gracias a nuevos soportes y signos distintos de la escritura plasmada en un documento de papel[13]. Como veremos la prueba electrónica se enmarca como medio probatorio dentro del derecho de las nuevas tecnologías.

El objeto del presente estudio se circunscribe al tratamiento de la prueba en los delitos cometidos por medios electrónicos o, por decirlo de otra forma, los delitos virtuales o delitos "on line", dentro de los cuales cabe incluir entre otros, el acoso y el abuso sexual, la usurpación de perfiles y violaciones de la privacidad, el ciberacoso, "sexting" y" sextorsión" y "grooming", no obstante, me voy a circunscribir a los delitos de violencia sexual cometidos a través de los instrumentos tecnológicos como son el "sexting" y el "grooming" o el "stalking". Todos ellos comportamientos delictivos con tintes sexuales, cometidos a través de las plataformas o sistemas virtuales tales como el correo electrónico, WhatsApps, redes sociales, blogs o foros, etc… Internet y los diferentes espacios virtuales están siendo el punto de encuentro para muchos jóvenes y

10 Véase a QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, op. cit., pág. 60 y ss, donde se ofrecen diferentes clasificaciones de *ciberdelito*.

11 Ibídem, pág. 48.

12 "La denominada violencia cibernética. Internet y las redes sociales", en *Consejo General de la Abogacía Española*, noviembre 2014, en https://www.abogacia.es/2014/11/26/la-denominada-violencia-cibernetica-internet-y-las-redes-sociales/

13 Véase a PÉREZ PALACI, Enrique, *La prueba electrónica: Consideraciones*, 2014, en www.proleg.org.

adolescentes, un hábitad natural aunque virtual en el que relacionarse, y no sólo en el ámbito social sino también sexual. En definitiva, las conductas de "sexting" ayudan a dar visibilidad a esta nueva realidad.

El Grupo de Trabajo del Consejo de Europa sobre el acoso *on line* y otras formas de violencia en línea, en particular contra las mujeres y los niños, en un estudio de 2018 -Mapping study on cyber violence[14]- describe la ciberviolencia como "el uso de los sistemas informáticos para causar, facilitar o amenazar a las personas con violencia causando o pudiendo causar daños o sufrimientos físicos, sexuales, psicológicos o económicos, incluyendo también la explotación de las circunstancias, características o vulnerabilidades individuales".

Al cometerse estos delitos a través de los medios electrónicos es evidente que es precisamente la prueba electrónica la que va a ser fundamental para poder perseguir y castigar estos hechos delictivos. En la práctica, actualmente en el 85% de las investigaciones penales se utilizan datos electrónicos y; además, de ese 85%, el 65% del total de las solicitudes se dirigen a proveedores de servicios con sede en otra jurisdicción[15].

Es patente que la forma en la que se comunican las personas es a través y cada vez más del uso del correo electrónico y de la mensajería instantánea, considerándose como piezas esenciales de la comunicación fundamentalmente entre jóvenes[16]. En este sentido, la prueba que demuestre la comisión de los hechos será fundamentalmente electrónica y aquí es donde surge un problema jurídico puesto que, aunque el derecho tiende a regular todos los aspectos de la sociedad, muchas veces va por detrás y sobre todo en materia de nuevas tecnologías, dado el desmesurado avance que están teniendo.

---

14 https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c

15 Véase a ALONSO LECUIT, Javier, "El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea", ARI 4/2021, 14 de enero de 2021, publicado en http://www.realinstitutoelcano.org/.

16 Véase a MONTESDEOCA RODRÍGUEZ, Daniel, "El delito de descubrimiento y revelación de secretos en el uso de las tecnologías de la información y comunicación: especial referencia a la mensajería instantánea", en *Diario LA LEY*, nº 9770, de 14 de enero de 2021, Nº 9770, 14 de enero de 2021, pág. 3, quien indica que "*Facebook tiene 2.449 millones de usuarios y su Facebook Messenger es utilizado por 1.300 millones de usuarios; WhatsApp alcanza los 1.600 millones de usuarios, mientras que Telegram tiene 400 millones de usuarios. Estas cifras son sin duda sorprendentes y ofrecen el ejemplo de cómo cualquier dato que enviamos a través de estas herramientas pueden tener un alcance inestimable*".

Aunque las nuevas tecnologías y singularmente las redes sociales están favoreciendo la aparición de nuevos hechos delictivos, no obstante, no se puede demonizar las redes sociales y concluir que estas no son buenas, las redes son un reflejo de nuestra sociedad y lo que ocurre fuera se refleja en ellas, el lado bueno es que sirven para denunciar hechos delictivos y que sean conocidos por todos, puesto que las redes sociales tienen un alcance mundial, el lado malo es que se están utilizando precisamente también para cometerse hechos delictivos. En definitiva, son una oportunidad, pero también una amenaza. De hecho, ya la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[17], establecía en su Considerando 6 que: "*Internet está revolucionado las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad*".

En este sentido, como ha indicado la doctrina "el derecho a la intimidad configurado como poder jurídico de la persona sobre la información relevante para su devenir vital, puede resultar menoscabado por las posibilidades ofrecidas por las nuevas y modernas técnicas de comunicación, en la medida en que permiten la captación de un conjunto de elementos, datos o informaciones, cuya interrelación puede dar lugar a un conocimiento de pautas conductuales"[18].

Como ha venido manifestado el Tribunal Constitucional, "el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 CE), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (SSTC 207/1996 , de 16 de diciembre, FJ 3; 186/2000, de 10 de julio, FJ 5; 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 4; y 159/2009, de 29 de junio, FJ 3)"·. El Tribunal Constitucional sigue indicando "que lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no

17 En eur-lex.europa.eu.

18 SUBIJANA ZUNZUNEGUI, Ignacio José, "Policial judicial y derecho a la intimidad en el seno de la investigación criminal", en *EGUZKILORE*, Número extraordinario 10, San Sebastián, Octubre 1997, págs. 126 y 127.

sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio (SSTC 127/2003, de 30 de junio, FJ 7 y 89/2006, de 27 de marzo, FJ 5)".

De la lectura de este artículo nuestro Tribunal Constitucional ha concluido que el derecho a la intimidad concede a la persona que lo ostenta el poder jurídico de imponer a terceros la obligación de abstenerse de toda intromisión en la esfera íntima y la prohibición de utilizar la información conocida (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2)[19].

Desde la Sentencia del Tribunal Constitucional 134/1999, de 15 de julio, la intimidad o el derecho a la intimidad ha ido transformándose hasta llegar a ser entendida como un bien jurídico relacionado con la libertad de acción de la persona, en el sentido de otorgarle de forma positiva el control de la información atinente tanto a su persona como a su familia en el ámbito público. De estar forma, puede decidir qué información conoce el tercero y cuál no, además de prohibir su difusión no consentida.

Nuestra sociedad actual ha tomado conciencia de ello y se está trabajando desde todos los ámbitos para perseguir estas conductas delictivas tanto desde el plano sustantivo como procesal. La utilización de las nuevas tecnologías conlleva que la prueba necesaria para acreditar los hechos objeto de debate sea precisamente la de tipo tecnológico, ello incrementará la eficacia judicial en la persecución de los hechos delictivos, sin perder de vista que muchos de ellos se cometen precisamente a través de estos medios, pero hay que tener en cuenta que la obtención de prueba tecnológica a su vez conllevará el riesgo de lesividad de los derechos fundamentales del investigado, fundamentalmente el derecho a la protección de datos personales[20].

Hay que recordar que nuestro Ordenamiento jurídico procesal está anclado en los principios basados en el Siglo XIX y ello conlleva que deba adaptarse y avanzar en materia de nuevas tecnologías regulando todos los aspectos referi-

19 STC 173/2011, en Tirant on line, DOCUMENTO TOL2.288.705.

20 En este sentido véase a PÉREZ ESTRADA, Miren Josune, "La vulneración de datos personales en la aportación de la prueba en el proceso penal", en *Justicia: ¿Garantías versus eficiencia?,* Tirant lo Blanch, 2019, pág. 884, quien indica que "se debería haber aprovechado la reforma de la legislación procesal para haber realizado una protección específica del derecho a la protección de datos personales, de manera separada al resto de derechos fundamentales que se contienen en el art. 18 CE".

dos tanto a su obtención, como a su incorporación y valoración probatoria en el proceso penal. Señala a este respecto ORTIZ PRADILLO, que "en el anverso de la moneda de este desarrollo tecnológico se encuentran los Derechos Fundamentales de las personas, que necesariamente deben ser reinterpretados para ofrecer una protección adecuada en la nueva Era Digital"[21]. A efectos de la investigación y enjuiciamiento de estos delitos, habrá que tener en cuenta que existen singularidades y dificultades para la averiguación y castigo de los culpables, las dificultades en la localización e identificación de las personas responsables de los hechos es una característica de la comisión de estos tipos delictivos.

Así, en el ámbito sustantivo penal, una de las últimas reformas ha sido precisamente la prevista por la Ley Orgánica 1/2015, de 30 de marzo del Código Penal surgida como consecuencia precisamente de los avances en materia de nuevas tecnologías. En concreto, esta Ley introduce nuevas figuras delictivas como son el delito de "sexting" y "grooming" dado el auge y la gravedad que estos fenómenos están teniendo en la sociedad debido fundamentalmente a los avances tecnológicos en las comunicaciones. Además, hay que tener en cuenta que, en este contexto de pandemia, se da un mayor uso de las redes sociales[22], lo que implica que el acceso por parte de los delincuentes a los menores de edad a través de las redes pueda realizarse con mayor facilidad y, por tanto, los menores puedan ser víctimas idóneas de estos delitos.

Se utiliza la terminología inglesa para referirse a estas conductas haciendo un brindis al derecho anglosajón, puesto que este fue el primero que inició la persecución de las mismas y tiene ya un recorrido en el análisis y forma de perseguirlas, por ello, la utilización de estos vocablos ingleses por parte de nuestro legislador[23].

El legislador ha tomado conciencia de la gravedad de estas conductas y de la problemática que plantea para el Derecho Penal[24]. La llegada de Internet

---

21 ORTIZ PRADILLO, Juan Carlos, *La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, en Fundación alternativas, 2013, pág. 4, véase en https://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf.

22 El uso de las redes sociales durante los días de pandemia por coronavirus (a fecha 22 de mayo de 2020) ha aumentado un 55%, véase abc.es

23 Véase al respecto a SALVADORI, Iván, "La controvertida relevancia penal del sexting en el derecho italiano y comparado", en *Revista Electrónica de Ciencia Penal y Criminología,* 2017, pág. 5, también en http://criminet.ugr.es/recpc – ISSN 1695-0194. Quien indica que "los primeros casos de sexting se han manifestado en los Países de habla inglesa más avanzados tecnológicamente".

24 Si bien es cierto, que hay que dejar constancia de que no toda la doctrina era parti-

ha provocado nuevas formas de interacción social que han facilitado la aparición de estas nuevas conductas delictivas que afectan gravemente a la privacidad de las víctimas, en muchos de los casos menores de edad. El triunfo de la tecnología ha dejado patente la falta de tipificación de esas conductas y ha venido a exigir una respuesta penal. Es evidente que era y es necesario nuevas formas de investigación para la averiguación de este tipo de delitos dada la singularidad del medio de comisión. La necesidad de transformar el Derecho Penal no tiene que significar en ningún caso que se dejen de lado sus garantías, no hay que olvidar que el Derecho Penal surgió precisamente para la protección de los bienes jurídicos, es por ello, por lo que ahora también en la esfera de lo tecnológico debe perseguir las conductas delictivas.

Por otro lado, en lo que se refiere al ámbito procesal penal, la situación en materia de nuevas tecnologías cambia también en el año 2015, en concreto con la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Hasta 2015 la situación procesal en materia de nuevas tecnologías era la insuficiente por no decir nula regulación legal, a partir de esta fecha el legislador regula dicha materia y, por tanto, además de implicar una novedad también significa un avance que necesariamente debía tomar la LECrim para adaptarse a la nueva realidad. Ahora bien, la cuestión es si esa regulación legal es idónea o adecuada para satisfacer las garantías probatorias necesarias en todo proceso penal. Esta ley viene a dar cobertura legal a una situación donde las intervenciones se llevaban a cabo sin una ley que respaldase la actuación.

En definitiva, el Derecho penal y el Derecho Procesal deben ir de la mano si se quieren erradicar estas conductas delictivas. El legislador es consciente de ello y a este propósito ha dirigido últimamente sus esfuerzos. Es evidente, que esta nueva criminalidad supone un verdadero reto en el que tienen que implicarse todos los poderes del Estado, es necesario aunar todos los esfuerzos para evitar la impunidad de esos delitos y, por otro lado, proteger los derechos fundamentales de las personas entre ellos la protección de datos personales, entre otros.

---

daria de criminalizar estas conductas, que la vía no puede ser la penal sino la jurisdicción civil a través de la L.O. 1/1982 de protección civil del honor, intimidad y la propia imagen. Véase el trabajo de PÉREZ CONCILLO, Eloísa, "la difusión de sexting ajeno como violencia de género", en *Revista Aranzadi de Derecho y Proceso Penal*, 2018, núm. 51.

I

LA CRIMINALIDAD INFORMÁTICA

Dentro del término "criminalidad informática"[1], se engloban tanto las conductas delictivas como los procedimientos que se utilizan para perseguir y castigar dichas conductas. Nuestra investigación en este sentido versará tanto sobre los aspectos materiales, si bien sin llegar a profundizar en ellos, como desde el punto de vista procedimental y, fundamentalmente, en lo que atañe a la prueba, por ser esta una cuestión que plantea verdaderas dificultades en lo que a la obtención de fuentes de prueba se refiere. Por tanto, dentro de la criminalidad informática nuestra investigación en el plano sustantivo penal versará exclusivamente sobre los delitos contra la intimidad o contra la libertad e indemnidad sexual y, más concretamente, los delitos de "sexting", "grooming" y "stalking" en el ámbito procesal trataremos la materia probatoria en la persecución de dichos delitos.

Desde el punto de vista sustantivo-material, hay que señalar que las nuevas tecnologías de la comunicación han provocado la aparición de una nueva criminalidad conocida como "criminalidad informática", un género de delincuencia surgida como consecuencia de dicho fenómeno.

Señala FLORES PRADA, que "las tecnologías han conseguido crear una nueva dimensión del espacio, que no es tangible o sensorial sino virtual, en el que se almacena o por el que circula información codificada a través de canales informáticos"[2]. En este espacio creado por Internet conocido como ciberespacio se han desarrollado conductas que vulneran bienes jurídicos necesitados de protección. El mismo autor manifiesta que "el ciberespacio está construido fundamentalmente sobre aparatos y técnicas de información; constituye en realidad un instrumento para tratar la información, pero, al menos por el momento y dentro de nuestro vigente ordenamiento penal, no ha hecho nacer nuevos valores que no fueran ya objeto de protección"[3]. En

1 En relación con el concepto de "criminalidad informática", véase el trabajo de FLORES PRADA, *Criminalidad informática. Aspectos sustantivos y procesales*, Tirant lo Blanch, 2012, en Tirant on line, Documento TOL2.696.348.

2 FLORES PRADA, I., *Criminalidad informática. Aspectos sustantivos y procesales*, op. cit.

3 Ibídem.

este sentido, con la aparición de Internet han nacido nuevas conductas susceptibles de ser tipificadas por vulnerar bienes jurídicos protegidos, los cuales no son nuevos, aunque la información se trasmita a través de la Red. Precisamente la utilización de las redes a través de Internet ha favorecido un incremento considerable de delitos contra la libertad sexual tanto de adultos como de menores, especialmente en el ámbito de los menores e incapaces, puesto que las nuevas tecnologías facilitan la creación y difusión de pornografía infantil, así como también la facilidad en el acceso a menores para obtener información o imágenes con carácter sexual. Ello, por un lado, porque también hay que tener en cuenta la facilidad con la que los menores pueden acceder a las redes y la posibilidad de interactuar de forma anónima y ocultando la edad, suplantando perfiles para facilitar la comunicación con otras personas. En este sentido, es verdaderamente importante el trabajo de prevención con los menores de edad para erradicar desde su origen estas conductas delictivas y en ello se está trabajando tanto desde el ámbito interno como internacional[4].

No obstante, teniendo en cuenta la importancia que tiene la prevención de esas conductas desde el origen, no hay que perder de vista el desafío que supone la criminalidad informática tanto para el Derecho material, derecho penal sustantivo, como para el Derecho Procesal. Son dos ámbitos de una misma realidad en la que necesariamente se tienen que producir cambios si se quiere luchar contra la delincuencia en el mundo virtual.

Como señalaba anteriormente, en el ámbito penal recientemente estamos asistiendo a la criminalización de conductas que se comenten en este ámbito virtual. En un primer momento estas conductas no estaban tipificadas, precisamente porque el legislador no conocía este espacio, para poder regularlo es necesario que se familiarice no sólo en el ámbito interno sino también en el internacional dada la singularidad de los delitos cometidos en la red. La tarea del legislador en este sentido es dar una respuesta a las conductas que violentan bienes jurídicos, sabiendo que las redes abarcan no sólo un ámbito nacional sino internacional. En este sentido, se está avanzando considera-

4 Actualmente, los menores de edad y con edades cada vez más termpranas acceden cada día más a las nuevas tecnologías, por ello necesitan toda la ayuda posible para saber utilizar con responsabilidad estas tecnologías, así iniciativas como la "Guía para un uso seguro y responsable de internet por los menores_itinerario de mediación parental", pueden ser una buena herramienta de ayuda. https://www.is4k.es/sites/default/files/contenidos/herramientas/is4k_guia_mediacion_parental_internet. pdf

blemente, tanto a nivel interno como a nivel internacional, aunque todavía queda bastante camino por recorrer.

Por lo que respecta al ámbito procesal no sustantivo, el avance de las tecnologías está necesariamente provocando cambios en ese ámbito, pero el legislador todavía va muy por detrás. Como indicaba anteriormente, una de las últimas reformas ha sido la llevada a cabo por la Ley Orgánica 13/2015, de 5 de octubre, ya citada[5], pero la cuestión es si esta regulación es suficiente o, por el contrario, todavía quedan aspectos sin regular. Tal y como evolucionan las nuevas tecnologías la respuesta es seguramente negativa, y es que en este ámbito es problemática la delimitación de qué se considera nuevo y qué viejo, en un contexto tan cambiante e innovador como el actual.

Si consideramos todo ello, esto es, los problemas de tipificación de conductas nuevas teniendo en cuenta que son especialmente técnicas, junto con la extraterritorialidad de la red, el anonimato que generalmente acompaña a los navegantes en Internet y la excesiva velocidad en los descubrimientos tecnológicos, podemos concluir que la materia es verdaderamente compleja.

En el marco de la Unión Europea ha sido relevante en este aspecto la Directiva UE 2016/1148, de 6 de julio, del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[6], la cual ha sido implementada en nuestro ordenamiento mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información[7]. Como se recoge en el informe recogido en *Estudios sobre cibercriminalidad en España* realizado en 2018, esta norma dispone el marco estratégico e institucional de la seguridad en las redes y sistemas de información en España haciendo especial hincapié en la necesidad de cooperar entre las autoridades públicas además de determinar la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten, así como a los que se aplicará. En el Estudio se indica que esa normativa entre otras finalidades

5 Se cumple con esta reforma con los compromisos que impone la ratificación del Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001, fue ratificado por España el 3 de junio de 2010 y entró en vigor para nuestro país el 1 de octubre de ese mismo año, que se aplica a la obtención de pruebas electrónicas, y se sigue la jurisprudencia de la Sala de lo Penal del Tribunal Supremo en materia de medidas de investigación tecnológicas. En https://www.boe.es/eli/es/ai/2001/11/23/(1).

6 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

7 https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf

también está la de fijar los poderes de inspección y control de las autoridades competentes y la cooperación con las autoridades nacionales de otros Estados miembros, añade que se tipifican una serie de infracciones y sanciones, y se regulan las obligaciones de seguridad de los operadores. Por último, trata la notificación de incidentes, poniendo el acento en los que tienen un impacto transfronterizo y la gestión de información y coordinación con otros Estados de la Unión Europea[8].

8 *Estudios sobre la cibercriminalidad en España*, 2018, pág. 10.

II

TIPIFICACIÓN DE LOS DELITOS

a. El delito de "sexting"

a.1. Delimitación conceptual

Con la finalidad de solucionar la falta de tipicidad de algunas conductas y para adaptar el texto del Código Penal a la realidad social, la Ley Orgánica 1/2015, modificó los delitos referidos a la intromisión en la intimidad de los ciudadanos sancionándose de forma específica el delito de "sexting" que a continuación paso a delimitar.

Con anterioridad a la reforma operada por la Ley Orgánica 1/2015, la conducta de difundir imágenes de sexo de la víctima, hubiesen sido o no enviadas por ella, no estaba penalizada en nuestro Ordenamiento jurídico. Ha sido a partir de la sentencia dictada por la Audiencia Provincial de Granada 351/2014, de 5 de junio[1], de carácter absolutoria, precisamente porque no estaba tipificada la conducta, cuando se consideró por parte del legislador la necesidad de criminalizar dichas conductas dada la repercusión social que provocó este asunto y las lagunas existentes en la regulación legal.

En la práctica, los supuestos más comunes de "sexting" son el reenvío a amigos o conocidos por WhatsApp u otras redes sociales de fotografías íntimas enviadas con la autorización de la pareja del autor delictivo; o la difusión de imágenes de encuentros ciber-sexuales con la víctima por Skype. Son comportamientos cada vez más generalizados sobre todo entre los adolescentes que les puede suponer un potencial peligro tanto en su existencia virtual como también en la vida real[2].

Señala SALVADORI, que "si bien no hay un acuerdo unánime sobre el sentido que hay que atribuirle al sexting, este término se emplea normalmente para definir las conductas de autoproducción, posesión, distribución o cesión

1 Rec. 351/2014. Roj: SAP GR 1051/2014 - ECLI:ES:APGR:2014:1051.

2 Véase en este sentido la tesis doctoral de ALONSO RUIDO, Patricia, *Evaluación del fenómeno del sexting y de los riesgos emergentes de la red en adolescentes de la provincia de Ourense*, dirigido por Rodríguez Castro, Yolanda y Lameiras Fernández, María, 2017, Universidad de Vigo, donde se refleja el estudio que se llevó cabo a adolescentes de la provincia de Ourense en relación con las prácticas de sexting.

de imágenes de menores desnudos o semidesnudos en actitudes sexualmente explícitas a través de dispositivos móviles (smartphone, tabletas, etc.) o servicios disponibles en red (Viber, WhatsApp, Facebook, Instagram, Snapchat, etc.)"[3].

Las principales características de este tipo delictivo se pueden resumir en las siguientes[4]:

a) la utilización de las nuevas tecnologías como por ejemplo el teléfono móvil, las tablets, el ordenador, las redes sociales, la mensajería instantánea, entre otras, para enviar, recibir o reenviar tanto mensajes de texto como videos y/o grabaciones de contenido sexual.

b) el carácter sexual y/o erótico de los contenidos.

c) la creación o el protagonista del material puede ser por el propio sujeto o por alguien ajeno el origen del contenido erótico sexual, pudiendo ser de producción propia o ajena.

d) El cuarto aspecto importante relacionado intrínsecamente con el anterior es la identidad de los protagonistas del vídeo, fotografía o texto erótico sexual. Ello supone una consecuencia perjudicial añadida del Sexting, considerando que si son menores de edad las consecuencias legales son todavía mayores.

e) Como quinta característica se encuentra la edad de las personas implicadas. Si bien las primeras investigaciones iban dirigidas a una práctica entre adolescentes, sin embargo, recientemente los estudios demuestran que también su práctica se encuentre entre personas adultas.

f) Otra característica se encuentra en la propia voluntad de enviar este tipo de contenidos, asumiendo la responsabilidad en el primer paso en su difusión.

Es importante indicar que la práctica de esta modalidad delictiva en las parejas de jóvenes, puede conducir a un sinfín de agresiones a través de las redes. La conducta que mantiene el delincuente en la práctica de este delito es progresiva, en el sentido de que comienzan en un primer momento presionando a la otra persona a que practique el "Sextin" para posteriormente pasar a chantajearle para llevar a cabo otras conductas también con fines ilegítimos. Por tanto, aunque en un primer momento no pareciera muy grave las acciones de gravarse sin embargo los riesgos que conlleva esa acción sitúan a

3 SALVADORI, Iván, "La controvertida relevancia penal del sexting en el derecho italiano…", op. cit., pág. 3.

4 Ibídem, págs. 88 a 90.

los adolescentes en una situación de verdadera vulnerabilidad e indefensión. De ello, derivan comportamientos como el Bullying o Ciberbullying, el Ciberstalking y derivado de estos, diferentes formas de Sextorsión como son el Grooming y la Teen Dating Violence[5]. En definitiva, todos estos fenómenos son distintas maneras de ejercer violencia a través de las TICS o de Internet, es decir manifestaciones de ciberviolencia.

g) También relacionada con esta característica estaría la que hace referencia a la voluntariedad a la hora tanto de crear los contenidos, como en su divulgación puesto que de no existir ese consentimiento nos encontraríamos con graves implicaciones legales.

h) Finalmente, otro aspecto de estos comportamientos tiene que ver con la presión e influencia que puede llegar a tener la sociedad en la creación de este tipo de contenidos vinculados a los cánones de belleza actuales[6].

Esas serían, por tanto, las características principales de las conductas delictivas que integran el delito de Sexting. Precisamente, los hechos que dieron lugar a la sentencia citada se basaban en la difusión a través de WhatsApp de una fotografía enviada de forma voluntaria por una menor de edad en la que

---

5 Conocido como la violencia en el noviazgo de adolescentes.

6 Señala ALONSO RUIDO, P., op. cit., pág. 90, que: "*Además, las normas de feminidad y masculinidad se ven reflejadas en los contenidos de Sexting. En este sentido Ringrose et al. (2012) afirman que los chicos desempeñan el rol activo en el proceso, pues solicitan, almacenan y distribuyen los sexts de las chicas y los utilizan como una mercancía o moneda para obtener algo a cambio. Por lo que podríamos decir que las chicas desempeñan el rol pasivo, produciendo los contenidos de Sexting para el consumo masculino. Asímismo siguiendo las aportaciones de Harris Davidson, Letourneau, Paternite y Miofsky (2013) los comportamientos de Sexting tienen una contextualización concreta, pues a pesar de mantener un patrón constante se encuentran influenciados por los factores ambientales, de desarrollo y situacionales de cada adolescente en cada cultura o ámbito concreto (ver Figura 1.7). Tal y como explican Harris et al. (2013) en primer lugar, en el contexto ambiental se incluyen la familia, el grupo de iguales, la comunidad en la que se encuentra el sujeto y la cultura popular, la escuela, las instituciones legales, comunitarias y sociales, así como los medios de comunicación y la comunicación digital. En segundo lugar, se halla el contexto de desarrollo, es decir desarrollo biopsicosocial en el que se encuentre el o la adolescente. En tercer lugar, se refiere al contexto situacional, que profundiza más en la conceptualización del sujeto, abarcando la propia construcción individual como persona autónoma y las dinámicas interpersonales. Todo ello configura, las denominadas Tecnologías de la información, la comunicación y la socialización "elementos descriptivos" del fenómeno del Sexting, es decir, las actividades, el contenido y el escenario en el que este se realiza*".

aparecía desnuda junto a otro menor con quien tenía una relación, quien a su vez la reenvió a otros móviles produciéndose una difusión a gran escala. Dada la repercusión social y gravedad de tales hechos se introdujo en la reforma del Código Penal de 2015, como conducta tipificada como delito[7].

Así, en el Capítulo I "Del descubrimiento y revelación de secretos" del Título X "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio" del Código Penal, se regula en su artículo 197 el delito conocido como "sexting"[8]. La Ley Orgánica 1/2015, de reforma del Código Penal modifica los delitos referidos a la intromisión en la intimidad mediante la tipificación de un nuevo delito de difusión de imágenes[9], las cuales se han obtenido con el consentimiento de la víctima, pero sin la autorización para su difusión. Hasta la reforma de 2015, en el Código Penal solo se castigaba, concretamente en el art. 197.1, el "apoderamiento o interceptación" de cartas o mensajes privados de la víctima, sin embargo, no se penaba cuando era la propia víctima la que facilitaba esos archivos a la persona que luego los difundía sin su autorización[10]. En el delito de "sexting" no hay, sin embargo,

---

7 En la sentencia citada, dictada por la Audiencia Provincial de Granada, se puso de manifiesto "*que el "sexting" supone el envío de imágenes estáticas (fotografías) o dinámicas (vídeos) de contenido sexual de mayor o menor carga erótica entre personas que voluntariamente consientes en ello y, que forma parte de su actividad sexual que se desarrolla de manera libre. La difusión de las imágenes por sus receptores no encuentra encaje en las conductas que describe el citado artículo, y por ello, el legislador, tras un escándalo mediático "caso Olvido Hormigos", pretende introducir una nueva conducta en el art. 197 del CP, el pfo. 4, en el Proyecto de Código Penal en el que se trabaja en la actualidad. Dicho precepto alude expresamente a los casos de obtención consentida de imágenes íntimas con difusión inconsentida posterior, conducta que debe ser regulada expresamente por la exigencia típica del consentimiento en los tipos precedentes*". Roj: SAP GR 1051/2014 - ECLI:ES:APGR:2014:1051.

8 Esta denominación deriva de la contracción de "sex" y "texting" y se refiere precisamente al envío de contenidos eróticos o pornográficos por medio de instrumentos tecnológicos.

9 La doctrina ha puesto de manifiesto que "*los defectos de los que adolece la redacción típica del art. 197.7 CP, donde ha sido incluida y los numerosos problemas interpretativos que suscita, junto con las principales críticas de las que ha sido objeto*", véase a PÉREZ CONCHILLO, Eloisa, *Intimidad y difusión de sexting no consentido*, Tirant lo Blanch, 2018.

10 Véase sobre el artículo 197 el trabajo de GONZÁLEZ COLLANTES, Tália, "Los delitos contra la intimidad tras la reforma de 2015: luces y sombras", en *Revista de Derecho Penal y Criminología*, 3.ª Época, n.º 13 (enero de 2015), págs. 51-84. Quien indica que "lo

una apropiación indebida de imágenes, que sí estaba penalizado en el artículo 197.1 del CP con anterioridad de la reforma por la Ley 1/2015, y su difusión en el artículo 197.4 del CP.

En concreto, en su apartado 7 se indica que: "*Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.*

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa".

Por consiguiente, se penaliza la conducta de la persona que reenvía imágenes sin consentimiento desvelando aspectos de la intimidad personal de un tercero, de esta forma, se vulneran sus derechos a la intimidad, al honor y a la propia imagen, y además cuando los hechos se llevan a cabo por el cónyuge o ex cónyuge, conviviente o ex conviviente, persona con relación de noviazgo presente o pasada, menor de edad, persona con discapacidad necesitada de especial protección, o los hechos se han cometido con una finalidad lucrativa y entonces se convierte en un tipo agravado.

El "sexting" se basa en la relación de confianza que existe entre la persona que consiente en ser grabada o fotografiada en escenas de contenido claramente sexual y la persona destinataria de dichas imágenes o vídeos[11]. Esta relación de confianza hace que entre ellas nazca un deber especial de confidencialidad que se ve roto por la difusión de dichas imágenes.

Como señala MAGRO SERVET se castiga la conducta de "*cualquier internauta que se dedique a «rebotar» un archivo íntimo sin la autorización de la persona en cuestión, y todo ello con independencia de que el internauta sea*

---

que venía pasando es que los operadores jurídicos, en ocasiones, en un intento de encontrar vías de punibilidad para evitar que estas conductas quedasen impunes, condenaban por un delito de injurias con publicidad". Ibídem, pág. 67.

11 PÉREZ CONCHILLO, Eloísa, *Intimidad y difusión de sexting no consentido*, op. cit., pág. 11.

o no el primer receptor de esas imágenes o simplemente se dedique a agrandar la difusión de una grabación ya extendida por la red"[12].

En concreto, cuatro son los elementos objetivos del tipo penal:

– Obtención de imágenes o grabaciones de la víctima

– Difusión, revelación o cesión a terceros de imágenes o grabaciones de la víctima

–Ausencia de autorización de la víctima para la difusión, revelación o cesión a terceros

– Que la difusión, revelación o cesión menoscabe gravemente la intimidad personal de la víctima[13].

La vulneración del derecho a la intimidad puede venir por diferentes vías que se han visto ampliadas por la aparición y avance de las nuevas tecnologías, unido ello además a la diferente manera de relacionarse entre sí, ya que ello ha supuesto a su vez la aparición de nuevos y avanzados medios de captación y transmisión de la imagen y el sonido, por lo que es fácilmente adsequible para los delincuentes tanto la obtención como la difusión de imágenes y grabaciones de la víctima[14].

Es importante resaltar que en este delito la mera conducta de divulgar o difundir imágenes de un tercero sin su consentimiento está penalizada, independientemente de que haya consentido su grabación. En este sentido, el que se haya grabado no implica en ningún caso que exista una autorización implícita por parte de la víctima a la difusión, al contrario, puesto que este consentimiento no se puede presumir por el simple hecho de que permita que se le grabe o sea ella misma la que se grabe[15]. Por tanto, para evitar que se castigue a quien difunda imágenes o grabaciones que se hayan producido en un ámbito personal y que pueden dañar considerablemente la intimidad de la persona es necesario que se demuestre que hay un consentimiento expreso a la divulgación de aquellas. Se penaliza la autoría de la difusión no autorizada

12 MAGRO SERVET, Vicente, "El delito de sexting (o difusión de imágenes tomadas con consentimiento de la víctima) en la violencia de género", *En la Ley Penal*, N 137, marzo-abril 2019.

13 Señala PÉREZ CONCHILLO, Eloísa, *Intimidad y difusión de sexting no consentido*, op. cit., pág. 12, que indica que "el sexting entre adolescentes y las graves repercusiones que ello tiene en las víctimas menores de edad. En este caso se puede llegar a afectar su indemnidad sexual, y no solo su intimidad personal".

14 Ibídem, pág. 24.

15 Véase a MAGRO SERVET, Vicente, "El delito de sexting (o difusión de imágenes tomadas con consentimiento de la víctima) en la…", op. cit., pág. 2.

de las imágenes o videos. La grabación de las imágenes o videos, por tanto, queda en la intimidad de los intervinientes sin que se pueda difundir sin el consentimiento de la persona grabada.

En este sentido, aunque las imágenes o el video los difunda quien haya participado en los mismos está penalizado, puesto que en el artículo 197.7 del CP se penalizan dos conductas: por un lado, quien habiendo protagonizado y grabado una relación íntima con un tercero, se dedica a difundir las imágenes sin el consentimiento de la otra parte; y a su vez, también se penaliza la conducta de aquellos que habiendo recibido las imágenes o el video las difunden sin autorización expresa del protagonista ya que lo que es objeto de sanción penal es la difusión y no la grabación.

En definitiva, el delito de "sexting" pretende preservar a la víctima del control del contenido de la grabación, aunque haya sido ella misma quien haya enviado las imágenes o video. Precisamente esta cuestión de la voluntariedad de la víctima a la hora de grabar las imágenes es el punto de partida o el eje central de la doctrina en la discusión sobre si el Derecho Penal debe o no intervenir en el castigo de dichas conductas puesto que si es precisamente la víctima la que permite que su derecho a la intimidad se vea afectado no hay razón que justifique el recurso al Derecho Penal, puesto que conforme a esta doctrina "conforme a los principios de intervención mínima, proporcionalidad y última ratio no es exigible demandar al Derecho Penal la protección de una conducta que ni tan siquiera el principal protagonista y afectado ha sido capaz de mantener a salvo de terceros al rebajar los niveles de autotutela"[16]. Esta postura doctrinal aboga porque sea la jurisdicción civil la competente para proteger estas conductas a través de la Ley Orgánica 1/1982 de Protección civil del honor, la intimidad y la propia imagen y no la jurisdicción penal.

En una de las sentencias más recientes del Tribunal Supremo, en concreto la 70/2020, de 24 de febrero[17], donde se condena por el delito del artículo 197.7 del CP, en un supuesto de reenvío a un tercero de una foto de un desnudo que la persona afectada había enviado voluntariamente a la persona que difundió las imágenes, se analiza si los terceros que reciben las imágenes y son ajenos al circulo de confianza en el que se ha creado el material gráfico o audiovisual y que consiguen esas imágenes sin conexión personal con la

16 Véase a PÉREZ CONCHILLA, Eloísa, *Intimidad y difusión de sexting inconsentida*, op. cit., págs. 68 y 69.

17 Número de recurso 3335/2018. Núm. Cendoj: 28079120012020100084; Núm. Ecli:ES:TS:2020:492.

víctima pueden ser también penados de acuerdo a dicho delito. En estos supuestos mantiene el Tribunal Supremo que están excluídos de su aplicación, literalmente indica que: "*La difusión encadenada de imágenes obtenidas a partir de la incontrolada propagación en redes telemáticas, llevada a cabo por terceros situados fuera de la relación de confianza que justifica la entrega, queda extramuros del derecho penal*". Sin embargo, si estos terceros conocen la procedencia ilícita de estas imágenes, entonces sí les será de aplicación dicho delito, aunque con una pena inferior.

En relación con las modalidades, señala DELGADO MARTÍN, que atendiendo al medio o soporte de grabación de las imágenes se puede hablar también del "sex-castin", como una modalidad del "sexting" que consiste en la grabación de imágenes de contenido sexual mediante webcam y su posterior difusión por redes sociales, mail o servicios de mensajería instantánea[18]. Entiendo por mensajería instantánea aquella que tiene una comunicación fluida y en tiempo real, como puede ser el Whatsapp o el chat, sea esta cerrado o abierto. El tratamiento procesal es el mismo independientemente de la modalidad escogida, lo único que difiere es el instrumento utilizado para transmitir las imágenes.

a.2. La carga de la prueba en el delito de "sexting"

Un aspecto que merece especial atención en el delito de "sexting" desde el punto de vista procesal es el relativo a la carga de la prueba de la falta de consentimiento para difundir o divulgar las imágenes grabadas o videos.

Como dije anteriormente se penaliza la conducta de difundir las imágenes aunque la víctima haya prestado el consentimiento para la grabación. Es importante resaltar que una de las peculiaridades de dicho delito es la voluntariedad de la víctima a la hora de producir y enviar ese contenido de forma voluntaria, sin ningún tipo de coacción ni error. Deviene de una conducta libre la cual parte en la mayoría de los casos sin sugestión por parte de la persona destinataria del mismo[19].

No se entiende que exista un consentimiento implícito a la difusión, aun-

18 DELGADO MARTÍN, Joaquín, *Investigación tecnológica y prueba digital en todas las jurisdicciones,* La Ley, 2018, pág. 339.

19 Véase a FERNÁNDEZ NIETO, Josefa, "Reforma del Código Penal hacia una nueva dimensión de la protección en los delitos de sexting y grooming", en *Diario la Ley*, Numero 8714, Sección Doctrina, 3 de Marzo de 2016, Ref. D-93, Editorial La Ley, pág. 7.

que haya consentido la grabación, por tanto, el acusado tiene que probar para no ser castigado que existía un consentimiento expreso para la difusión de las imágenes[20]. En este sentido, la carga de la prueba recae en el acusado y no en la víctima puesto que si ésta tuviese que probar que no existió consentimiento ni expreso ni tácito sería una prueba diabólica, como sabemos prohibida por nuestro ordenamiento.

Por tanto, si el acusado alega que hubo consentimiento por parte de la víctima para la difusión de las imágenes o los videos en él recae la carga de la prueba. Esta es una de las cuestiones más problemáticas en lo que respecta a la prueba, puesto que el problema que surge ahora es cómo se puede probar que hubo consentimiento para la difusión de las imágenes. Entendemos que el consentimiento tiene que ser expreso y no cabe en este tipo de delitos el consentimiento tácito. Por tanto, si existe alguna exteriorización suficiente para que quede plasmado el consentimiento será fácil probarlo, pero si no existe ninguna constancia se entiende que no existe consentimiento para la difusión.

a.3. El delito de "sexting" en el ámbito de la violencia de género

El legislador penal ha contemplado en el artículo 197.7 del CP el delito básico del "sexting" y en su segundo párrafo el delito de "sexting" cometido en el ámbito de la pareja como tipo agravado. Así en dicho párrafo se establece que "*la pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa*".

Por tanto, uno de los subtipos agravados es que el que se refiere a que el sujeto activo sea el cónyuge o persona con quien mantenga o haya mantenido una análoga relación de afectividad, aun sin convivencia. En este sentido, el Código Penal agrava la pena cuando existe una especial relación de afecti-

20 Señala la doctrina que "se vulnerará este derecho fundamental cuando la penetración en el ámbito propio y reservado del sujeto, aun autorizada en un principio, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando así la conexión, entre la información personal que se recaba y el objeto tolerado para el que fue recogida". VILLEGAS GARCÍA, M.A., "Imágenes íntimas e internet. Cerco legislativo a la venganza privada en la red", en *Aranzadi*, número 876, 2014, pág. 2

vidad. No obstante, esta agravación se aplica independientemente si la violencia es de género o doméstica, puesto que se penaliza tanto al hombre que difunde "sexting" ajeno, como a la mujer.

En la práctica, en la mayoría de los casos en los que los tribunales han resuelto sobre esta figura son casos donde la víctima era mujer[21] y de ello ha sido consciente nuestro legislador puesto que en la propia Exposición de Motivos de la L.O. 1/2015 reclamaba la necesidad de dar una mayor protección a la mujer con la creación de nuevos tipos penales entre ellos el de "sexting". Por tanto, aunque se penaliza tanto a la mujer como al hombre que difunde videos o imágenes de otra persona, lo que se entiende como "sexting", el hecho de que en la práctica mayoría de los casos enjuiciados la víctima ha sido una mujer nos permite pensar con gran acierto que el legislador ha creado estas nuevas figuras delictivas para proteger precisamente a la mujer.

La agravación de la pena tiene el fundamento, a mi parecer, en la mayor lesividad que se produce en el derecho a la intimidad basada en la especial relación de confianza, por ello, cuando existe una relación de afectividad la vulneración del derecho a la intimidad es más grave puesto que se produce una injustificada traición a la expectativa de confidencialidad[22]. Como indica la doctrina, en la práctica este supuesto agravado se aplicará con mayor frecuencia que el básico, pues es más fácil la captación de imágenes sensibles entre personas que han tenido una relación afectiva, aunque haya sido breve en el tiempo, que entre aquellas que no la han tenido[23].

No obstante, el legislador no diferencia entre violencia de género o violencia doméstica, no existe una tutela penal reforzada por violencia de género.

---

21 Señala PÉREZ CONCHILLO, "La difusión de sexting ajeno como violencia de género", en *Revista Aranzadi de Derecho y Proceso Penal*, 2018, núm. 51, que "la mayoría de sexting que se han planteado a la jurisprudencia hasta ahora muestras como elementos comunes los siguientes: 1) existencia de relación sentimental, 2) Captación consentida de imágenes o grabaciones en las que la víctima es fundamentalmente la mujer, ya sean captadas por ella y luego compartidas con la pareja o bien directamente tomadas por la pareja mediando consentimiento de la mujer, 3) traición a la expectativa de confidencialidad, reenviando la pareja las fotografías o vídeos de terceros, bien en un intento de alarde, bien tras la ruptura de la relación con un ánimo de venganza, amenaza, etc".

22 Véase a PÉREZ CONCHILLO, Eloísa, "La difusión de sexting ajeno como violencia de género", op. cit.

23 Véase a GONZÁLEZ COLLANTES, TÁLIA, "Los delitos contra la intimidad tras la reforma de 2015: Luces y sombras", en *Revista de Derecho penal y criminología*, 3.ª Época, n.º 13 (enero de 2015), págs. 71.

b. El delito de "sextorsión"

b.1. Delimitación conceptual

Podemos decir que la extorsión es el paso siguiente al delito de "sexting", y si hablamos de hacerlo de forma *on line*, lo denominamos "sextorsión", que no sería más que un chantaje de tipo sexual *on line*.

Así, el delito de "sextorsion" o abuso sexual *on line* tipifica la conducta consistente en la tenencia de imágenes íntimas para chantajear a la víctima con la finalidad de ejercer control y dominio bajo amenaza para bien tener relaciones sexuales o bien otras finalidades[24]. La jurisprudencia ha venido recogiendo la expresión de *sextorsión* para denominar a los actos delictivos de abusos sexuales cometidos por internet y con la extorsión que lleva implícita la falta de consentimiento de las víctimas[25].

Si el chantaje se hace a quien ha sido o es tu pareja es un delito de violencia de género. En estos supuestos el chantaje puede consistir en continuar la relación de pareja o mantener relaciones sexuales con la misma.

Esta conducta puede ser tipificada como un delito de coacciones del art. 172 del Código Penal[26], y si procediera a la difusión de las imágenes puede incurrir en un delito de "sexting", comentado anteriormente y tipificado en el artículo 197.7 del Código Penal, con la agravante de que, si éstas se obtuvieron sin consentimiento, nos llevaría al delito tipificado en el art. 197.3 del CP. Además, hay que tener en cuenta la posible comisión de otros delitos contra la libertad sexual.

El Tribunal Supremo en STS 377/2018, de 23 de julio, analizó un caso en el que se enjuiciaba un delito de abuso sexual *on line* en el que el delincuente para acceder al contenido del ordenador de la víctima lo infectaba con un virus que le permitía el acceso, para después obtener imágenes y videos privados que podían comprometer su intimidad si los mismos se llegaban a difundir. El Tribunal Supremo en dicha sentencia señaló que: "*generalmente el "modus operandi" consiste en la mecánica por la que el autor del delito*

24 Véase a DELGADO MARTÍN, Joaquín, *Investigación tecnológica*..., op. cit., pág. 342.

25 Véase la STS 377/2018, de 23 de julio, Núm. Cendoj: 28079120012018100388.

26 En dicho artículo 172 del Código Penal, apartado 1, se establece que: "*1. El que, sin estar legítimamente autorizado, impidiere a otro con violencia hacer lo que la ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto, será castigado con la pena de prisión de seis meses a tres años o con multa de 12 a 24 meses, según la gravedad de la coacción o de los medios empleados*".

envía un correo electrónico a su víctima con un enlace atractivo para ella, y al "pinchar" en el mismo se descarga el "malware" en su ordenador"[27]. Con ello, el delincuente tenía acceso a sus contenidos y podía descargarse archivos e imágenes o videos, los cuales servían para posteriormente llevar a cabo la extorsión, lo que lleva a calificar los actos como "sextorsión"[28].

En dicho asunto, al acusado se le condenó por un lado a cuatro delitos continuados de abusos sexuales cometidos por internet y, por otro lado, también se le condenó por delitos de amenazas y contra la intimidad del art. 197 del Código Penal con distintas mujeres víctimas, puesto que en este caso al registrar el ordenador del acusado se encontraron datos de otras mujeres víctimas de hechos semejantes a los que se estaban investigando tras el registro con consentimiento del ordenador del autor de los hechos de la primera a las cuales se las citó.

En este asunto se analizan distintas cuestiones, por un lado, se analiza el delito de abusos sexuales del art. 181 del CP cometido por internet o "sextorsión" y, por otro lado, se examinan las diligencias de investigación llevadas a cabo por la policía para localizar los archivos informáticos que conducían a la comisión del delito contemplado en el art. 197 del CP[29].

No obstante, como señalé anteriormente, la primera sentencia anterior a la reforma del Código Penal de 2015, recogiendo un caso de "sexting" fue la dictada por la Audiencia Provincial de Granada el 5 de junio de 2014 resol-

---

27 Como se indica en el *Estudio sobre la Cibercriminalidad en España*, 2018, pág.15, www.interior.gob.es, "*cabe reseñar que los cibercriminales se van adaptando con mayor rapidez a ciertos entornos, como pueden ser el mayor uso por parte de los usuarios de los dispositivos móviles*". En este sentido, en el Informe Anual 2018 de "Dispositivos y comunicaciones móviles" (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3009-ccn-cert-bp-08-redes- sociales/file.html), del Centro Criptológico Nacional, citado en el *Estudio sobre la Cibercriminalidad en España*, se estudian diferentes peligros de seguridad vinculados a los mismos como son: la adopción de las últimas versiones de los sistemas operativos, el mecanismo de autentificación biométrica, el desbloqueo y extracción forense datos, los mecanismos de seguridad avanzada y código dañino, y la privacidad en plataformas móviles. En definitiva, se observa un elevado uso a nivel mundial del malware móvil, extremo que se ve corroborado por otros informes internacionales.

28 En https://vlex.es/vid/736120665?_ga=2.211779221.1850157538.1590854. También véase el comentario que se hace sobre esta sentencia en GALLARDO, Miguel, en *Extorsionabilidad, extorsionistas y extorsionología pericial forense Hacia la victimología de los chantajeados por "extorsionoscopia"*, en https://www.miguelgallardo.es/extorsionologo.pdf.

29 Ibídem.

viendo a favor de los imputados. En esta sentencia se puso de manifiesto que en el artículo 197 del CP se exige el acceso sin consentimiento a un secreto para que concurra el delito de descubrimiento y revelación de secretos. Al ser la misma menor la quien envió la imagen al acusado no habría falta de consentimiento. Aunque sea menor de edad (en el momento de los hechos tenía 15 años, anterior a la reforma del Código Penal elevando la edad para mantener relaciones sexuales consentidas a los 16 años), su consentimiento es válido, pues lo que se sostiene es que si el Legislador considera válido el consentimiento de una persona a partir de los trece años (actualmente 16 años) para mantener relaciones sexuales, también lo es para enviar una fotografía donde aparece desnuda. En este sentido el Tribunal Supremo estimó el recurso de apelación[30]. La atipicidad en aquel momento de la conducta condujo a la absolución no solo de los recurrentes sino también del condenado no recurrente por el efecto expansivo que para el recurso de casación se prevé en el artículo 903 de la Ley de Enjuiciamiento Criminal.

La relevancia de la sentencia estribó fundamentalmente en dar un concepto del delito de "sexting" que lo definió como "*el envío de imágenes estáticas (fotografías) o dinámicas (vídeos) de contenido sexual de mayor o menor carga erótica entre personas que voluntariamente consienten en ello y, que forma parte de su actividad sexual que se desarrolla de manera libre*".

En definitiva, Internet se consolida como un medio relevante para la comisión de delitos que con anterioridad tenían lugar mediante otros procedimientos más basados en el contacto personal y directo entre víctima y autor. Las posibilidades que ofrece Internet para perpetrar hechos delictivos son muy variadas. En este sentido, se viene hablando del uso de la "ingeniería social" en las redes sociales como el instrumento que posibilita a los delincuentes la obtención de información sobre datos personales relevantes sobre sus víctimas que hace más creíbles las amenazas y extorsiones. Los delincuentes utilizan técnicas básicas de "ingeniería social" efectuadas a partir del análisis de la huella en redes sociales de las víctimas para la comisión de los hechos delictivos.

En una operación que recientemente llevó a cabo la Guardia Civil sobre extorsiones tras la contratación de servicios sexuales en páginas web, los delincuentes utilizaban esa técnica de ingeniería social para formar un perfil de la víctima y poderlas extorsionar. Así, en estos casos las víctimas asumían que sus datos personales (identidad, trabajo, dirección, teléfono...etc) y los de

30 Véase en https://2019.vlex.com/#vid/542256650.

su entorno, eran perfectamente conocidos por los delincuentes. Igualmente se hacían creer a las víctimas (y en algunos casos así era) que se disponía de imágenes y grabaciones de audio sobre las relaciones que en su caso había mantenido. De esta forma, muchas de las víctimas realizaban los pagos solicitados por vergüenza a que sus familiares y entorno fueran conocedores de la contratación de este tipo de servicios, lo que podía dar lugar, siendo éste un hecho diferencial frente a otros tipos de extorsiones que no se basan en explotar la vida íntima y personal de las víctimas, a que no se llegase a interponer denuncia por temor a que los hechos trascendieran hacia dicho entorno[31].

c. El delito de "stalking"

c.1. Delimitación conceptual

Se trata de una modalidad de acoso por la red y aplicaciones móviles que describe un "acecho" incesante o reiterado a otra persona. De nuevo es un anglicismo que deriva del verbo "acechar", que según el diccionario de la Real Academia Española significa "observar, aguardar cautelosamente con algún propósito". En la práctica[32] este tipo de acecho o acoso afecta más a mujeres que a hombres y se suele dar en el ámbito de la violencia de género, pero el tipo básico regulado en el Código Penal no diferencia entre hombres o mujeres. En estos casos la gravedad del delito y por lo tanto la pena es mayor, así se establecen penas de prisión de entre uno y dos años o trabajos en beneficio de la comunidad de entre 60 y 120 días.

Aunque este delito tiene bastantes similitudes con otras conductas delictivas, como las amenazas o las coacciones, sin embargo, tiene características propias que le diferencia de ellas.

En concreto, el delito de "stalking" está regulado en el Código Penal dentro de los delitos contra la libertad y se regula por primera vez tras la reforma introducida por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal, incluyéndose como delito autónomo en un nuevo artículo -art. 172 ter-, dentro de los delitos contra la libertad de obrar, por lo que anteriormente estas conductas quedaban impunes a no ser que se encajaran dentro del maltrato psicológico. De hecho, hasta entonces la jurisprudencia

31 Documento de análisis de riesgos y difusión operativa, DARDO 3/2019.

32 Véase la Macroencuesta de violencia contra la mujer de 2009. Delegación del Gobierno contra la violencia de género, en https://violenciagenero.igualdad.gob.es/violenciaEnCifras/macroencuesta2015/pdf/Macroencuesta_2019_estudio_investigacion.pdf.

venía utilizando distintos delitos para incriminar las conductas de acoso persecutorio.

Tal y como se pone de manifiesto en la Exposición de Motivos de la ley de 2015 lo que se penaliza son "las conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la víctima, a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas, u otros actos continuos de hostigamiento". Para castigar esta conducta es necesario que la víctima vea limitada su libertad de obrar no valdría sólo con infundirle temor, sino que es necesario que exista una estrategia de persecución que le limite la libertad de obrar, entendida como la capacidad de decidir libremente, por lo que la conducta tiene que ser insistente y continuada, descartándose los actos aislados, debe por consiguiente alterar el *modus vivendi* de la víctima.

Muy poco después de introducirse este nuevo delito en el Código Penal, el Juzgado de Instrucción número 3 de Tudela, Navarra, dictó una relevante sentencia, de 23 de marzo de 2016[33], donde analizaba los requisitos y características del nuevo delito de acoso reiterado e ilegítimo[34]. Fue la primera sentencia de carácter condenatorio por el nuevo delito de acoso o "stalking" donde se definen de manera genérica todos los elementos del tipo delictivo.

Como se establece en dicha sentencia, las conductas incardinadas en el delito de "stalking" atañen al proceso de formación de la voluntad de la víctima puesto que la sensación de temor e intranquilidad o angustia que produce el continuo acechamiento por parte del acosador, le lleva a modificar todos sus hábitos, tanto sus horarios, como sus lugares de paso, sus números de teléfono, cuentas de correo electrónico e incluso de lugar de trabajo y de residencia[35]. Además de protegerse el bien jurídico de libertad también se protege el bien jurídico de la seguridad en el sentido del derecho al sosiego y a la tranquilidad personal. Sin embargo, se recalca en la sentencia que "sólo adquirirán relevancia penal las conductas que limiten la libertad de obrar del sujeto pasivo, sin que el mero sentimiento de temor o molestia sea punible"[36].

---

33 En los hechos probados de la sentencia se recoge que, conociendo a la denunciante por haber perdido y posteriormente recuperado a su perro, comienzan continuas llamadas telefónicas a la víctima, así como también mensajes de WhatsApp escritos y de audio, en un primer momento enviándoles fotografías para finalmente remitirle mensajes de contenido sexual, provocando una alteración de la vida normal de la denunciante.

34 ECLI: ES: JI:2 016: 3, Cendoj 31232430032016100001.

35 Ibídem.

36 Ibídem.

Entre los bienes jurídicos que pueden verse afectos por la conducta de "stalking" estaría en primer lugar la libertad, también estarían el honor, la integridad moral o la intimidad, dependiendo de los actos en los que se concrete el acoso.

Se trata de un delito común, por lo que puede cometerse por cualquier persona frente a cualquier otra. Si bien, como se indica en la sentencia, se trata de un delito que se introduce pensando en el ámbito de la violencia de género[37], sin embargo, el legislador no lo ha limitado al ámbito de la violencia de género, puesto que no se exigen características específicas del sujeto activo y pasivo, incluyendo tanto hombres como mujeres y siendo la relación entre ellos irrelevante. No obstante, se establece un subtipo agravado para los supuestos en los que el acoso se lleve a cabo en el ámbito familiar[38]. En estos casos, a diferencia del tipo básico no se exige la denuncia previa de la persona agraviada. Existe además una especial protección también a través de las figuras agravadas cuando la víctima es una persona especialmente vulnerable por razón de su edad, enfermedad o situación.

La norma incluye en la propia definición del delito el término "acosar" para referirse posteriormente a cómo debe realizarse dicho acoso, que es "llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes". En este sentido, no se establece el número de veces que debe realizarse la conducta para que sea relevante

37 De hecho, la incorporación de ese delito obedece fundamentalmente a la propuesta de criminalización del acoso que se lleva a cabo en el artículo 34 del Convenio del Consejo de Europa para la Prevención y la Lucha contra la Violencia contra las Mujeres y la Violencia Doméstica, adoptado en Estambul el 11 de mayo de 2011, firmado y ratificado por España y en vigor desde agosto del 2014.

38 En este sentido, se fija un subtipo agravado castigado con pena de prisión de uno a dos años o trabajos en beneficio de la comunidad de sesenta a ciento veinte días, cuando las víctimas fueran alguna de las personas que se incluyen en el artículo 173.2 del Código penal:

– Quienes sean o hayan sido cónyuges del autor o hayan estado ligados a él por relación análoga de afectividad, aun sin convivencia.

– Descendientes, ascendientes, hermanos por naturaleza, afinidad o adopción, propios o del cónyuge conviviente.

– Menores o personas con discapacidad necesitadas de especial protección que convivan con él o que se hallen sujetos a la potestad, tutela, curatela, acogimiento o guarda de hecho del cónyuge o conviviente, o sobre persona amparada en cualquier otra relación por la que se encuentre integrada en el núcleo de su convivencia familiar.

– Personas que por su especial vulnerabilidad se encuentran sometidas a custodia en centros públicos o privados.

penalmente, pero queda claro con la expresión "de forma insistente y reiterada" que nos encontramos ante un patrón de conducta y no de actos aislados que pueda llevar a cabo. Además, es necesario que la conducta a parte de ser "insistente y reiterada" implique una maniobra de persecución constante, compuesta por distintas acciones encaminadas al logro de una determinada finalidad que las vincule entre sí.

Está asentado tanto por la doctrina como por la jurisprudencia que lo esencial en el "stalking" sería la estrategia sistemática de persecución, no las características de las acciones en que ésta se concreta[39].

c.2. Conductas objeto de delito

Las conductas que puede adoptar el acechador son variadas, de acuerdo al artículo 172 ter del Código Penal, serían las siguientes:

1. La vigile, la persiga o busque su cercanía física. Tal y como se indica en la sentencia citada[40], no sólo se penalizan conductas de proximidad física sino también de observación a distancia y a través de dispositivos electrónicos como GPS y cámaras de video vigilancia.

2. Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas. Igualmente, establece la jurisprudencia que se incluye en esta conducta tanto la tentativa de contacto como el propio contacto.

3. Mediante el uso indebido de sus datos personales, adquiriera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella. Por tanto, se comprenderían dentro de esta conducta los supuestos en los que el sujeto activo publica un anuncio en Internet ofreciendo algún servicio que conlleva que la víctima reciba múltiples llamadas.

4. Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella. No queda claro qué clase de atentado contra la libertad o patrimonio puede incluirse, en el sentido de si es de los que ya están específicamente tipificados en el Código Penal, o por el contrario se incluirían además conductas no tipificadas como delito. A este

39 RUIZ SIERRA, Joana, "El delito de "stalking"", en *Revista Foro FICP (Tribuna y Boletín de la FICP)*, 2017-2 (septiembre 2017), pág. 553 y ss, en https://ficp.es/wp-content/uploads/2013/06/Foro-FICP-2017-2.pdf.

40 Sentencia del Juzgado de Instrucción de Tudela, Navarra de 23 de marzo de 2016, citada anteriormente.

respecto la doctrina no es unánime, parte de la doctrina defiende la inclusión de la amenaza de atentado a la libertad, y de la amenaza y atentado contra la vida y la integridad física. Si bien estos delitos ya se encuentran tipificados en el propio delito de amenazas o coacciones, es cierto que también lo están los correspondientes delitos contra el patrimonio y contra la libertad[41].

La primera vez que se mide estadísticamente el acoso sexual y el acoso reiterado (stalking) es en el año 2019, son datos que se reflejan en la *Macroencuesta de Violencia contra la Mujer de 2019*, elaborada por la Delegación de Gobierno contra la Violencia de Género[42]. En esta Macroencuesta en concreto en relación con el acoso sexual se preguntaba por varios comportamientos no deseados y con una connotación sexual, en concreto, se hacía hincapié entre estas conductas a miradas insistentes o lascivas, contacto físico no deseado, exhibicionismo, envío de imágenes o fotos sexualmente explícitas que le hayan hecho sentirse ofendida, humillada, o intimidada a la mujer, por citar algunos ejemplos. En relación a ello, la encuesta refleja que 3 de cada 4 (75,2%) afirman que el acoso sexual ha ocurrido más de una vez y en la franja de edad de 16 a 24 años el 60,5% de las mujeres han sufrido acoso sexual.

En concreto a la conducta de "stalking" o acoso reiterado, en la encuesta se realizaban distintas preguntas a las mujeres entrevistadas, en concreto, se les preguntaba por diferentes comportamientos llevados a cabo por una misma persona de forma repetida causando miedo, ansiedad o angustia a la mujer entrevistada, como podían ser las llamadas telefónicas obscenas, amenazantes, molestas o silenciosas, que a la mujer le hayan seguido o espiado, que le hayan dañado intencionadamente cosas suyas o le hayan hecho propuestas inapropiadas en internet o en redes sociales, por citar algunos ejemplos. Los datos reflejan que el porcentaje de mujeres de 16 o más años que han sufrido "stalking" a lo largo de su vida es el 15,2 % y de este porcentaje el 3,7 % en la infancia. Además, casi el 60% de las mujeres que han sufrido "stalking" lo sufrían con una frecuencia semanal o diaria. Finalmente, en relación al tipo de agresor el 87,9 % eran hombres, de ellos, el 33,6 % eran desconocidos, el 39,9 % eran amigos o conocidos y el 21,3 % era pareja o expareja masculina[43].

41 Véase a DELGADO MORÁN, Juan José, *Sociedad de Control y Panóptico Electrónico. La Victima de la Videovigilancia*, Murcia, septiembre, 2018, en http://repositorio.ucam.edu/bitstream/handle/10952/3839/Tesis.pdf?isAllowed=y&sequence=1.

42 Véase los principales resultados en la página siguiente: https://violenciagenero.igualdad.gob.es/violenciaEnCifras/macroencuesta2015/pdf/Principales_Resultados_Macroencuesta2019.pdf.

43 Los datos recogidos en la Macroencuesta citada anteriormente serían los siguientes:

En definitiva, la encuesta refleja datos más que preocupantes que evidencian la necesidad de actuar urgentemente contra estas conductas delictivas, tanto desde la prevención como en la persecución y sanción penal.

c.3. El cyberstalking

Por otro lado, una concreta forma de "stalking", o diferente modalidad a la anterior es la denominada "cyberstalking", es la misma conducta que la descrita, aunque adaptada a la sociedad actual donde predomina el uso de las nuevas tecnologías, por tanto, aunque parte de la misma conducta tiene singularidades respecto al "stalking" tradicional, constituye un fenómeno cada vez más creciente en nuestra sociedad surgido a raíz de la evolución de las nuevas tecnologías de la comunicación y de la información. Cuando el acechamiento y hostigamiento se haga a través de las nuevas tecnologías o Internet se denomina "cyberstalking". Las características propias del ámbito en el que se desarrollan estos delitos conllevan que presente especialidades con respecto al "stalking" tradicional, como es el anonimato de quien lleva a cabo la conducta de hostigamiento, la difusión masiva a través de las redes, o la ausencia de barreras físicas y temporales, lo que implica que afecte aun si cabe más los bienes jurídicos de la víctima[44].

"El 12,1% de las mujeres que han sufrido stalking alguna vez en la vida lo denunciaron en la Policía, en la Guardia Civil o en el juzgado y el 4,5% acudieron a un servicio médico o de atención psicológica. El porcentaje de denuncia en la Policía, Guardia Civil o en el juzgado, aun siendo bajo, es superior al de denuncia por acoso sexual o por violencia sexual fuera de la pareja. Más habitual es contar el stalking a alguien del entorno: el 43,7% de las mujeres que han sufrido stalking lo hablaron con un amigo o amiga, el 32,7% con un familiar y el 19,4% con su pareja o expareja. El 22,8% afirma que no se lo contó a nadie".

En relación con mujeres con discapacidad, en el mismo estudio se refleja que "no hay diferencias estadísticamente significativas entre las mujeres con y sin discapacidad acreditada en relación con la prevalencia del acoso reiterado a lo largo de la vida, en los últimos 4 años, en los 12 meses previos a las entrevistas, o en la infancia. Tampoco hay diferencias significativas en la frecuencia con la que ha tenido lugar el stalking. Si bien, las mujeres con discapacidad que han sufrido stalking lo han denunciado en mayor medida (22,0%) que las mujeres sin discapacidad (11,4%). Lo mismo sucede en el caso de la ayuda formal: el 27,1% de las mujeres con discapacidad que han sufrido stalking han buscado ayuda formal para afrontar sus consecuencias frente al 14,0% de las mujeres sin discapacidad. En cambio, las mujeres con discapacidad que han sufrido acoso sexual han contado lo sucedido a personas del entorno en menor medida (57,0%) que las mujeres sin discapacidad (70,2%)".

44 Para mayor profundidad sobre las características, véase a GARCÍA GONZÁLEZ, J.,

Aunque reitero que es la misma conducta, pero adaptada a la sociedad de la información y de la comunicación, la peculiaridad es que en relación con la investigación y persecución de este delito en la modalidad de "cyberstalking" supone una mayor dificultad a la hora de descubrir la autoría como ocurre con todos los delitos que se cometen *on line*. Brevemente señalar que, dentro de las diligencias de investigación, la identificación del autor dependerá de la efectiva localización del aparato desde el que se ha llevado a cabo la comisión de los hechos delictivos, puesto que, como veremos más adelante, todos los aparatos tienen asignada una IP que una vez localizada es necesario saber a qué usuario ha sido asignada, para lo cual se necesitará autorización judicial[45]. El Tribunal Supremo ha manifestado que "el carácter de la dirección IP como dato personal ha sido reconocido por la jurisprudencia de esta Sala en numerosas resoluciones (cfr. por todas, SSTS 249/2008, 20 de mayo; 236/2008, 9 de mayo; 680/2010, 14 de julio y 292/2008, 28 de mayo)[46].

El siguiente paso consistirá en acceder a la información, datos que necesariamente deben conservar las operadoras de telecomunicaciones y redes y que una vez solicitado por la autoridad judicial deben ceder, tal y como se indica en la Ley 25/2007, de 18 de octubre de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Si, además existe algún elemento transfronterizo es necesario acudir a la cooperación judicial internacional puesto que de otra forma es difícil la averiguación y persecución del autor del delito, así como de la obtención de la prueba que le incrimine.

Añadido a los problemas de autoría están las dificultades de determinar la jurisdicción competente y la ley aplicable puesto que en estos delitos cometidos *on line* o en el ciberespacio no existen fronteras físicas, por lo que determinar el lugar de comisión es tarea más que ardua.

Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, Tirant lo Blanch, Valencia, 2010, págs. 17 y ss.

45 Señala FLORES PRADA, I., que "*dentro de la Red, cada ordenador que se conecta a Internet se identifica por medio de lo que se conoce como dirección IP. Ésta se compone de cuatro grupos de números comprendidos entre el 0 y el 255 y separados por puntos. El usuario de Internet no necesita conocer ninguna de estas direcciones IP para comunicarse. Las direcciones las usan los ordenadores en la comunicación por medio del denominado protocolo TCP/IP de manera transparente para el usuario*", en "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia", en *Revista Electrónica de Ciencia Penal y Criminología*, núm. 17, 2015. Disponible en internet: http://criminet.ugr.es/recpc/17/recpc17-21.pdf.

46 Véase la STS 342/2013, 17 de abril de 2013, en https://vlex.es/vid/438315958.

d. El delito de "grooming"

d.1. Delimitación conceptual

La palabra "grooming" deriva del verbo inglés "groom", que se refiere a conductas de "acercamiento o preparación para un fin determinado".

El delito de "grooming" está regulado en el Capítulo II bis "De los abusos y agresiones sexuales a los menores de dieciséis años" del Título VIII "De los delitos contra la libertad e indemnidad sexual" del Código Penal, en concreto, en el artículo 183 ter, añadido por la Ley Orgánica 1/2015, de reforma del Código Penal, se indica que: "*1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183*[47]

47 En dicho artículo se indica literalmente que: "*1. El que realizare actos de carácter sexual con un menor de dieciséis años, será castigado como responsable de abuso sexual a un menor con la pena de prisión de dos a seis años.*

2. Cuando los hechos se cometan empleando violencia o intimidación, el responsable será castigado por el delito de agresión sexual a un menor con la pena de cinco a diez años de prisión. Las mismas penas se impondrán cuando mediante violencia o intimidación compeliere a un menor de dieciséis años a participar en actos de naturaleza sexual con un tercero o a realizarlos sobre sí mismo.

3. Cuando el ataque consista en acceso carnal por vía vaginal, anal o bucal, o introducción de miembros corporales u objetos por alguna de las dos primeras vías, el responsable será castigado con la pena de prisión de ocho a doce años, en el caso del apartado 1, y con la pena de doce a quince años, en el caso del apartado 2.

4. Las conductas previstas en los tres apartados anteriores serán castigadas con la pena de prisión correspondiente en su mitad superior cuando concurra alguna de las siguientes circunstancias:

a) Cuando el escaso desarrollo intelectual o físico de la víctima, o el hecho de tener un trastorno mental, la hubiera colocado en una situación de total indefensión y en todo caso, cuando sea menor de cuatro años.

b) Cuando los hechos se cometan por la actuación conjunta de dos o más personas.

c) Cuando la violencia o intimidación ejercidas revistan un carácter particularmente degradante o vejatorio.

d) Cuando, para la ejecución del delito, el responsable se haya prevalido de una relación de superioridad o parentesco, por ser ascendiente, o hermano, por naturaleza o adopción, o afines, con la víctima.

e) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

y 189[48]*, siempre que tal propuesta se acompañe de actos materiales enca-*

f) Cuando la infracción se haya cometido en el seno de una organización o de un grupo criminal que se dedicare a la realización de tales actividades.

5. En todos los casos previstos en este artículo, cuando el culpable se hubiera prevalido de su condición de autoridad, agente de esta o funcionario público, se impondrá, además, la pena de inhabilitación absoluta de seis a doce años".

48 Se establece que: "*1. Será castigado con la pena de prisión de uno a cinco años:*

a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.

b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.

c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

2. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:

a) Cuando se utilice a menores de dieciséis años.

b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio.

c) Cuando el material pornográfico represente a menores o a personas con discapacidad necesitadas de especial protección que sean víctimas de violencia física o sexual.

d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

minados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas

---

e) Cuando el material pornográfico fuera de notoria importancia.

f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

g) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, del menor o persona con discapacidad necesitada de especial protección, o se trate de cualquier otro miembro de su familia que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.

h) Cuando concurra la agravante de reincidencia.

3. Si los hechos a que se refiere la letra a) del párrafo primero del apartado 1 se hubieran cometido con violencia o intimidación se impondrá la pena superior en grado a las previstas en los apartados anteriores.

4. El que asistiere a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de seis meses a dos años de prisión.

5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación.

6. El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o una persona con discapacidad necesitada de especial protección y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o persona con discapacidad necesitada de especial protección, será castigado con la pena de prisión de tres a seis meses o multa de seis a doce meses.

7. El Ministerio Fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.

8. Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español.

Estas medidas podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal.

correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.

2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años".

Por tanto, las conductas que engloban el delito de "grooming" requieren:

a) Un contacto a través de los medios tecnológicos con un menor de 16 años para su captación.

b) Proponer un encuentro para cometer cualquiera de los delitos descritos en los artículos 183 a 189 del CP.

c) El llevar a cabo actos materiales encaminados al acercamiento.

d) La voluntariedad de cometer cualquiera de los delitos de los artículos 183 y 189 del CP[49].

Esta conducta delictiva se cataloga como delito de peligro o de riesgo puesto que no es necesario que exista un resultado o lesión, sino que se castiga la puesta en peligro de la indemnidad sexual del menor de 16 años[50]. Con anterioridad a la reforma por la Ley Orgánica 1/2015, la edad del menor estaba situada en 13 años. Por tanto, como indica la jurisprudencia "en relación con su naturaleza se trata de un supuesto en el que el derecho penal adelanta las barreras de protección, castigando la que, en realidad, es un acto preparatorio para la comisión de abusos sexuales a menores de 16 años (la sentencia citada se refirió a 13 años porque es anterior a la reforma de 2015)"[51].

---

49 FERNÁNDEZ NIETO, Josefa, "Reforma del Código Penal hacia una nueva dimensión de la protección en los delitos de sexting y grooming", op. cit., pág. 8.

50 Ibídem, pág. 5.

Señala VELASCO, Eloy, y SANCHIS CRESPO, Carolina, *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, Valencia, 2019, pág. 159, que se configura como "un delito de peligro, un adelantamiento de la barrera de protección que castiga un acto preparatorio para la comisión de abusos sexuales de menores de 13 años –hoy, de 16– y que no requiere contacto físico entre agresor y agredido, configurando un nuevo tipo delictivo que trasciende al mero acto preparatorio, aunque participa de su naturaleza, por cuanto sólo con el fin de cometer abusos sexuales a menor de 13 años (ahora 16), ya es típica la conducta".

51 STS 823/2015, en Tirant on line, DOCUMENTO TOL4.776.958. En este sentido,

Por tanto, esta conducta estaría tipificada independientemente de las penas que quepa además imponer por los demás delitos cometidos, ya sea abuso o agresión sexual o cualquiera de los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores. Si no se materializa efectivamente la conducta sexual entonces el delito de "grooming" se castigará como tal sin añadir ninguna pena más.

La primera sentencia (anterior a la reforma del CP por la Ley Orgánica 1/2015) condenando por el delito de "grooming" es la STS 823/2015, de 24 de febrero[52] en la que un adulto, mayor de edad, contacta con un menor de 11 años a través de las redes sociales, Twiter, Facebook, Tuenti, llegándole a regalarla un móvil para comunicarse con él vía Whatsapp. La intención del adulto es tener contacto sexual con el menor, a quien le llega a ofrecer dinero con dicho objetivo. En esta sentencia se describe la conducta tipificada como "grooming" cuando se refiere a: "*las acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un menor con el fin de preparar el terreno para el abuso sexual del menor. En cuanto a la naturaleza se trata de un supuesto en el que el derecho penal adelanta las barreras de protección, castigando la que, en realidad, es un acto preparatorio para la comisión de abusos sexuales a menores de 13 años. La naturaleza de este delito es de peligro por cuanto se configura no ateniendo a la lesión efectiva del bien jurídico protegido, sino a un comportamiento peligroso para dicho bien. Por ello, el bien jurídico protegido es la indemnidad sexual de los menores de 13 años más allá de su libertad sexual*"[53].

Esta sentencia hace referencia a la amplitud del ámbito del tipo objetivo al establecer que el legislador no establece una lista cerrada de actos que se

---

el TS indica en dicha sentencia que "*el acto preparatorio pertenece a la fase interna y no externa o ejecutiva del delito, existiendo unanimidad en reconocer la irrelevancia penal a todo proyecto que no supere los límites de una fase interna. Ahora bien, en este caso, el legislador expresamente ha considerado que las conductas de ciberacoso sexual son un acto ejecutivo de un nuevo delito que trasciende al mero acto preparatorio, aunque participan de su naturaleza, por cuanto solo con el fin de cometer los delitos de abusos sexuales a menores de 13 años puede entenderse típica la conducta.*

La naturaleza de este delito es de peligro por cuanto se configura no atendiendo a la lesión efectiva del bien jurídico protegido, sino a un comportamiento peligroso para dicho bien".

52 La Ley 18405/2015. También en Tirant on line, DOCUMENTO TOL4.776.958. ECLI:ES:TS:2015:823

53 Fundamento jurídico 3 de la STS 823/2015.

tienen que dar para llegar a un acercamiento con el menor, sino que se está ante un *numerus apertus* de actos y solo concreta que la naturaleza del acto es material y no meramente formal.

No obstante, como ha resaltado la doctrina, el delito de "*grooming"* no es que sea un fenómeno reciente, puesto que dejando a un lado su modalidad tecnológica ha venido acompañando a un número considerable de casos de abuso en los que estas tecnolo´gias no habían tenido nada que ver. No obstante, la doctrina destaca que "*el peligro que representa ha sido socialmente construido y ha tomado verdadera relevancia a partir del momento en que este tipo de conductas han accedido a la Red*"[54], es cierto, que con la llegada de la era digital estas conductas se han visto aumentadas puesto que la red facilita la comisión de actividades delictivas. Además, también hay que tener en cuenta que el número de menores que actualmente acceden a las redes sociales se ha visto considerablemente aumentado[55]. Y a todo ello hay que añadir además la situación actual por la que estamos atravesando provocada por la crisis del virus del Covid-19, que ha propiciado que nos tengamos que aislar y ello ha provocado a su vez que se haya aumentado el uso de Internet como forma de comunicarnos y relacionarnos.

El Tribunal Supremo ha dictado una sentencia recientemente muy relevante porque hace alusión expresa a la "ciberintimidación", concepto de nuevo cuño, en la misma pone en contexto la violencia sexual a través de la intimidación "on line" o digital, y concluye que "*los supuestos de ciberviolencia o ciberintimidacón sexual pueden alcanzar la tasa de idoneidad y lesividad exigible a la violencia* o intimidación *típica empleada en los delitos de agresión sexual"*. El Tribunal Supremo en los hechos objeto de esta reso-

54 VILLACAMPA ESTIARTE, Carolina, *El delito de online child grooming o propuesta sexual telemática a menores*, 2015, Tirant on line, TOL5.204.097.

55 Véase al respecto los dos Informes emitidos por EU Kids Online, en *ehu.eus*:

– EU Kids Online I (2006-2009), financiado por el Programa Safer Internet Plus de la Comisión Europea, es una red de 21 países europeos que tiene por objetivo examinar los aspectos culturales y contextuales y los riesgos del uso de las tecnologías online entre menores en Europa.

– EU Kids Online II (2009-2011) es un proyecto de investigación diseñado para examinar las experiencias de uso, riesgos y seguridad online de los niños, niñas, padres y madres en Europa.

– En la edición del informe español, el equipo de EU Kids Online Spain (UPV/EHU), ha contado con el apoyo institucional del Instituto Nacional de Ciberseguridad (INCIBE) a través de Internet Segura for Kids, en el marco del proyecto SIC -Spain.

lución considera que no solamente hubo una conducta de embaucamiento, tal y como se exige en el 183 ter.2 de la LECRim, por engaño para obtener las grabaciones de la menor tocándose, sino que hubo un verdadero escenario de intimidación y la intimidación empleada fue muy intensa y potente al amenazar a la menor con revelar las imágenes a todos sus contactos y denunciar a sus padres, causándole miedo y atemorizándola.

El Tribunal Supremo destaca que en estos casos la dimensión social de las TIC que facilita el intercambio de imágenes y vídeos de los actos de cosificación sexual, puede ser un *potentísimo instrumento de intimidación,* que ha dado lugar al llamado escenario digital de la polivictimización. Y asimismo elegir a víctimas menor de edad que su mayor fragilidad hace más eficaz la intimidación y merece una mayor protección.

En este sentido, es verdaderamente importante la reflexión que efectúa el Tribunal Supremo en esta sentencia sobre la implicación del ciberespacio y su afectación a la intimidad, y el impacto que sobre las mujeres y niñas puede tener la sextorsión como una de las formas más graves de ciberviolencia intimidatoria, no solamente por su cosificación sexual y la divulgación de imágenes de ella desnuda y su afectación a la intimidad, sino también por la alteración de sus relaciones sociales y de su propia autopercepción personal y social.

Finalmente, concluye que ha quedado afectada la libertad de autodeterminación personal de la menor al ser obligada bajo intimidación a realizarse tocamientos con contenido sexual, no exigiendo el tipo penal que sea el autor quien ejecute de manera física y directa la acción. Es decir, no se exige contacto directo con la víctima[56]. En definitiva, destaca que el escenario ofensivo en el que se produce, marcado por la distancia física entre victimario y víctima, no desnaturaliza la acción en términos de tipicidad ni compromete, en atención a criterios de proporcionalidad, su ubicación y sanción por el tipo de la agresión sexual. El escenario digital no altera los elementos esenciales de la conducta típica. Es más, la dimensión social de las TIC, al facilitar el intercambio de imágenes y vídeos de los actos de cosificación sexual, puede convertirse en un potentísimo instrumento de intimidación con un mayor impacto nocivo y duradero de lesión del bien jurídico. Así, no debe perderse de vista que las TIC han aumentado los modos de accesibilidad a los niños y niñas por parte de personas que buscan, como único objetivo, su abuso y explotación sexual[57].

56 STS núm. 447/2021. Recurso de casación/3097/2019.

57 Sentencia citada.

El Tribunal Supremo en este sentido concluye que "este nuevo ciberespacio de interacción social fragiliza los marcos de protección de la intimidad, convirtiendo en más vulnerables a las personas cuando, por accesos indebidos a sus datos personales, pierden de manera casi siempre irreversible, y frente a centenares o miles de personas, el control sobre su vida privada".

El legislador consciente de estos peligros, ha regulado recientemente en la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia[58], en su artículo 45, dentro del Capítulo VIII, "De las nuevas tecnologías", un uso seguro y responsable de Internet en el caso de los menores de edad. En este sentido el legislador ha establecido que: "*Las administraciones públicas desarrollarán campañas de educación, sensibilización y difusión dirigidas a los niños, niñas y adolescentes, familias, educadores y otros profesionales que trabajen habitualmente con personas menores de edad sobre el uso seguro y responsable de Internet y las tecnologías de la información y la comunicación, así como sobre los riesgos derivados de un uso inadecuado que puedan generar fenómenos de violencia sexual contra los niños, niñas y adolescentes como el ciberbullying, el grooming, la ciberviolencia de género o el sexting, así como el acceso y consumo de pornografía entre la población menor de edad.*

Asimismo, fomentarán medidas de acompañamiento a las familias, reforzando y apoyando el rol de los progenitores a través del desarrollo de competencias y habilidades que favorezcan el cumplimiento de sus obligaciones legales y, en particular, las establecidas en el artículo 84.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales".

Para ello, de acuerdo con el artículo 46 de la misma Ley, "*las administraciones públicas, en el ámbito de sus competencias, deberán realizar periódicamente diagnósticos, teniendo en cuenta criterios de edad y género, sobre el uso seguro de Internet entre los niños, niñas y adolescentes y las problemáticas de riesgo asociadas, así como de las nuevas tendencias*". Es importante, la colaboración de las administraciones públicas con el sector privado para conseguir precisamente que la utilización de Internet por parte de todos, tanto menores como adolescentes, familiares, y profesionales que trabajen con menores, sea segura y responsable.

Añadido a ello, el legislador también consciente de la especial relevancia que tiene en este ámbito la protección de los datos personales en el caso de

58 Publicado en el BOE núm. 134, de 05/06/2021.

menores de edad, ha previsto en el artículo 52 de la anterior Ley Orgánica que la Agencia Española de Protección de Datos personales ejerza sus funciones y potestades correspondientes para garantizar una protección específica de los datos personales de aquellas personas en los casos de violencia ejercida sobre la infancia y la adolescencia, especialmente cuando se realice a través de las tecnologías de la información y la comunicación. Hace hincapié en la especial gravedad que puede tener para los menores de edad el uso de las tecnologías de la información y comunicación como instrumento para ejercer la violencia. Para cumplir eficazmente con esta función de protección, la Ley ha previsto la disponibilidad de un canal accesible y seguro de denuncia de la existencia de contenidos ilícitos en Internet que puedan comportar un menoscabo grave del derecho a la protección de datos personales. Entre otras previsiones se establece que los menores de edad podrán denunciarlo por sí mismos sin la necesidad de que estén acompañas siempre que el funcionario público correspondiente estime que tiene la madurez suficiente para realizar la denuncia.

d.2. La prueba del desconocimiento de la edad del menor

Hay que señalar que en este delito el desconocimiento de la edad del menor (menor de 16 años) es un aspecto verdaderamente importante porque el desconocimiento de la edad del menor no es suficiente para la exculpación, sino que es necesario que dicho desconocimiento sea probado. Si bien es difícil en muchas ocasiones saber con certeza la edad de un menor, más difícil lo es todavía cunado la comunicación o el contacto se lleva a cabo a través de los medios tecnológicos y no físicamente. En este sentido, el conocimiento de la edad del sujeto pasivo plantea un problema práctico que, como señala GALLEGO SOLER, puede surgir con facilidad, puesto que las formas de contacto que hoy facilitan las nuevas tecnologías de la comunicación no siempre permiten la posibilidad de conocer que la edad del menor es inferior a dieciseis años (el autor hace referencia a 13 porque es anterior a la reforma de 2015)[59].

En este sentido, la jurisprudencia ha venido indicando que el conocimiento por parte del autor del delito de que el menor tiene una edad inferior a 16 años, no sólo lo puede adquirir el Juzgador por prueba directa de conocimiento del dato, sino, como en el caso objeto de enjuiciamiento, por la repre-

59 GALLEGO SOLER, *Comentarios al Código Penal. Reforma LO 5/2010*, Tirant lo Blanch, Valencia, 2010, pág. 440.

sentación del riesgo y la asunción del comportamiento, no obstante, el peligro relevante[60].

En efecto, en el caso concreto, no habiendo duda de que el contacto que persigue el autor es de índole sexual según el contexto de las conversaciones que se relatan en el *factum* de la sentencia, tampoco genera duda de que se trata de una menor de edad, sobre la que aquel asume no alcance la edad de disposición de la libertad sexual –entonces 13, ahora 16 años–, manteniendo esa situación de riesgo para el bien jurídico sin hacer nada para adecuar su conducta a la no realización del tipo penal, continuando y asumiendo su conducta sobre un menor sin capacidad de disposición, y aunque la misma dijera tener ya 13 años de edad, también es obvio que manifestaba su ansiedad por conseguir dinero de cualquier forma, representándose el autor no sólo su minoría de edad –conforme se interpreta de las conversaciones en sus 74 contactos telefónicos–, sino su actitud omisiva por comprobarla, no haciendo nada para obviar esa representación de una edad típica, asumiendo una situación arriesgada y no obstante, manteniendo su conducta, decidiendo –dolo– continuar, siendo consciente de la situación de riesgo, en su realización y continuando en la conducta desatendiendo la representación que así se hacía de la lesión al bien jurídico. Por tanto, los hechos descritos en la sentencia comentada demuestran que hubo representación de peligro y desprecio a la lesión que producía[61].

El Tribunal Supremo tiene asentado que "*es indudable que el dolo exigido al agente para la correcta aplicación del art. 187.1 y 2 CP o en su caso del art. 183 bis puede acomodarse al dolo eventual y, dentro de este concepto, al llamado dolo de indiferencia. Más allá de las limitaciones puestas de manifiesto por la dogmática para supuestos fronterizos, lo cierto es que cuando el autor desconoce en detalle uno de los elementos del tipo, puede tener razones para dudar y además tiene a su alcance la opción entre desvelar su existencia o prescindir de la acción. La pasividad en este aspecto seguida de la ejecución de la acción no puede ser valorada como un error de tipo, sino como dolo eventual. Con su actuación pone de relieve que le es indiferente la concurrencia del elemento respecto del que ha dudado, en función de la ejecución de una acción que desea llevar a cabo. Actúa entonces con dolo eventual (SSTS 123/2001, 5 de febrero y 159/2005, 11 de febrero). Y*

60 STS de 24 de febrero de 2015, ya citada anteriormente.

61 VELASCO, Eloy, y SANCHIS CRESPO, Carolina, *Delincuencia informática. Tipos delictivos…,* op. cit., pág. 160.

el dolo eventual deviene tan reprochable como el dolo directo, pues ambas modalidades carecen de trascendencia diferencial a la hora de calibrar distintas responsabilidades criminales pues, en definitiva, "todas las formas de dolo tienen en común la manifestación consciente y especialmente elevada de menosprecio del autor por los bienes jurídicos vulnerados por su acción" (SSTS 737/1999, de 14 de mayo; 1349/20001, de 10 de julio; 2076/2002, de 23 enero 2003)"[62].

Sigue manteniendo la jurisprudencia que "*la doctrina de esta Sala ha reiterado que debe probarse el error como cualquier causa de irresponsabilidad, por lo que no es suficiente con la mera alegación. El desconocimiento de la edad, como argumento cognoscitivo de defensa, ha de ser probado por quien alega tal exculpación e irresponsabilidad, sobre la base de que se trata de una circunstancia excepcional que ha de quedar acreditada como el hecho enjuiciado*"[63].

d. 3. Datos estadísticos

En relación con los datos estadísticos he analizado el *Informe sobre libertad e indemnidad sexual,* elaborado por el Ministerio de Interior, en el mismo se observa que en los hechos relacionados con ciberdelincuencia sexual, destacan los delitos de contacto mediante tecnología con fines sexuales con menores de 16 años, abuso sexual, corrupción de menores/persona con discapacidad y el acoso sexual[64]. En las conclusiones de dicho Informe se refleja un fenómeno preocupante asociado a la ciberdelincuencia sexual y es el relativo a que cuantitativamente las tres primeras tipologías están relacionadas con hechos cuyas víctimas son menores de edad, alcanzando aproximadamente el 75,8% del total de hechos conocidos. El perfil del ciberdelincuente sexual, es el de hombre, español, grupo de edad de 41 a 64 años y por delito relacionado con pornografía de menores[65].

Recientemente, se ha dado en España uno de los casos más graves de "grooming", el 17 de mayo de 2018, se detuvo al presunto autor de una red de contactos que había atrapado a 43 niñas, de entre 11 y 15 años de edad a

62 STS 97/2015, de 24 de febrero. En Tirant on line, DOCUMENTO TOL4.776.958.

63 Ibídem.

64 Véase el *Informe sobre libertad e indemnidad sexual en España de 2018*, interior.gob.es, pág. 38.

65 Ibídem, pág. 46.

través de las redes sociales. El presunto autor de 25 años de edad contactaba con las niñas a través de redes sociales con las que mas tarde mantenía conversaciones de mensajería instantánea proponiendo encuentros íntimos e intercambiando fotos y vídeos de contenido sexual. La identificación de estas menores llevó a su localización en distintas provincias españolas como Las Palmas, Santa Cruz de Tenerife, Barcelona, Valencia, Zaragoza, Jaén, Huelva, Salamanca, Murcia, La Coruña, Toledo, Valencia, Almería y Alicante[66].

Estos datos reflejan sin duda alguna, la necesidad de establecer mecanismos legales que protejan, eviten y, en último lugar, castiguen estas conductas delictivas, sobre todo teniendo en cuenta la especial protección que se debe ofrecer a las víctimas menores de edad, siendo éstas las que más sufren estos tipos delictivos.

66 Noticia publicada el 17/05/2018, en www.vozpopuli.com.

III

LA PRUEBA EN LA COMISIÓN DE LOS DELITOS CONTRA LA INTIMIDAD, LIBERTAD E INDEMNIDAD SEXUAL A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS

a. El principio de libertad de prueba

El derecho a utilizar los medios de prueba pertinentes es un derecho fundamental contemplado en el artículo 24.2 de la CE, en el cual se indica que: "*Asimismo, todos tienen derecho a (...) utilizar los medios de prueba pertinentes para su defensa...*". En este sentido, el legislador no establece una lista cerrada de medios de prueba a proponer y practicar en el proceso, sino que, por el contrario, existe una libertad a la hora de utilizar cualquier medio de prueba que sirva para acreditar los hechos objeto de debate. Si bien, este derecho a utilizar los medios de pruebas no es un derecho absoluto, sino que, tal y como tiene establecido la doctrina jurisprudencial "no atribuye un ilimitado derecho de las partes a que se admitan y practiquen todos los medios de prueba propuestos"[1], ya que no se trata de un derecho incondicional y absoluto, sino vinculado a la pertinencia y necesidad[2], es esencial que se ajuste a lo dispuesto por la ley.

---

1 STC 70/2002, de 3 de abril, ECLI:ES:TC:2002:70 o STS 2420/2017 - ECLI:ES:TS:2017:2420, entre otras.

2 El Tribunal Supremo manifiesta en la sentencia de 4 de marzo de 1996, en *Tirant on line*, DOCUMENTO TOL5.140.035, que: "*Como ya se ha reiterado en resoluciones de esta Sala, el derecho a la prueba no puede ser tan absoluto e ilimitado que obligue al tribunal ante el que la prueba se pide a realizar absolutamente todas las que las partes soliciten. Comoquiera que constitucionalmente se proscribe toda indefensión, el criterio para la realización o la denegación de prueba ha de guiarse por esa regla de tal modo que, si la prueba propuesta puede conducir a una defensa eficaz de las pretensiones de las partes, este derecho ha de prevalecer sobre cualquier otro.*

Pero si la actividad probatoria no puede conducir a esa finalidad la denegación de la práctica de prueba es pertinente. Es preciso, además, que la denegación de la práctica recaiga sobre pruebas de sustancial importancia para los intereses de la parte proponente, de tal modo que su denegación inmotivada le prive de elementos indispensables para el éxito de sus pretensiones (sentencias de 7 de Febrero de 1.992, 13 de Abril de 1.993 y 7 de Diciembre de 1.994). Además de formularse oportuna protesta ante la decisión de prescindirse por el tribunal de la prueba, es preciso, para que una queja sobre esa denegación prospere, que se argumente sobre la trascendencia que la inadmisión pudo

Junto a esa necesidad, es requisito imprescindible que estos medios de prueba, además de ser útiles y pertinentes, sean lícitos, es decir, que no vulneren los derechos fundamentales de la persona a la que afecta. De esta forma, no vulnerando los derechos fundamentales son perfectamente admisibles en el proceso penal. Por tanto, siendo el medio de prueba lícito es admisible. El principio de libertad de prueba es entendido como libertad de utilización y de apreciación, en este sentido, no existe limitación de los medios de prueba a utilizar en el proceso penal, y se consagra además el principio de libre valoración.

En relación con los nuevos medios de prueba, la jurisprudencia en este sentido ha avanzado considerablemente y es que desde la sentencia del Tribunal Supremo de 30 de noviembre de 1981 en la que se negaba eficacia probatoria a una grabación en cinta magnetofónica, la posterior línea jurisprudencial (a partir de las STSS de 5 y 17 de julio de 1984), ha venido sosteniendo la admisibilidad de los llamados "nuevos medios de prueba", basándose en la necesidad de interpretar las disposiciones legales de acuerdo a la realidad social actual, de acuerdo a lo previsto en el artículo 31 del Código Civil, siempre, como comentaba antes, que en la obtención de estos medios de prueba y en su incorporación al proceso se respeten las normas legales y los derechos fundamentales: respeto a la dignidad, a la intimidad, al honor de las personas, a la posibilidad de contradicción, etc.

La regulación legal vía artículo 230 de la Ley Orgánica del Poder Judicial permite la utilización en el proceso de cualesquiera medios técnicos de documentación y reproducción, siempre que cumplan con todas las garantías legales de autenticidad e integridad del contenido.

Por tanto, en el ámbito en el que estos delitos se comenten o desarrollan, que no es otro que el entorno digital, los medios de prueba que se van a aportar al proceso serán en la mayoría de los casos evidencias digitales, puesto que la comisión de los delitos que estamos estudiando, delitos contra la intimidad, libertad e indemnidad sexual a través de las nuevas tecnologías de la información y comunicación, se lleva a cabo a través de mecanismos o instrumentos tecnológicos, de manera que la prueba que acredite la comisión de dichos hechos delictivos será también digital o tecnológica.

Es evidente que, tratándose de entornos tecnológicos, los medios de prue-

---

tener sobre la sentencia luego dictada, porque, solo si se comprueba que el fallo pudo haber sido otro gracias a la práctica de la prueba omitida, cabe aceptar la existencia de indefensión para la parte proponente (sentencia de 18 de Noviembre de 1.992)".

ba estarán asociados a la tecnología de la información y de la comunicación. Probablemente esta prueba será la fundamental para acreditar los hechos delictivos, pero no hay que descartar otros medios de prueba clásicos como son las declaraciones de los testigos, copias en papel, etc.

b. Las dificultades de probar los delitos sexuales cometidos *on line*

Como indicaba anteriormente, los delincuentes encuentran en el ámbito de Internet y de las redes sociales muchas oportunidades para delinquir. En la práctica, dadas las características típicas de los ciberdelitos, los delincuentes se encuentran mas motivados a la hora de cometer esos hechos delictivos. Por un lado, desde el punto de vista de la accesibilidad y ubicuidad, es decir, la localización del ilícito es verdaderamente complejo en relación con otros tipos penales que no tienen a Internet como medio de comisión del delito o de lesión del bien jurídico. A mayor abundamiento, el *modus operandi* en estos delitos radica en el anonimato del delincuente que presume que pasará inadvertido. Además de estas características se encuentran también las siguientes: a) la cantidad de usuarios con acceso a internet; b) el anonimato del ciberdelincuente; c) la distribución o movilidad indiscriminada y rápida de los datos; d) la no necesidad de que confluyan los sujetos, o e) la localización global y la ausencia de autoridades que disuadan al ciberdelincuente[3].

Es más que evidente que la prueba fundamental de la comisión de estos delitos será la prueba digital puesto que estos se comenten a través de las nuevas tecnologías. Es precisamente esta cuestión la que mas problemática plantea puesto que existen muchas dificultades para los Cuerpos y Fuerzas de Seguridad del Estado a la hora de encontrar pruebas digitales de la comisión de los hechos ya que los delincuentes utilizan técnicas de cifrado y redes servidores y redes sofisticadas que les garantizan en la mayoría de los casos el anonimato[4]. En la práctica los medios de investigación tradicionales se muestran claramente insuficientes para investigar este tipo de delitos. Por ello, siendo la prueba digital la fundamental para poder descubrir a los autores de los hechos

3 Clough, J. (2010). *Principles of Cybercrime*. Cambridge: Cambridge University Press, citado por AGUILAR CÁRCELES, Marta María, "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido", op. cit., 121-135.

4 Véase a FERNÁNDEZ NIETO, Josefa, "Reforma del Código Penal hacia una nueva dimensión de la protección en los delitos de sexting y grooming", op. cit., pág. 9.

delictivos la misma será la mas difícil de localizar y por ello muchos de los delitos quedan impunes dadas las dificultades. Ya indicaba BENTHAM que "*el arte del proceso es, en realidad, el arte de la prueba*"[5]. Como señala BUENO DE MATA, "*la importancia de la fase probatoria en el proceso se infiere a través de múltiples referentes, lo cual nos revela hasta qué punto sin prueba no habría proceso, o hasta qué punto el proceso sólo se justifica porque existe algo que probar*"[6]. Precisamente, es en estos delitos donde adquieren mayor relevancia dichas afirmaciones dadas las dificultades de obtener pruebas de la comisión de esos delitos y es evidente que sin prueba no hay proceso. De hecho, el Ministerio de Interior publicó en el *Informe sobre delitos contra la libertad e indemnidad sexual en España en 2018*[7] que "*los delitos contra la libertad e indemnidad sexual, presentan una de las más altas tasas de esclarecimiento, situándose con el mayor porcentaje de hechos esclarecidos los delitos relativos a la prostitución. No obstante, cabe reseñar que en el escalón más bajo de esclarecimiento están los delitos de contacto con menor de 16 años para fines sexuales, amparándose en la tecnología*"[8]. Por tanto, son las dos caras de una misma moneda, por un lado, la tecnología facilita la comisión de hechos delictivos y, por otro lado, dificulta el descubrimiento de los autores puesto que este tipo de pruebas es mucho más manipulable.

Dada la naturaleza volátil de la prueba digital, es bastante difícil acreditar la autoría de la comisión de los delitos sexuales *on line*, primero porque es complicado identificar al usuario o usuarios y después porque son fácilmente manipulables o alterables. Como señala FLORES PRADA, "*la arquitectura de Internet favorece un alto nivel de opacidad en las conexiones y facilita el anonimato de los internautas, lo que hace difícil la identificación y el rastreo de los datos de navegación*"[9].

Por ello, hay que tender a posibilitar mecanismos que permitan almacenar y conservar posteriormente estos datos de forma segura con la finalidad de incorporarlos al proceso penal en los supuestos de comisión de hechos delictivos. Es importante, que se acredite el cumplimiento de la cadena de

5 BENTHAM, J., *Antología,* (Traducciones de HERNÁNDES ORTEGA, G. y VANCELLS, M.) Barcelona, 1991, pág. 35.

6 BUENO DE MATA, Federico, *Prueba electrónica y proceso 2.0, Especial referencia al proceso civil*, Tirant lo Blanch, 2014, en Tiran on line, Documento TOL4.147.241.

7 Citado anteriormente.

8 Véase interior.gob.es, pág. 6.

9 En *Criminalidad informática. Aspectos sustantivos y procesales*, op. cit., Documento TOL2.696.346.

custodia para evitar precisamente las posibles irregularidades y todo ello con el fin de garantizar la eficacia procesal.

Ya de por sí, como veremos a continuación, es bastante difícil identificar a un usuario de Internet, mas aún cuando es posible que una dirección IP (Internet Protocol) esté siendo utilizada por varios usuarios.

En concreto, en relación con el delito de "grooming" en la Directiva 2011/93/UE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011[10], ya se ponía de manifiesto en su Considerando 19 que: "*El embaucamiento de menores con fines sexuales constituye una amenaza con características específicas en el contexto de Internet, ya que este medio ofrece un anonimato sin precedentes a los usuarios puesto que pueden ocultar su identidad y sus circunstancias personales, tales como la edad. Al mismo tiempo, los Estados miembros reconocen la importancia de luchar también contra el embaucamiento de menores al margen del contexto de Internet, especialmente cuando no tiene lugar recurriendo a las tecnologías de la información y la comunicación. Se exhorta a los Estados miembros a que tipifiquen como delito la conducta en la que el embaucamiento del menor para que se reúna con el delincuente con fines sexuales se desarrolla en presencia o cerca del menor, por ejemplo, en forma de delito preparatorio especial, tentativa de las infracciones contempladas en la presente Directiva o como una forma especial de abuso sexual. Independientemente de la solución jurídica por la que se opte a la hora de tipificar como delito el embaucamiento de menores sin recurrir a Internet, los Estados miembros deben velar por que se procese de alguna manera a los autores de tales delitos*".

Por tanto, es patente la preocupación de las autoridades competentes de la Unión Europea por castigar estas conductas teniendo en cuenta la especial protección que se debe otorgar a los menores de edad y fundamentalmente cuando se da en el contexto de Internet por las dificultades que conlleva añadidas, como es la identificación del autor de dichas conductas delictivas.

---

10 Publicado en Diario Oficial de la Unión Europea el 7.12.2011, L 335/1. Además, en el Considerando 26 de la misma Directiva se sigue indicando que: "*Debe facilitarse la investigación y el enjuiciamiento penal de estas infracciones, habida cuenta de la dificultad de las víctimas para denunciar los abusos y del anonimato de los delincuentes en el ciberespacio. Para garantizar el enjuiciamiento e investigación adecuados de las infracciones contempladas en la presente Directiva, su inicio no debe depender, en principio, de la presentación de una deposición o denuncia por la víctima o su representante. La duración del período de prescripción de estas infracciones debe determinarse con arreglo al Derecho nacional aplicable*".

c. Las evidencias electrónicas

Como he apuntado anteriormente, es verdaderamente problemático averiguar la autoría de los delitos cometidos *on line,* a través de Internet, puesto que la dirección IP identifica a un ordenador o a un aparato, pero no a un usuario.

Señala ALONSO que en relación con el funcionamiento de cada ordenador que se conecta a Internet éste se identifica por medio de la dirección IP. La misma se compone de cuatro grupos de números comprendidos entre el 0 y el 255, ambos inclusive y separados por puntos. El Internauta no necesita conocer ninguna de estas direcciones IP para comunicarse puesto que estas las utilizan los ordenadores en la comunicación por medio del denominado protocolo TCP/IP con total transparencia para el usuario. El usuario de Internet tan solo debe conocer el *nombre de dominio* de su interlocutor, esto es, su dirección normal de Internet[11]. La información a través de la red no llega toda junta o a la vez, sino que lo hace de forma separada en paquetes, y una vez que llega al destino a través de diferentes dispositivos de interconexión se junta y estaría disponible[12].

La Agencia Española de Protección de Datos (AEPD) indicó que "*el TCP/IP se trata de un protocolo básico de transmisión de datos en Internet, donde cada ordenador se identifica con una dirección IP numérica única. En este sentido, las redes TCP/IP se basan en la transmisión de paquetes pequeños de información, cada uno de los cuales contiene una dirección IP del emisor y del destinatario*"[13]. Como señala FLORES PRADA, "es fácil advertir que el nuevo espacio digital permite múltiples aplicaciones en el almacenamiento, tratamiento, codificación y transmisión de la información"[14].

Por otro lado, se sigue indicando en el Informe de la AEPD que reproduzco literalmente por la complejidad de la materia que "*el sistema de nombre de dominio (DNS) es un mecanismo de asignación de nombres a ordenadores identificados con una dirección IP. Ciertas herramientas existentes en la red permiten encontrar el enlace entre el nombre de dominio y la empresa*

11 ALONSO, Adolfo, "La investigación policial de los delitos relacionados con nuevas tecnologías", *Estudios Jurídicos. Ministerio Fiscal*, número 2, 2003, págs. 47 y ss.

12 Ibídem, págs. 48 y 49.

13 Informe 327/2003, en https://www.aepd.es/informes/historicos/2003-0327.pdf.

14 FLORES PRADA, I., *Criminalidad informática. Aspectos sustantivos y procesales*, Tirant lo Blanch, 2012, en Tirant on line, Documento TOL2.696.345.

o el particular. A su vez, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, generalmente mantiene un fichero histórico con la dirección P (fija o móvil) asignada, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección[15]*. Además, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación*". Concluye el Informe citado que "*en estos casos, ello significa que, con la asistencia de terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil, en concreto, el nombre, dirección, número de teléfono, etc., por medios razonables*"[16].

En otros casos, como se indica en el Informe de la AEPD, "*un tercero puede llegar a averiguar la dirección IP dinámica o móvil de un usuario, pero no ser capaz de relacionarla con otros datos que le permitan identificarlo. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones estáticas. No obstante, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como cookies con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación*"[17].

En definitiva, la AEPD considera que no en todos los casos es posible iden-

---

15 A este fichero se le denomina fichero log, en este fichero de registro, queda anotado normalmente por cada acceso de usuario: a) fecha y hora; b) dirección IP asignada al usuario; c) dirección visitada URL; d) dirección IP correspondiente a la dirección visitada; d) otras informaciones de interés. En los casos de correo electrónico se anota: a) fecha y hora del mensaje; b) dirección IP y nombre del ordenador al que se envía el mensaje, así como la cuenta de correo del destinatario; c) dirección IP y nombre del ordenador que envía al usuario un mensaje de correo, así como la cuenta del remitente; d) número de identificación del mensaje. Véase a ALONSO, Adolfo," La investigación policial de los delitos …", op. cit., págs. 53 y 54.

16 Informe 327/2003, en https://www.aepd.es/informes/historicos/2003-0327.pdf.

17 Ibídem.

tificar a un usuario de Internet, aunque en muchos de los casos es posible, tanto sean redes fijas como móviles. Además, las direcciones IP se consideran datos de carácter personal y por tanto le son de aplicación la normativa sobre protección de datos[18].

Además, en relación con la telefonía móvil, como se ha indicado, estamos asistiendo a la denominada "tercera generación de la telefonía", que permite, a través del sistema UMTS (Sistema Universal de Telecomunicaciones Móviles), vehiculizar por banda ancha la información que hasta ahora sólo circulaba por internet; de ese modo, los teléfonos móviles van a constituir un nuevo objeto de investigación, cuya problemática deriva esencialmente de su movilidad, que es muy superior a la de los PC, así como del anonimato que generan las tarjetas prepago[19]. La posibilidad de obtener los números de las tarjetas de prepago solo es posible si es a través de autorización judicial.

Por otro lado, en relación a la ingerencia en los derechos fundamentales, la particularidad de estos aparatos es que pueden contener datos, información que afecte a diferentes derechos fundamentales, a este respecto la doctrina ha manifestado que: "*los teléfonos móviles tienen una característica particular, y es que son "inteligentes", lo que conocemos como Smartphone y ello significa que un mismo dispositivo puede realizar multitud de funciones que realizarían también otros instrumentos independientes, por ejemplo puede servir como cámara de fotos, agenda personal, GPS, email, teléfono, etc... lo que hace que puedan converger en el mismo la afectación de varios derechos: por una parte el derecho a la intimidad (privacidad) del art. 18.1 CE y por otra parte el derecho al secreto de las comunicaciones del art. 18.3 CE, lo que supone además que puedan converger también dos tipos de diligencias diferentes, la propia del registro de dispositivos de almacenamiento masivo y la diligencia de interceptación de comunicaciones telefónicas y telemáticas e incluso también se podría hablar de la diligencia de seguimiento y localización*"[20].

Por tanto, las diligencias de investigación que se pueden llevar a cabo sobre los dispositivos móviles pueden ser diferentes, así como también lo es la implicación de los derechos fundamentales que pueden verse afectados y es

18 Ibídem.

19 ORTUÑO NAVALÓN, María del Carmen, *La prueba electrónica ante los Tribunales*, Tirant on line, 2014, DOCUMENTO TOL4.125.957.

20 AIGE MUT, María Belén, "Las nuevas diligencias de investigación tecnológica", en *ibdigital.uib.cat*.

que las funciones que pueden cumplir esos dispositivos entendidos como "inteligentes" ha superado ya con creces la mera función de servir para llamar.

c.1 Concepto de prueba electrónica

En nuestro Ordenamiento no tenemos una definición legal de qué se entiende por prueba electrónica, también conocida como prueba tecnológica, digital, informática, ePrueba o cibernética o telemática[21]. De hecho, muchas veces se habla de prueba electrónica para hacer referencia única y exclusivamente al documento electrónico, sin embargo, a mi juicio, el documento electrónico es solo una modalidad de aquella. En relación con el documento electrónico sí tenemos una definición de lo que se entiende por documento electrónico, así como también de firma electrónica contenidas ambas definiciones en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica que más adelante analizaré.

Por tanto, considerando esta falta de concreción legal de lo que se entiende por prueba electrónica, voy a empezar de lo más a lo menos, para intentar dar una definición de prueba electrónica o tecnológica, separando, por un lado, el concepto de prueba y, por otro, la consideración de electrónica o tecnológica.

Muy brevemente, por prueba se entiende la actividad que llevan las partes para acreditar ante el juez los hechos alegados. CARNELUTTI afirmaba que "que el uso de la palabra prueba se limita a los procedimientos instituidos por el juez para la comprobación de los hechos controvertidos"[22].

Siguiendo con el concepto de prueba electrónica, el sentido de electrónico o tecnológico se refiere a la información contenida en instrumentos o aparatos electrónicos, por lo que se incluye en este término, tanto, teléfonos móviles, smartphones, tabletas, ordenadores, dispositivos USB, ZIP, Cd-Rom, DVD, reproductores de MP3 o MP4, servidores de información, etc[23].

En relación con el concepto de "correo electrónico" hay que acudir la definición ofrecida por la Directiva 58/2002[24], de 12 de julio, en la que se indica

21 Véase a ARRABAL PLATERO, Paloma, *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, 2019, en Tirant on line, DOCUMENTO TOL7.712.006.

22 CARNELUTTI, *La prueba civil*, Ediciones Depalma, Buenos Aires, 1982, página 43.

23 DELGADO MARTÍN, Joaquín, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer, 2018, pág. 39.

24 DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la

que «correo electrónico» es "*todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo*". Por tanto, se encuadraría dentro de esa definición tanto el *Short Message System* (SMS), que transmite mensajes por escrito electrónicamente y el *Multimedia Messaging System* (MMS), que transmite imágenes entre teléfonos móviles.

La información contenida en estos aparatos o instrumentos electrónicos es de difícil lectura para aquellos que no son especialistas en informática, es necesario que un dispositivo electrónico convierta la información que está cifrada en un texto en lenguaje natural alfabético que pueda leerse en la pantalla de este dispositivo[25].

La información digital o electrónica usa "*un lenguaje binario a través de un sistema que trasforma impulsos o estímulos eléctricos o fotosensibles y, por cuya descomposición y recomposición informática grabada en un formato electrónico, genera y almacena la información. Dicho lenguaje es un código ininteligible para aquéllos que no son informáticos. La visualización del texto en pantalla es una traducción en lenguaje alfabético común, descodificado*"[26]. Esta es una de las características que diferencian a la prueba electrónica del resto de pruebas[27].

Por tanto, para poder entender el contenido de la información digital o electrónica hay que transformar lo conservado que está en un sistema estructurado en dígitos binarios y una vez transformado lo que se exterioriza es un lenguaje con letras de nuestro alfabeto[28]. En este sentido, hay que diferenciar

---

intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). (DO L 201, 31.7.2002, p.37).

25 DELGADO MARTÍN, Joaquín, *Investigación tecnológica y prueba*..., op. cit., pág. 39.

26 GARCÍA TORRES, María Luisa, "La tramitación electrónica de los procedimientos judiciales, según la ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y comunicación en la administración de justicia. Especial referencia al proceso civil", en *Revista Internacional de Estudios de Derecho Procesal y Arbitraje*, www.riedpa.com, núm. 3, 2011, http://www.riedpa.com/COMU/documentos/RIEDPA31102.pdf, pág. 14.

27 Véase a DELGADO MARTÍN, Joaquín, "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma operada por LO 13/2015", en *Diario LA LEY*, nº 8693, de 2 de febrero de 2016, pág. 3.

28 En este sentido, GARCÍA TORRES, María Luisa, "La tramitación electrónica de

la información que está almacenada de la información que se exterioriza; la información almacenada se somete a procesos informáticos para que la información almacenada digital se transforme a un formato inteligible para el ser humano. Un ejemplo de lo expuesto es lo que ocurre con los correos electrónicos, cuando nosotros lo vemos escrito es porque el fichero informático codificado ha pasado un proceso de transformación para que pueda ser leído por el ser humano. Es esencial tener claro este concepto.

Finalmente, si aunamos los dos conceptos podemos definir a la prueba electrónica o prueba digital como "toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio"[29]. Como podemos observar esta definición es bastante amplia pues incluye dentro de dicho concepto todo tipo de información que sea creada, almacenada o transmitida por medios electrónicos y sirva para acreditar los hechos objeto de prueba en el proceso. Sin embargo, parece que cuando hablamos de prueba electrónica nos referimos siempre a documento electrónico y ello no es así, puesto que el documento electrónico, a mi parecer, es sólo una modalidad de prueba electrónica. Muchas veces se utiliza como medio de prueba para incorporar la información al proceso el documento electrónico, aunque el medio o el acceso al proceso se puede hacer por otros instrumentos, los cuales pueden ser los tradicionales como son el documento público o privado o como, por ejemplo, el informe pericial, la declaración testifical, la de las partes, etc, o varias a la vez. Pero además de estos medios de prueba clásicos, los avances tecnológicos han supuesto que el legislador regule los nuevos medios de prueba haciendo referencia a la prueba electrónica y diferenciándola del documento electrónico.

Estas pruebas tradicionales o clásicas al fusionarse con las nuevas tecnologías de la información se individualizan y crean la necesidad de un tratamiento singularizado[30]. Como señala la doctrina las especificidades que se

---

los procedimientos judiciales, según la ley 18/2011, de 5 de julio reguladora del uso de las tecnologías…", op. cit., págs. 14 y 15.

29 DELGADO MARTÍN, Joaquín, *Investigación tecnológica y prueba digital…,* op. cit., pág. 40.

30 Como señala ROUANET MASCARDÓ, Jaime, "Valor probatorio procesal del documento electrónico", en *Informática y Derecho*, dialnet.unirioja.es, pág. 164, "El desarrollo actual de la Tecnología ha provocado el surgimiento de diversos instrumentos que, por sus características, se apartan de los tradicionales; así desde los más simples hasta los más sofisticados: máquina de escribir, telégrafo, teléfono, fonógrafo, cinematógrafo, dictáfono, cinta magnetofónica, fotocopiadora, contestadores telefónicos automáticos,

plantean, demandan un análisis de las peculiaridades que ofrece la valoración de tales medios probatorios, cuestión para la que resulta esencial, a fin de no perdernos en una auténtica "selva informática", contar con una serie de criterios valorativos clave[31].

A mi parecer, el soporte electrónico no puede convertir la información en documento electrónico, no hay que confundir el continente con el contenido, teniendo en cuenta, fundamentalmente, las consecuencias que ello puede derivar en el proceso, en concreto, me refiero a la valoración que puede tener si estamos en el proceso civil. Considero que el error puede tener su origen en el propio artículo 3.5 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica que define al documento electrónico de la siguiente manera: "*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*". Esta definición, a mi parecer, convierte toda la información en documento electrónico si el soporte en el que está archivado es electrónico. Ello conlleva diferentes consecuencias en materia probatoria puesto que no tiene la misma fuerza probatoria un documento, sea este electrónico o no, que el resto de medios de prueba.

La Ley de Firma Electrónica no hace nada más que copiar la definición que ofrece el artículo 26 del Código Penal al indicar que documento es "*todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica*". Por tanto, a efectos penales todo soporte material, y por tanto, todo instrumento electrónico que incorpore datos, hechos, etc., será considerado documento a efectos probatorios[32]. Si bien, en el proceso penal, todos los medios de prueba tienen la

---

procesadores de textos, correo electrónico, videotex, telefax, télex, satélites de comunicación".

31 DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba*..., op. cit., pág. 48.

32 STS 524/1996 de 10 de julio de 1996, en la que el Tribunal Supremo indica que: "*El art. 26 del nuevo Código Penal aprobado por la LO 10/1995, de 23 de noviembre, aceptando el reto suscitado por doctrina y jurisprudencia, dispone que "a los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica". Concretamente en el ámbito doctrinal se consideró que si en cualquiera de las fases del procedimiento informativo se introdujera dolosamente un dato no verdadero, se alterase alguno de los ya incorporados, se suprimiera el existente, se simularan datos*

misma fuerza probatoria, todos ellos son de valoración libre, conforme a las reglas de la sana crítica.

En el proceso civil, la regulación es diferente, tanto en cuanto a la naturaleza jurídica de la información digital o tecnológica como a la propia valoración de la misma[33]. En este sentido, si consideramos que la naturaleza jurídica de la información contenida en soporte electrónico es de documento electrónico la valoración no es libre conforme a las reglas de la sana crítica sino de valoración tasada. Los documentos electrónicos a su vez pueden ser públicos o privados, tal y como se especifica en el apartado 6 del artículo 3 de la Ley de Firma Electrónica, y tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable (apartado 7, artículo 3 de la Ley de Firma Electrónica). En definitiva, los documentos públicos tienen valor probatorio sin necesidad de ser reconocidos por la parte que los presenta, y los documentos privados tienen valor probatorio si no son impugnados por la parte contraria. De esta forma, si no se impugna, cuestión que trataré más adelante, entraría en juego lo especificado en el artículo 326 de la Ley de Enjuiciamiento Civil. En este artículo se indica que: "*Los documentos privados harán* prueba plena *en el proceso, en los términos del artículo 319,* cuando su autenticidad no sea impugnada *por la parte a quien perjudique".*

Hay que tener en cuenta que, aunque cada orden jurisdiccional tiene sus propias reglas procesales, cuando no existen disposiciones legales específicas, la Ley de Enjuiciamiento Civil es de aplicación tanto para al ámbito penal, como contencioso-administrativo, laboral y militar. Por tanto, de acuerdo al artículo 4 de la LEC sería de aplicación a todos estos procesos.

Dejando al margen el documento electrónico, cuya fuerza probatoria está contemplada en la Ley de Firma Electrónica como acabo de exponer, a la prueba electrónica se le deberán aplicar o bien las normas referidas a los lla-

---

de manera que induzcan a error sobre su autenticidad, etc., habría de entenderse producido un delito de falsificación de documentos subsumible en el tipo penal que corresponda, conforme a la naturaleza pública o privada del documento". En https://vlex.es/vid/-53579432.

33 Aunque no voy a profundizar en ellos, quisiera apuntar, aunque sea a nota a pie de página, que existen dos estándares generales que diferencian la valoración de la prueba civil y penal. Así, como sostiene DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba…*, op. cit., pág. 28, "en el proceso civil se formula con la teoría de la "probabilidad prevalente" medida de modo racional. Mientras en el proceso penal, la clave sobre la decisión de fondo se asienta en la existencia de una "prueba más allá de toda duda razonable".

mados medios de prueba análogos, como son los regulados en los artículos 299.2 y 3, y 384.1 de la LEC, referidos a los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso; o bien, de acuerdo a los artículos 299.2, 382.1 y 382.2 de la LEC los que se refieren a los medios audiovisuales cuando éstos sean electrónicos, es decir, medios de prueba que permitan la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes[34], y, por tanto, la valoración será libre, conforme a las reglas de la sana crítica.

La doctrina maneja un concepto amplio de prueba electrónica que incluye tres variantes:

a) la creada directamente a través de la informática como es, por ejemplo, un correo electrónico;

b) la que procede de medios de reproducción o archivo electrónicos, como son los vídeos, fax, fotografía digital y, por último;

c) la que se presenta mediante instrumentos informáticos del tipo disquettes, pen-drives, bases de datos, etc[35].

En definitiva, tal y como lo define BUENO DE MATA, "cualquier prueba presentada informáticamente y que estaría compuesta por dos elementos: uno material que depende de un hardware, la parte física y visible de la prueba para cualquier usuario de a pie, por ejemplo, la carcasa de un Smartphone o una memoria USB; y por otro lado un elemento intangible que es representado por un software consistente en los metadatos y archivos electrónicos modulados a través de unas interfaces informáticas"[36]. Señalar que los metadatos comprenden una ingente cantidad de datos personales que se almacenan en los archivos de los proveedores de servicios de comunicaciones electrónicas y de redes públicas de comunicaciones[37].

---

34 OLIVA LEÓN, Ricardo, *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016, pág. 58.

35 Véase a DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba electrónica,* Tirant lo Blanch, 2009, en Tirant on line, Documento TOL1.436.940.

36 BUENO DE MATA, Federico, *Prueba Electrónica y proceso 2.0*., op. cit., pág. 130.

37 Véase a ENCINAR DEL POZO, M.A., "La invalidez de la Directiva sobre Conservación y Cesión de los datos relativos a las Comunicaciones", en Revista SEPIN/SP/DOCT/18682, 7 de noviembre de 2014; también QUEVEDO GÓNZALEZ, Marta María, *Investigación y prueba del ciberdelito*, op. cit., pág. 197.

En el ámbito europeo, la primera vez que se contempla el concepto de prueba electrónica es en la Decisión 2002/630/JAI, del Consejo de 22 de julio de 2002, de Cooperación Policial y Judicial en Materia Penal, configurando una definición de prueba electrónica que abarque toda su complejidad, de manera que por prueba electrónica se define a «*la información obtenida a partir de un dispositivo electrónico o medio digital el cual sirve para adquirir convencimiento de la certeza de un hecho*» y por medio de prueba «*los soportes técnicos que recaen la prueba electrónica*».

Al respecto, cabe mencionar la Decisión incluida en el Programa Marco AGIS156 de la Dirección General de Justicia de la Comisión Europea sobre cooperación judicial y policial en materia penal donde, también, se dió una definición de prueba electrónica como «*la información obtenida a partir de un dispositivo electrónico o medio digital el cual sirve para adquirir convencimiento de la certeza de un hecho*»[38].

Aunque la prueba digital o electrónica sirva para acreditar todo tipo de hechos o infracciones penales investigadas en el proceso penal, en este trabajo me voy a circunscribir a la prueba electrónica que sirve para acreditar los delitos de violencia sexual cometidos on line como son el "sexting", "grooming", "stalking", etc. En estos delitos precisamente la prueba fundamental será la prueba electrónica puesto que la comisión de los mismos requiere que sea a través de instrumentos electrónicos.

c.2 Fuentes y medios de prueba

Necesariamente cuando hablamos de prueba, y más si cabe cuando hablamos de prueba electrónica, debemos diferenciar entre fuente y medio de prueba que, aunque son conceptos que obedecen a una misma realidad, sin embargo, los planos en los que se mueven son totalmente distintos, es así que la fuente de prueba existe fuera del proceso, es previa e independiente al mismo obedece a una realidad anterior y extraña al proceso y, en cambio, el medio de prueba se circunscribe al proceso y, por tanto, tiene naturaleza procesal. Los medios de prueba solo existen en el proceso, no tienen naturaleza propia, más allá de las normas procesales que los preveen. Estos tienen por objeto aportar al juez el conocimiento que la fuente

38 Decisión 2002/630/JAI del Consejo, de 22 de julio de 2002, relativa a la cooperación policial y judicial en materia penal (AGIS), Diario Oficial L 203 de 1 de agosto de 2002.

de prueba proporciona, trasladando al proceso la información contenida en dichas fuentes[39].

Las fuentes de prueba pueden ser tanto objetos como personas que en cuanto pueden proporcionar conocimientos para apreciar o acreditar los hechos afirmados por una parte procesal, pueden tener trascendencia en el proceso y constituir material de referencia para la decisión a adoptar por el órgano judicial[40]. La obtención de la información contenida en la fuente de prueba es una actividad incardinada en la fase de investigación o averiguación de los hechos delictivos y es a través del medio de prueba como se incorpora la fuente y la información contenida en la misma.

Las técnicas de investigación criminal han avanzado considerablemente y en materia de recolección de fuentes de prueba permiten la obtención de información que hasta no hace mucho tiempo era impensable. Una característica común a muchos de estos adelantos científicos y técnicos es su objetividad y su contrastada fiabilidad en cuanto a los resultados que ofrecen, así como el alto grado de especialización y de conocimientos que debe tener la persona o personas que los practican[41]. No obstante, precisamente la cuestión más problemática es la fiabilidad de la prueba electrónica, puesto que la superioridad o perfección de la tecnología no sólo sirve para obtener resultados mas ajustados a la realidad sino también precisamente esas inmensas posibilidades pueden ser utilizadas para una más sofisticada manipulación de la realidad que pretenden demostrar[42].

De esta forma, en línea con la doctrina referida la fuente de prueba electrónica o digital consiste en la información contenida o transmitida por medios electrónicos y el medio de prueba será el instrumento que se utiliza para incorporar esa información al proceso. Así, fuentes de prueba serían las imágenes, las palabras y los sonidos que son la realidad pasada y recogida o almacenada en los medios de prueba que serían los soportes o instrumentos[43].

---

39 Véase a MORENO CATENA, Víctor, *Derecho procesal penal* (con CORTÉS DOMÍNGUEZ), Tirant lo Blanch, 2021, 1ª ed., pág. 444.

40 Véase MORENO CATENA, V., y CORTÉS DOMÍNGUEZ, *Manual de Derecho procesal penal*, 7 ª ed., Tirant on line.

41 Véase a GUZMÁN FLUJA, Vicente, *Anticipación y preconstitución de la prueba en el proceso penal*, Tirant on line, 2006, DOCUMENTO TOL865.119.

42 Ya lo apuntaba DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba*..., op. cit., pág. 51.

43 Véase PÉREZ PALACI, José Enrique, "La prueba electrónica: Consideraciones", 2014, pág. 3, en www.prolex.org

Esta actividad probatoria será utilizada por el Juez para obtener información de los hechos relevantes del proceso y poder determinar la culpabilidad o inculpabilidad de una persona.

Los instrumentos utilizados como medios de prueba se refieren a la declaración testifical, al informe pericial, a la prueba documental, al interrogatorio de las partes, al reconocimiento judicial y otros medios de prueba. Estos instrumentos transmiten al juez la percepción sensible del objeto de prueba, excepto en el reconocimiento judicial que al ser un medio de prueba directo el juez percibe el objeto de la prueba a través de su propia intuición. En el ámbito electrónico o digital dada la evolución de las nuevas tecnologías están apareciendo nuevos instrumentos informáticos que incorporan nuevas fuentes de prueba; entre ellos, podemos destacar entre otros, teléfonos móviles, smartphones, ordenadores, tabletas, dispositivos USB, Cd-Rom, DVD, etc[44].

La aparición de Internet supone una inmensa fuente de información, ya que se concibe como un conjunto de miles de redes de ordenadores conectados entre sí, por tanto, Internet no sería un medio de prueba sino una fuente de prueba que debe ser llevada al proceso a través de un medio de prueba.

En definitiva, todas estas heterogéneas fuentes de prueba que incorporan información relevante para acreditar los hechos debe ser incorporada al proceso a través de alguno de los medios de prueba existentes, en concreto, se incorporaran como prueba de instrumentos tecnológicos prevista en el artículo 299.2 de la Ley de Enjuiciamiento Civil, como prueba documental, como prueba pericial, como reconocimiento judicial y también es posible que se incorporen como prueba de interrogatorio de la parte o del testigo si ha tenido contacto con los instrumentos electrónicos. La doctrina señala que los medios de prueba modernos o actuales serían los contemplados en el artículo 299.2 de la LECivil, mientras que en el apartado 3 del artículo 299 de la misma Ley que alude a "*cualquier otro medio de prueba expresamente previsto*", si del mismo "*pudiera obtenerse certeza sobre hechos relevantes*", deja abierta la puerta a todos aquellos medios de prueba futuros, siendo una clausula abierta para poder incorporar todos los medios de prueba desconocidos actualmente. En este sentido, la actual regulación sobre medios de pruebas, en el orden civil, da cabida a los presentes y futuros, ya que el legislador ha regulado de forma amplia con la introducción de términos in-

44 Ibídem, pág. 42.

determinados, permitiendo que la norma se adapte a la evolución del desarrollo tecnológico por sí sola[45].

Por tanto, en relación con los soportes informáticos en el proceso penal a excepción de algún concreto precepto, en puridad no existe un régimen jurídico aplicable; en el proceso civil tales deficiencias se suplen con los preceptos de la LECivil, tanto el apartado 2 como el 3 del artículo 299 de la LECivil, que se aplican de forma supletoria tanto en el procedimiento penal, como en el resto de las jurisdicciones[46]. Por tanto, no es un *numerus clausus* los medios de prueba que pueden utilizarse en el proceso civil, y por tanto en el penal, sino que el legislador deja la puerta abierta a cualquier otro medio de prueba, siempre que sea legal, lícito, etc, que pueda obtenerse certeza sobre los hechos.

Por tanto, los pasos a seguir en el procedimiento probatorio serían primero acceder u obtener la información contenida en las fuentes de prueba para posteriormente incorporarla al proceso a través de algunos de los medios de prueba previstos legalmente. Tanto el acceso u obtención como la incorporación al proceso tiene que hacerse de forma lícita y legal, por tanto, sin vulnerar ningún derecho fundamental ni contravenir la ley. De otra forma, no tendrá valor probatorio lo obtenido de forma ilícita, de acuerdo al artículo 11.1 de la Ley Orgánica del Poder Judicial es nula de pleno derecho, por lo que no puede ser utilizada contra ninguna persona dentro del proceso.

Finalmente, el último paso es la valoración de la información obtenida e incorporada al proceso, será valorada por el órgano judicial pudiendo producir eficacia probatoria siempre y cuando ésta sea auténtica e íntegra.

En definitiva, la obtención de la información incorporada en las distintas fuentes de prueba tiene que hacerse de forma lícita, sin vulnerar ningún derecho fundamental, teniendo en cuenta quien accede a la fuente de prueba, si el particular o la autoridad pública encargada de la investigación penal, y teniendo en cuenta la modalidad de la comunicación, es decir, si la información está contenida en dispositivos electrónicos o es información transmitida por redes de comunicación, sea ésta abierta o cerrada.

---

45 Véase a FERNÁNDEZ MARTÍNEZ, Juan Carlos, "Especialidades de la prueba cuando, esta, es tecnológica", op. cit., pág. 335.

46 ORTUÑO NAVALÓN, María del Carmen, *La prueba electrónica ante los Tribunales*, Tirant lo Blanch, 2014, en Tirant on line, Documento TOL4.125.955.

c.3 Soporte "duradero"

Vamos a analizar todos los preceptos donde se hace referencia al "soporte". Así, como he comentado anteriormente tanto la Ley de Firma Electrónica como el Código Penal hablan de soporte para referirse a la prueba electrónica. Así, en el artículo 3 apartado 5 de la Ley de Firma Electrónica se indica que: "*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*", por tanto, se refiere al soporte electrónico. De igual manera en el art. 26 del Código Penal se menciona al soporte, aunque aquí se habla de soporte material para referirse al documento, en concreto, se indica que "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica" se considera documento.

En el apartado primero del artículo 743 de la LECrim cuyo epígrafe se refiere a "Medios de registro de la sesión. Documento electrónico", el legislador ofrece una definición de documento electrónico al indicar que: "*El desarrollo de las sesiones del juicio oral se registrará en soporte apto para la grabación y reproducción del sonido y de la imagen*".

Por otro lado, la Real Academia Española (RAE) define "soporte" como "*el material en cuya superficie se registra información como el papel, la cinta de video o el disco compacto*"[47]. Además, dado el avance de las tecnologías también podemos incluir un lápiz de memoria (Pendrive), una cinta magnética, un disco duro (Hard Disk Drive), entre otros. Estos soportes son el almacenamiento de datos, es decir "el antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho"[48].

Por tanto, para hacer referencia al documento, se utiliza el término "soporte", bien sea éste electrónico o material. Si bien, no se da una definición exacta de qué se entiende por soporte. Como ha señalado la doctrina "todo este abanico legislativo, la falta de unicidad y claridad ha conllevado a distintas clasificaciones de lo que se entiende por soportes electrónicos"[49]. Para lle-

47 Diccionario de la Real Academia Española.

48 ANGUIANO JIMÉNEZ, José María, "La prueba electrónica en la banca digital. El soporte duradero", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016, págs. 69 y ss.

49 PÉREZ PALACI, José Enrique, "La prueba electrónica: Consideraciones", op. cit., pág. 11.

gar a entenderlo mejor es preferible utilizar el término fichero, así, el fichero electrónico incorpora datos, cifras, etc.

Este fichero electrónico puede ser una fuente de prueba relevante para el proceso, la cual puede ser incorporada a través de un soporte, el cual será material[50]. Este soporte será el que se incorpore al proceso con eficacia probatoria. Ahora bien, permanece la discusión de si es considerado documento como medio de prueba, o se incluye dentro de los otros medios de prueba que recoge el artículo 299 de la Ley de Enjuiciamiento Civil. No obstante, se acoja una u otra consideración, en cualquier caso, el soporte que se incorpora al proceso es un soporte material que puede recoger un fichero electrónico. La Ley de Firma Electrónica equipara el fichero electrónico con el soporte electrónico. El fichero electrónico se puede incorporar a un dispositivo de almacenamiento (prendrive, disco duro, CD, etc) que será considerado un soporte material a incorporar al proceso.

En definitiva, el fichero electrónico es un soporte inmaterial que puede ser incorporado al proceso a través de un soporte material. Ahora bien, también ese fichero electrónico puede ser incorporado al proceso de forma telemática, el soporte sigue siendo inmaterial[51]. En el momento actual que estamos viviendo, donde la evolución de las tecnologías es algo imparable, donde el campo digital está sustituyendo a pasos avanzados al analógico y se está dejando de usar el papel, la aportación del papel está siendo sustituida por ficheros, y los papeles rubricados con firmas manuscritas se están sustituyendo por ficheros firmados electrónicamente. Es la nueva era digital donde estamos inmersos.

---

50 Los ficheros en soportes físicos tenemos tres categorías los dispositivos magnéticos, discos duros o HDD, los dispositivos ópticos, CD o DVD, y por último, la memoria sólida o SSD, es decir, tarjetas de memoria, dispositivos USB..., véase a FERNÁNDEZ MARTÍNEZ, Juan Carlos, "Especialidades de la prueba cuando, esta, es tecnológica", op. cit., pág. 336.

51 Señala ANGUIANO JIMÉNEZ, José María, "La prueba electrónica en la banca digital. El soporte duradero", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016, que: "Es claro que el fichero es inmaterial. Puede ser telemáticamente transportado. Interpretando literalmente el artículo, el fichero solo gozaría de la condición de documental cuando se incorporase a un dispositivo de almacenamiento, que es el soporte material. De optar por esta interpretación se podría llegar a excluir de la condición documental al fichero telemáticamente remitido al proceso. Sería un error, sobre todo teniendo en consideración la novedosa tendencia a la remisión telemática de determinadas aportaciones judiciales".

Sin embargo, como apunté anteriormente, a diferencia de lo recogido en papel, donde hay una identidad entre lo grabado y lo exteriorizado, lo almacenado en soporte electrónico no se exterioriza y si lo hace, realmente no hay identidad entre lo conservado y lo exteriorizado, ya que los signos de escritura no existen en la realidad natural sino en la virtual[52]. Si bien, en el ámbito de la Administración Pública, la Ley que regula el derecho de acceso electrónico de los ciudadanos a los servicios públicos, permite que el documento administrativo electrónico sea reproducible en documento electrónico, es decir, en el ámbito administrativo sí existe la posibilidad de aportar copias electrónicas de documentos electrónicos, aunque con algunos recelos[53].

Por otro lado, si acudimos al ámbito de los consumidores y usuarios, en relación con los contratos celebrados a distancia de ciertos bienes o servicios, tanto la normativa nacional como la comunitaria también utilizan el término de "soporte duradero" que parece coincidir con "los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas" a los que se refiere el artículo 299 de la Ley de Enjuiciamiento Civil.

En concreto, el término de "soporte duradero" nace con la específica finalidad de acreditar la obligación de información que se debe dar a los consumidores o usuarios cuando contratan bienes o servicios.

En la sociedad actual la tecnología biométrica permite que la declaración de la prestación del consentimiento, denominado como firma vocal, pueda quedar incorporada en el documento electrónico, de igual forma que una firma manuscrita se incorpora a un documento en papel.

Así, se consigue unir la tradición de la prestación verbal del consentimiento o el contrato "de palabra" con la posibilidad de que quede protegido en un soporte duradero, tal como preceptúa, por ejemplo, la normativa de protección de consumidores, que en el artículo 5 de la Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia y el artículo 98 de la Ley General para la Defensa de los Consumidores y Usuarios según redacción dada por la Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el

52 MIRA ROS, Corazón de María, "La prueba electrónica: algunas concesiones a la seguridad jurídico preventiva", véase en https://www.uv.es.

53 Ibídem.

Real Decreto Legislativo 1/2007, de 16 de noviembre, se establece de dicha manera[54].

La finalidad de la normativa se circunscribe a que quede acreditada la información que necesariamente debe recibir cualquier consumidor o usuario cuando contrata algún bien o servicio, utilizando el soporte electrónico como medio de prueba que acreditar tales extremos.

c.4 Los diferentes medios de prueba para incorporar la información digital o electrónica

Como anteriormente he señalado, los instrumentos que se utilizan para incorporar al proceso la información obtenida en las fuentes de prueba son los previstos legalmente, es decir, la prueba electrónica, por tanto, puede acceder al proceso a través de los medios de prueba clásicos que se recogen en el artículo 299 primer apartado de la LEC. Hemos mencionado la prueba documental, la pericial, la testifical, el reconocimiento judicial, el interrogatorio de las partes, entre otros, pero también puede acceder, como veremos posteriormente, a través de los otros medios de prueba contemplados en el segundo apartado del artículo 299 de la LEC.

En este sentido, la información obtenida en dispositivos electrónicos o digitales puede ser incorporada al proceso a través del documento en soporte papel, por lo que se incorporará al proceso a través de la prueba documental, pudiendo ser esta pública o privada, siendo de aplicación el régimen general previsto para la prueba documental[55]. Si ninguna de las partes impugna el

54 *Firma electrónica remota mediante la biometría con voz con validez jurídica*, en http://www.firmavocal.com/author/jinza/page/2/.

55 Señala PÉREZ PALACI, José Enrique, que la prueba electrónica accede al proceso como documento público, aportando acta notarial de la prueba electrónica bien: i. Protocolizando el medio de prueba impreso con anterioridad por el particular (artículo 145 del Reglamento Notarial); ii. Mediante el acta de presencia en la que le son exhibidos al notario documentos procediendo el mismo a describirlos en el acta "tal y como resulte de su percepción", (artículos 199 y 200.3 del Reglamento Notarial); iii. Mediante el testimonio de exhibición previsto en el artículo 251 del Reglamento Notarial; iv. Mediante el acta de exhibición (artículo 207 del Reglamento Notarial); v. Mediante el acta de presencia acreditando la realidad o verdad del hecho que motiva su autorización (artículo 199 el Reglamento Notarial); vi. Mediante acta de protocolización (artículo 211 del Reglamento Notarial); vii. Mediante acta de referencia (Artículo 208 del Reglamento Notarial). En "La prueba electrónica: Consideraciones", op. cit., pág. 7.

documento, éste adquiere fuerza probatoria, si es impugnado por las partes habrá que determinar la autenticidad del mismo a través de los mecanismos oportunos.

También el documento puede ser electrónico, por lo que el régimen previsto para estos casos no es el de la prueba documental sino, más concretamente, el de la prueba de instrumentos electrónicos previsto en el artículo 299 apartado segundo de la LEC y desarrollados en los artículos 383 y 384 de la misma Ley, y también en el artículo 3 de la Ley de Firma Electrónica[56].

En relación con la prueba documental en soporte papel puede ocurrir que la fuente y el medio de prueba concurran a la vez, sin embargo, cuando el documento es digital o electrónico la fuente y el medio de prueba están disociados[57]. La fuente o declaración de voluntad se plasma en un soporte magnético u óptico, el cual requiere que se materialice para aprehenderlo[58].

Además del documento como prueba, también hay que tener en cuenta los otros medios de prueba antes citados, en concreto, la prueba testifical, la pericial, el reconocimiento judicial y el interrogatorio de las partes.

No hay mucho que decir de la prueba testifical o la declaración de las partes, puesto que no hay ninguna especialidad en relación con los datos electrónicos o digitales. En este sentido, el testigo o las partes podrán ofrecer su testimonio en relación con la información que se contiene en dispositivos electrónicos (Whatssap, SMS, correo electrónico, etc) o redes de comunicación (Internet, páginas web, Facebook, Twiter, etc).

Por lo que respecta a la prueba pericial o reconocimiento judicial sí que conlleva alguna particularidad que seguidamente paso a comentar junto con la prueba documental electrónica.

---

56 Ley 59/2003, de 19 de diciembre, de firma electrónica. Publicada en el BOE, número 304, de 20/12/2003.

57 Véase a LEDESMA NARVÁEZ, Marianella, "La prueba documental electrónica", en *Revista Foro Jurídico*, número 15, 2016, págs. 17 a 25, quien indica que "*los documentos pueden ejercer doble función documental: la de fuentes y la de medios de prueba. Como fuentes, son documentos aquellos objetos en los que se ha dejado un registro material; como medios, son los elementos que se utiliza para requerir los conocimientos de la fuente. La fuente documental puede requerir un medio documental para traer el conocimiento al proceso, pero también puede requerir un medio de informes, un medio pericial, un medio declarativo o un conjunto de ellos, bajo presunciones*".

58 Ibídem.

a) La prueba documental electrónica

Como indiqué en otro apartado anterior, la definición de documento electrónico está prevista en el artículo 3, apartado 5, de la Ley de Firma Electrónica antes citada. En dicho artículo se indica que: "*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".*

El documento electrónico, al igual que el documento en soporte papel, puede tener la naturaleza de documento público o privado, para ello, en el apartado 6 del mismo artículo 3, se establece que "*el documento electrónico será soporte de:*

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados".

Ahora bien, en el apartado 8 del mismo artículo 3 de la Ley de Firma Electrónica se especifica que "*el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio*". Este apartado lo que hace es diferenciar la naturaleza del soporte considerándole documento o no atendiendo al requisito de la firma electrónica. Por tanto, ese soporte será considerado documento electrónico si el mismo está firmado electrónicamente. A sensu contrario, a mi parecer, si ese soporte incluye información no firmada electrónicamente no se le puede considerar documento electrónico por lo que necesariamente debe tener otra consideración que no es otra que la de otro instrumento de prueba vía artículo 299 de la LEC, ya que, de otra forma, no tendría sentido la especificación que realiza el legislador en el apartado 8 del artículo 3 de la Ley de Firma, al tratar el soporte firmado electrónicamente[59].

En definitiva, aunque en el apartado 3 del artículo 5 de la Ley de Firma

59 Véase a ANGUIANO JIMÉNEZ, José María, "La prueba electrónica en la banca digital. El soporte duradero", en *La prueba electrónica. Validez y eficacia procesal*, op. cit., págs. 69 y ss.

Electrónica se defina como documento electrónico a cualquier información archivada en soporte electrónico, sólo se va a considerar documento electrónico a aquel que lleve la firma electrónica. De lo contrario, cualquier soporte electrónico que contenga información que no lleve aparejada la firma electrónica no tendrá la consideración de documento electrónico, su naturaleza, por tanto, será la de los instrumentos previstos en el apartado segundo del artículo 299 de la LEC. Esta aportación se valorará conforme a las reglas de la sana crítica, y sólo tendrá una valoración tasada el soporte electrónico que lleve la firma electrónica. En el proceso penal, independientemente de la naturaleza del instrumento la valoración es siempre libre conforme a las reglas de la sana crítica, de la experiencia, etc.

b) La prueba pericial como medio de incorporar información contenida en instrumentos electrónicos o digitales

La prueba electrónica por su complejidad técnica puede necesitar de una pericial informática, así, en el artículo 352 de la LEC se indica que la prueba pericial puede servir "*para conocer el contenido o sentido de una prueba o para proceder a su más acertada valoración…*". En este sentido, la pericial informática puede tener lugar en tres circunstancias diferentes:

a) puede darse cuando se impugna la autenticidad o integridad de un documento privado aportado por la parte;

b) como auxiliar de la prueba;

c) o, también puede darse como dictamen autónomo[60].

En relación con este último, el dictamen autónomo pretende conseguir convertir las evidencias digitales o registros electrónicos en instrumentos de valor legal en el proceso, es decir, convertir las evidencias en verdaderas pruebas. En este sentido la informática y la telemática tiene como base el estudio de todo tipo de evidencias digitales. Ahora bien, como se ha puesto de manifiesto las periciales informáticas todavía hoy tienen un alcance limitado. Hay veces que no se puede llegar a conocer todos los datos producidos por los mecanismos tecnológicos y otras veces, aunque se conozcan tampoco se puede determinar con exactitud si han sido o no manipulados[61].

---

60 Véase a PÉREZ PALACI, José Enrique, "La prueba electrónica: Consideraciones", op. cit., pág. 7.

61 ARRABAL PLATERO, Paloma, *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, 2019, en Tirant on line, DOCUMENTO TOL7.712.006.

En relación con el contenido del dictamen pericial informático debe hacer referencia a los siguientes aspectos:

1. Identificación del origen y existencia de los datos.

La acreditación de estos concretos datos puede llevarse a cabo a través de cualquier medio que esté a su disposición tanto fotografías, como grabación de vídeos, colaboración de testigos, así como también el concurso de un fedatario público o tercero de confianza que puedan dar fe sobre el particular.

2. Obtención de los datos de forma lícita.

Es fundamental la obtención de los datos sin vulnerar ningún derecho fundamental y de acuerdo con la normativa de aplicación sobre el particular.

3. La no manipulación de los datos, ni pérdida de información relevante, a la hora de acceder a la información por parte del perito informático ya sea por la propia naturaleza o por descuido negligente de éste.

4. El acceso a datos que obran en poder de la otra parte en el litigio, en el caso de que se diese esta circunstancia.

Toda esta información es necesaria para que posteriormente se pueda valorar lo recogido en el informe[62].

c) La prueba del reconocimiento judicial de la información contenida en instrumentos electrónicos o digitales

En relación con este medio de prueba, el propio órgano judicial puede proceder de modo directo al reconocimiento del objeto de la prueba tanto en la sede del tribunal como en el lugar donde se halle el soporte electrónico en el que se encuentra la prueba electrónica de acuerdo al artículo 353 de la LEC. Es una prueba directa porque es el propio juez quien a través de la intuición percibe el objeto de prueba, pero dadas las características técnicas tan complejas necesitará del profesional que le pueda auxiliar en la apreciación. Además, el órgano judicial puede ser asistido por un perito o práctico en la materia, además de que se adopten las medidas necesarias para la lograr la efectividad del reconocimiento judicial, de acuerdo al artículo 354.1 de la LEC, entre las cuales se puede fijar la entrada en el lugar donde se encuentre el medio de prueba garantizando los derechos fundamentales de las personas, como el derecho a la intimidad, a la inviolabilidad del domicilio, etc.

62 Véase FLORENCIO MOLINA, Miguel*, La prueba digital,* Manuales de Derecho Aplicado, junio de 2017, pág. 20, en https://www.miguelflorencio.com/books/Derecho/pruebadigital.pdf.

d. La admisión de la prueba electrónica

Una de las especialidades de la prueba estriba precisamente en el trámite de su admisión puesto que para ser admitida es preciso que esa prueba no comporte ningún atisbo de manipulación ni de alteración. Como señalaba DE URBANO CASTRILLO[63], la necesidad de que la prueba electrónica pase el test de admisibilidad es especialmente significativo en esta clase de pruebas. Dado el componente técnico jurídico el funcionamiento de dichas pruebas es bastante complejo por lo que en la mayoría de los casos será necesario un perito informático que indique las condiciones relativas a la apreciación de la prueba en lo que respecta fundamentalmente a la fiabilidad de la misma. De hecho, hay quienes califican a esta prueba de "sospechosa" por ser fácilmente alterable, ya que habitualmente no se adopta ninguna prevención en su creación y conservación, y siempre, como veremos a continuación, puede haber sido manipulada por su creador tanto en su contenido (retoques) como en la información adjunta al fichero (cambio en los metadatos)[64]. Por ello, en el marco de una investigación penal, las características de la evidencia digital (inmaterial o intangible, replicable, dispersa, volátil y fácilmente manipulable, entre otras) hacen que puedan plantear problemas tanto en la propia adquisición como en cuanto a su incorporación y valoración[65].

Cuando se habla de "evidencia digital", en concreto, se esta haciendo referencia a una expresión que se utiliza de manera amplia para describir cualquier documento, fichero, registro, dato, etc. almacenado en un soporte informático, susceptible de tratamiento digital, y que pueda ser utilizado como evidencia en un proceso legal como, por ejemplo:

– Documentos de ofimática (Word, Excell, etc.)
– Comunicaciones digitales (e-mails, SMS, fax)
– Imágenes digitales (fotos, videos, etc.)
– Bases de datos
– Ficheros de actividad (LOGS -que es un registro de actividad de un sis-

63 *La valoración de la prueba electrónica*, op. cit.

64 PERALES CAÑETE, Rafael, "Exiftool: Los metadatos sirven de algo", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016, pág. 115.

65 MARTÍN RÍOS, Pilar, "El "primer acceso policial" a dispositivos de almacenamiento digital o de cuando las garantías se supeditan a la búsqueda de la eficiencia", en *Justicia: ¿Garantías versus eficiencia?,* Tirant lo Blanch, 2019, págs. 839 y 840.

tema, que generalmente se guarda en un fichero de texto, y que sirve, por ejemplo, para guardar incidencias, errores, accesos a usuarios, etc.)[66].

En este sentido, hay ciertas garantías específicas que ha de cumplir, como son: la integridad (el soporte que se presenta no ha sido manipulado), la autenticidad (confirmación de la realidad del sujeto al que se atribuye y del contenido que refleja) y la licitud (obtención salvaguardando los derechos y libertades fundamentales). Por tanto, el juez no debe tener ninguna duda sobre dos aspectos fundamentales, una vez que la prueba ha sido obtenida lícitamente como es el de la autenticidad del origen y la integridad del contenido.

En relación con la autenticidad del origen, no debe haber confusión entre el autor aparente y el autor real y, en relación con la integridad del contenido, se requiere que los datos no hayan sido alterados, que no haya habido ningún tipo de manipulación ni modificación pues de lo contrario el juez no podrá entrar a valorar la prueba dada la ineficacia probatoria de la misma.

En el momento que vivimos actualmente, conocido como era digital, es necesario que también el juez se adapte a las nuevas tecnologías, pero sin perder de vista el respeto a los derechos fundamentales de las personas, por tanto, no puede cerrar los ojos a la dimensión que la implantación y evolución de las nuevas tecnologías están teniendo en muchos ámbitos de la sociedad incluido en el ámbito del proceso, pero debe hacerlo teniendo en cuenta el respeto a los derechos fundamentales. Es más que primordial en este tipo de pruebas ser escrupuloso con el plazo fijado para la proposición y aportación de la prueba electrónica ya que teniendo en cuenta la facilidad a la hora de manipular la misma, este tiempo debería ser el más breve posible para garantizar que no se rompa la cadena de custodia, y con ello asegurar la autenticidad, inalterabilidad e indemnidad de la prueba electrónica[67].

d.1 La cadena de custodia

La recopilación de las evidencias digitales para poder incorporarlas al juicio oral es una tarea complicada por la complejidad técnica que conlleva este tipo de pruebas. La mayoría de las veces la validez legal y licitud de la prueba

66 SANZ-GADEA GÓMEZ, Juan Bautista, *Los informes periciales informáticos en el ámbito de las nuevas tecnologías y prueba ilícita (RJC 39/2015), 2015,* Tirant on line, DOCUMENTO TOL5.638.931.

67 Véase a OLIVA LEÓN, Ricardo, "La prueba electrónica envenenada", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016, pág. 58.

va a depender del tratamiento realizado en la recopilación y preservación de las mismas. Por ello, es muy importante el papel que puede llevar a cabo el perito informático a la hora de garantizar la consistencia de las evidencias obtenidas que solo lo puede hacer mediante un proceso técnico que garantice la no alteración de las pruebas, su custodia y su posterior documentación. En este sentido, la finalidad de la cadena de custodia es precisamente garantizar el mantenimiento de las evidencias de igual forma que fueron conseguidas, con independencia de cualquier tipo de investigación, sea o no informática. Con este procedimiento se permite dejar constancia de la identidad, autenticidad e integridad de una prueba digital indiciaria o demostrativa de un hecho con relevancia procesal, desde que es localizada e intervenida hasta que es aportada al proceso penal consiguiendo con ello valor probatorio.

Así, la "cadena de custodia" hace referencia a ese proceso mediante el cual la misma evidencia de la pericia o fuente de convicción es transmitida sin modificación sustancial desde que se obtiene hasta que se analiza, de manera que exista una identidad durante todo el proceso, y para su validez, es suficiente que se pueda dar cuenta de la misma por quienes la han realizado[68]. Como ha señalado la jurisprudencia "*en nuestro sistema jurídico procesal la cadena de custodia es el procedimiento documentado a través del cual se garantiza que lo examinado por el perito es lo mismo que se recogió en la escena del delito y que, dadas las precauciones que se han tomado (sea por la policía judicial, sea por los peritos, sea por el Juez) no es posible el error o la "contaminación" y así es posible el juicio científico del perito que, tras su ratificación en Juicio, adquirirá el valor de prueba. Así resulta de los* arts. *326, 292, 770.3 y 338 de la Ley de Enjuiciamiento Criminal*"[69].

En nuestro ordenamiento jurídico no se encuentra regulado expresamente el procedimiento de custodia, aunque sí es cierto que la LECrim hace referencia a ella en varias normas, en concreto, en el artículo 282, se establece que la Policía Judicial, procederá a recoger todos los efectos, instrumentos o pruebas del delito, poniéndolos a disposición de la correspondiente Autoridad Judicial. Esta diligencia se lleva a cabo a través de la inspección ocular, y la misma se regula en el art. 334 de la LECrim. Aunque hay alguna referencia más en la ley, el último artículo que hace especial mención es el art. 796.6º, en

68 SANZ-GADEA GÓMEZ, Juan Bautista, *Los informes periciales informáticos en el ámbito de las nuevas tecnologías y prueba ilícita (RJC 39/2015)*, en Tirant on line, 2015, DOCUMENTO TOL5.638.931.

69 STS de 31 de octubre de 2017, DOCUMENTO TOL6.467.549.

el que se indica que las evidencias recogidas serán enviadas a los laboratorios pertinentes.

Más concretamente, el Tribunal Supremo ha sintetizado la doctrina jurisprudencial en relación con la cadena de custodia. Reproducimos aquí dicha doctrina que indica: "*En nuestra STS 340/2016, de 6 de abril, citando a la sentencia de esta Sala 675/2015, de 10 de noviembre, que sintetiza la doctrina jurisprudencial en relación a la cadena de custodia, cuyo quebrantamiento también denuncia el motivo que nos ocupa, y en palabras igualmente de la STS 1/2014, de 21 de enero, la cadena de custodia no es un fin en sí mismo, sino que tiene un valor instrumental. Lo único que garantiza es la indemnidad de las evidencias desde que son recogidas hasta que son analizadas, lo que en caso de quiebra puede afectar a la credibilidad del análisis pero no a su validez (SSTS 129/2011 de 10 de marzo; 1190/2009, de 3 de diciembre o 607/2012, de 9 de julio).*

Recordaba la STS 725/2014, de 3 de noviembre, que la cadena de custodia constituye una garantía de que las evidencias que se analizan y cuyos resultados se contienen en el dictamen pericial son las mismas que se recogieron durante la investigación criminal, de modo que no existan dudas sobre el objeto de dicha prueba.

De acuerdo con la STS 587/2014, de 18 de julio, la cadena de custodia no es prueba en sí misma, sino que sirve de garantía formal de la autenticidad e indemnidad de la prueba pericial. Su infracción afecta a lo que JURISPRUDENCIA se denomina verosimilitud de la prueba pericial y, en consecuencia, a su legitimidad y validez para servir de prueba de cargo en el proceso. En palabras de la STS 195/2014, de 3 de marzo, no es una cuestión de nulidad o inutilizabilidad, sino de fiabilidad (en el mismo sentido STS 320/2015 de 27 de mayo o STS 388/2015 de 18 de junio).

Para examinar adecuadamente si se ha producido una ruptura relevante de la cadena de custodia no es suficiente con el planteamiento de dudas de carácter genérico, es necesario que el recurrente precise en qué momentos, a causa de qué actuaciones y en qué medida se ha producido tal interrupción, pudiendo, en su caso, la defensa, proponer en la instancia las pruebas encaminadas a su acreditación.

Que pueda existir alguna irregularidad en los protocolos establecidos como garantía para la cadena de custodia no equivale a nulidad. Habrá que valorar si esa irregularidad existe y es idónea para despertar dudas sobre la autenticidad o indemnidad de la fuente de prueba".

En definitiva, el Tribunal Supremo en dicha sentencia resume el significado que tiene la cadena de custodia en el proceso y así, establece que:

"*a) No es un fin en sí mismo, sino que tiene un valor instrumental.*

b) Garantiza la indemnidad de las evidencias desde que son recogidas hasta que son analizadas.

c) No afecta a la nulidad de la prueba sino a su fiabilidad.

d) La irregularidad tiene que ser causal o material respecto a la pérdida de valor de lo incautado con fines analíticos, no meramente formal.

e) No basta con afirmar dudas, hay que probar los vicios de la ruptura de la cadena de custodia, pues las actuaciones procesales, incluido el comportamiento de la policía judicial, se presume lícito mientras no se pruebe lo contrario"[70].

Dada la volatilidad de las pruebas electrónicas, la exigencia de respetar la cadena de custodia es si cabe mayor que en el resto de modalidades de prueba para prevenir y evitar precisamente la alteración y manipulación de los datos electrónicos almacenados, fundamentalmente teniendo en cuenta que se ponen en juego derechos fundamentales recogidos en el artículo 18 de la Constitución. Para ello es fundamental asegurar la prueba lo que se puede hacer en sede judicial, mediante la correspondiente solicitud al Juez o previamente al proceso a través de la fe pública del Notario protocolizando la información, o también puede llevarse a cabo mediante un informe pericial que acredite que no se ha realizado ninguna manipulación de la prueba. Es lo que denomina la jurisprudencia como "mismisidad de la prueba" y ello significa que se ha de tener la certeza de que lo que se traslada, se mide, se pesa y se analiza es lo mismo que se recoge para el estudio del lugar del delito[71].

Esta "mismisidad", o mejor dicho no "mismisidad" de la prueba se suele alegar en la práctica por parte de los abogados como defensa para sostener que se ha roto la cadena de custodia[72]. La jurisprudencia en relación con ello

---

70 STS 5 de abril de 2017, sentencia núm. 250/2017, en Tirant on line, DOCUMENTO TOL6.057.598.

71 STS 1190/2009, de 3 de diciembre (Tol 1762123). Más recientemente véase la STS de 31 de octubre de 2017, DOCUMENTO TOL6.467.549.

72 El Tribunal Supremo en sentencia de 20 de diciembre de 2019, DOCUMENTO TOL7.687.769, ECLI: ES:TS:2019:4281ha indicado que: "*Esta Sala señala que a través de las declaraciones testificales de los Policías o de los expertos forenses, que aseguraron y examinaron las fuentes de prueba, se pueden aclarar en el juicio las cuestiones controvertidas que las partes, al formular las preguntas, tengan sobre la conservación o ruptura de la cadena de custodia - STS 195/2014, de 3 de marzo. Son pues sus declaraciones*

mantiene que quien alega que se ha roto la cadena de custodia debe probarlo[73]. Así, indica el Tribunal Supremo en la sentencia 541/2018, que: «*Para examinar adecuadamente si se ha producido una ruptura relevante de la cadena de custodia no es suficiente con el planteamiento de dudas de carácter genérico, es necesario que la parte que la cuestione precise en qué momentos, a causa de qué actuaciones y en qué medida se ha producido tal interrupción, pudiendo proponer en la instancia las pruebas encaminadas a su acreditación.*

En cualquier caso habrá de plantearse en momento procesalmente hábil para que las acusaciones, si a su derecho interesa, puedan contradecir eficazmente las objeciones planteadas"[74].

---

y la valoración judicial que se hace de ellas, las que permiten al Tribunal mantener la fiabilidad, autenticidad e integridad que se predica de las muestras y el material intervenido relacionado con el acto delictivo.

Y, además, se añade que la cadena de custodia y su ruptura está conectada con las consecuencias jurídicas que se prevén cuando se formula su fractura o se predica de ella su inutilidad.

En este tema hay que distinguir que una cosa son las meras irregularidades, o defectos formales presentes en el iter que dibuja la cadena de custodia por los diversos lugares por donde transita la muestra o evidencia, tales como:

1.- Defectuosa o errónea numeración de las cajas que contienen la fuente de prueba;

2.- No consta el número de diligencias;

3.- No consta el acta de remisión de los elementos empíricos desde que se recogieron hasta su entrega en la sede policial;

4.- Falta de precinto;

5.- Embalaje inadecuado que no afecta a la muestra y a la información que cabe extraer de ella; o

6.- Mero retraso en la remisión al laboratorio de la sustancia intervenida para su análisis.

Se añade por esta Sala que estos casos y otros similares, no siembran dudas sobre la identidad de las sustancias u objetos ocupados, ya que se corresponde con lo intervenido policialmente. Estamos ante disfunciones de tipo más bien burocrático, que, en principio, salvo que vayan acompañadas de otra serie o conjunto de irregularidades que hagan peligrar la seguridad de la cadena de custodia, no tienen porqué cuestionar la autenticidad y mismisidad de los vestigios y evidencias que fundamentan la prueba de cargo, y que son objeto de valoración judicial. Irregularidad en los protocolos establecidos como garantía para la cadena de custodia no equivale a nulidad -STS 339/2013, de 20 de marzo-".

73 STS, de fecha 4 de abril de 2006 (Tol 948907).

74 STS 541/2018, 8 de Noviembre de 2018, ECLI: ES:TS:2018:3787, en https://vlex.

Con carácter general la carga de la prueba la tiene quien aporta la prueba no quien la impugna. En este sentido, difiriere de quien tiene la carga de la prueba cuando se impugna la aportación de un WhatsApp puesto que en este caso quien tiene que probar la autenticidad de la prueba es la parte que lo aporta y no quien lo impugna[75]. El Tribunal Supremo ha indicado que: "*El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido*"[76].

Además, otra cuestión relevante en el ámbito de la cadena de custodia es que cuando se produce la ruptura de la cadena de custodia no se convierte en prueba prohibida declarándose la nulidad de la misma, sino que, al no poderse acreditar la autenticidad de la prueba, la misma no puede llegarse a valorarse. La cadena de custodia permite asegurar que lo recogido, analizado y llevado al juicio oral es lo mismo, por ello, si esto se cuestiona se convertiría en un problema de autenticidad no de prueba prohibida. La regulación legal actualmente no recoge tal extremo por lo que la jurisprudencia viene acogien-

---

es/vid/746472021, citada por la Sentencia de la Audiencia Provincial de Madrid, de 23 de noviembre de 2018, Número Sentencia: 673/2018 Número Recurso: 1228/2018, en Tirant on line, DOCUMENTO TOL7.090.319.

75 En la sentencia de esta Sala del Tribunal Supremo, Sala Segunda, de lo Penal, Sentencia 300/2015 de 19 de mayo de 2015, Rec. 2387/2014, ya citada, se pone de manifiesto que "*respecto a los archivos de impresión con conversaciones en sistemas de mensajería instantánea y la carga de la prueba:*

La prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas por la posibilidad de manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido".

76 STS 754/2015, 27 de Noviembre de 2015, en https://vlex.es/vid/591346098.

do el criterio de no confundir los dos planos, el de la irregularidad con el de la ilicitud, estableciendo que la irregularidad en los protocolos establecidos como garantía para la cadena de custodia no equivale a nulidad. Así, el Tribunal Supremo ha establecido que no es una cuestión de prueba prohibida, en la Sentencia 339/2013, de 20 de marzo, señala lo siguiente:

"Como explicaban las SSTS 506/2012, de 11 de junio y 767/2012, de 11 de diciembre es cierto que la regularidad de la cadena de custodia es un presupuesto para la valoración de la pieza o elemento de convicción ocupado. Se asegura de esa forma que lo que se analiza es justamente lo ocupado y que no ha sufrido contaminación alguna. El decaído proyecto de Ley de Enjuiciamiento Criminal de 2011 contenía una sintética regulación de esa materia (arts. 357 a 360), hoy ausente, al menos en esa visión integrada, en nuestra Legislación procesal, sin perjuicio de algunas inequívocas referencias (vid. art. 334, entre otros). Con el valor puramente doctrinal que cabe atribuir a ese texto, se establecía por vía de principio la obligación de cuantos se relacionan con las fuentes de prueba de garantizar su inalterabilidad, o dejar constancia de las eventuales modificaciones que hayan podido producirse como consecuencia de su depósito, recogida, inspección, análisis o depósito. Disposiciones de rango reglamentario estarían llamadas a regular un procedimiento de gestión de muestras, cuyos hitos básicos, que habían de documentarse, se reflejaban legalmente: dejar constancia de las circunstancias del hallazgo, personas y lugares que hayan tenido a su cargo la muestra, tiempo y motivo de los sucesivos traspasos, así como detalle de las técnicas que hayan podido aplicarse y el estado inicial y final de las muestras (art. 359).

Sin necesidad de tan específicas disposiciones a nivel legal es exigible también hoy asegurar y documentar la regularidad de la cadena para garantizar la autenticidad e inalterabilidad de la fuente de prueba. Cuando se comprueban deficiencias en la secuencia que despiertan dudas razonables, habrá que prescindir de esa fuente de prueba, no porque el incumplimiento de alguno de esos medios legales de garantía convierta en nula la prueba, sino porque su autenticidad queda cuestionada. No se pueden confundir los dos planos. Irregularidad en los protocolos establecidos como garantía para la cadena de custodia no equivale a nulidad. Habrá que valorar si esa irregularidad (no mención de alguno de los datos que es obligado consignar; ausencia de documentación exacta de alguno de los pasos...) es idónea para despertar dudas sobre la autenticidad o indemnidad de la fuente de prueba. Ese es el alcance que se atribuía a la regularidad de la cadena de custodia en la normativa proyectada aludida: "El cumplimiento de los procedimientos de gestión y custodia determinará la autenticidad de la fuente de prueba llevada al juicio oral... El quebrantamiento de la cadena de custodia será valorado por el tribunal a los efectos de determinar la fiabilidad de la fuente de prueba " (art. 360). No es una cuestión de nulidad o inutilizabilidad, sino de fiabilidad"[77].

77 ECLI:ES:TS:2013:1925, en https://vlex.es/vid/438314490; o Sentencia de la Audiencia Provincial de Barcelona de 29 de diciembre de 2017, Número Recurso: 74/2016, DOCUMENTO TOL6.473.659, entre otras.

En definitiva, el proceso de valoración sería la última fase del procedimiento probatorio, y sólo se llega a él cuando la prueba aportada al proceso es admitida por ser fiable, por el contrario, será nula cuando en su obtención se hayan vulnerado derechos fundamentales.

d.2 Procedimientos que verifican la no manipulación de la información

Solemos pensar que cuando borramos un email o un Whassapp eliminamos por completo la información contenida en ellos, pero ello no es del todo cierto. La verdad es que la información eliminada de los dispositivos de almacenamiento digital, suelen dejar rastro, es lo que se viene denominando "huella digital", la cual se puede analizar, este análisis conlleva una serie de pasos que se pueden desarrollar a través de diferentes métodos, que sirven tanto para recuperar el archivo eliminado como para verificar que la información no haya sido manipulada en su contenido y emisor. Para ello, se han venido utilizando diferentes métodos, los más tradicionales son el de la copia Bit a Bit y los Algoritmos pero existen algunos más. Vamos a ver los más utilizados.

a) Copia Bit a Bit

Es una herramienta que se creó específicamente para la administración de sistemas y para hacer respaldo de datos, pero dada la eficacia de tal herramienta se empezó a utilizar el programa "dd" que posibilita realizar el proceso de copia de la información contenida en el medio de almacenamiento desde cualquier ordenador y tiene un porcentaje de efectividad del 100%[78].

Actualmente se ha avanzado tanto en las nuevas tecnologías que, aunque los dispositivos de almacenamiento digital hayan sufrido daños, se pueden hacer copias Bit[79] a Bit sin influir estos daños en el resultado o la veracidad de

78 Véase a MONTOYA ROJAS, Alejandra, "La informática forense como herramienta para la aplicación de la prueba electrónica", en *Revista CES Derecho*, vol. 1, nº 1, 2010. pág. 10.

79 Señala FLORES PRADA, I., "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia", en *Revista Electrónica de Ciencia Penal y Criminología*, núm. 17, 2015, pág. 3, que el Bit "es el elemento más pequeño en el ADN de la información. Consiste en combinaciones binarias compuestas exclusivamente por dos números, el 1 y el 0. Los bits han sido siempre el elemento básico de la computación digital, pero durante los últimos veinticinco años hemos ampliado enormemente nuestro vocabulario binario hasta poder representar mucho más que números. Hemos conseguido

la información almacenada en el dispositivo[80].

La copia se realiza, por tanto, a los bits no al dispositivo de almacenamiento, y son los bits los que servirán de elementos material probatorio. Los análisis forenses se realizarán en la copia que se debe hacer de la réplica y ésta a su vez de la original. Mediante este procedimiento se consigue verificar que la información contenida en el dispositivo no haya sido manipulada, sino que también se podrán recuperar archivos e información borrada[81].

Este sistema permite que la información no sufra ningún cambio en su contenido original, puesto que se trabaja sobre las copias, sobre el dispositivo de almacenamiento sólo se lleva a cabo una lectura y, por tanto, queda incólume el elemento material probatorio.

b) Los algoritmos

Los algoritmos son un "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema"[82]. Los algoritmos se encargan de localizar el lugar donde está almacenado el programa, para cargarlo y mostrárselo al usuario.

Esta herramienta al igual que la copia Bit a Bit, permite conservar la cadena de custodia y, por tanto, se dirige a la verificación de no adulterabilidad o manipulación de la información, pero esta no es la finalidad principal de dicha herramienta, sino que lo que se quiere conseguir es preservar y garantizar la cadena de custodia, pero para ello se tiene que pasar por la verificación de veracidad de los datos. La ventaja de esta herramienta, a diferencia de la copia Bit a Bit es que en archivo grandes el error en cuanto a la verificación de inalterabilidad de la información es mucho menor. En este sentido, las dos herramientas, aunque tienen finalidades distintas en sentido estricto, sin embargo, las dos sirven como medio para garantizar o dar seguridad de la inalterabilidad de la información e idoneidad de la prueba electrónica o mensajes de datos.

---

digitalizar cada vez más tipos de información, auditiva y visual, por ejemplo, reduciéndolos de igual manera a unos y ceros".

80 Señala MONTOYA ROJAS, "La informática forense…, op. cit., pág. 10, que: "La información contenida en el documento electrónico, no es sólo una combinación de átomos sino que también existen documentos conformados por Bits, lo que hace más fácil la copia bit a bit y, por tanto, el resultado de la copia es de mayor confianza en cuanto a la veracidad e inmodificabilidad de la información".

81 MONTOYA ROJAS, "La informática forense…, op. cit., pág. 10.

82 Definido así por el Diccionario de la Real Academia de la Lengua Española.

c) Herramientas adicionales: los MFT (Managet File Transfer) y FAT (File Asignation Table)

Además de las dos herramientas comentadas anteriormente que son las mas utilizadas, existen otras que también sirven a la misma finalidad.

Por un lado, el MFT, Managet File Transfer o tabla maestra de archivos es el primer archivo de un volumen NTFS[83]. Sin profundizar en las funciones de esta herramienta, hay que decir que consiste en un directorio que centraliza todos los ficheros del disco y de sí misma, haciendo referencia de manera continua a los ficheros mientras el sistema accede a la información, la procesa y la escribe en el disco. Por otro lado, el FAT o Tabla de Asignación de Archivos, es un sistema de ficheros muy simple, que consiste en que a cada disco se asocia una tabla (FAT) con una entrada por cada bloque de disco. Cada entrada de la FAT puede contener: una dirección de disco, una marca de bloque libre (significa que el bloque no está asignado), una marca de bloque defectuoso o una marca de fin de archivo (EOF)[84].

Además de estas herramientas, la informática forense cuenta con otros sistemas sobre los cuales no vamos a entrar por exceder del objeto del trabajo pero que también sirven al mismo propósito.

En definitiva, en la elaboración del informe pericial forense, el perito Forense informático hace uso de determinadas herramientas informáticas que son la base esencial de los análisis de las evidencias digitales, que deben ser confiables y predecibles para el investigador, y deben ser identificadas en su Informe, con la finalidad de dar soporte al mismo, y transmitir transparencia[85].

d.3 Fiabilidad

En relación con los requisitos de validez que debe tener la prueba electrónica para considerar que no ha sido manipulada, no quisiera dejar de hacer

83 El sistema de archivos NT (NTFS), que a veces también se denomina Sistema de archivos de nueva tecnología, es un proceso que utiliza el sistema operativo Windows NT para almacenar, organizar y encontrar archivos en un disco duro de manera eficiente.

84 VILLARREAL, Vladimir, Sistemas Operativos, 2017, pág. 76. En Fuente del documento Repositorios Institucional UTP-Ridda2: http://ridda2.utp.ac.pa/handle/123456789/5074.

85 SANZ-GADEA GÓMEZ, Juan Bautista, *Los informes periciales informáticos*..., op. cit.

referencia a una sentencia que tuvo bastante repercusión mediática en la cual el Tribunal Supremo establece los presupuestos para aceptar los mensajes de las redes sociales como prueba en los juicios, en concreto, la Sentencia del Tribunal Supremo de 19 de mayo de 2015[86]. En esta Sentencia, el Tribunal Supremo resuelve un recurso de casación por infracción de ley, quebrantamiento de forma y vulneración de precepto constitucional contra una sentencia dictada por la Audiencia Provincial de Valladolid condenando al acusado a cinco años y un día de prisión por un delito de abusos sexuales. La importancia de esta sentencia es que el Tribunal Supremo analiza la viabilidad de los "pantallazos" obtenidos de las redes sociales, en concreto en este caso de Tuenti para concluir su validez y autenticidad.

No obstante, el Tribunal Supremo en dicha sentencia adoptó una postura contradictoria, puesto que, aunque en el caso concreto admitió la validez de los pantallazos como prueba electrónica en el juicio, sin embargo, las apreciaciones que realizó de la misma iban encaminadas a ser cauteloso con la admisión de este tipo de pruebas. Así, el Tribunal Supremo es consciente de la volatilidad de las conversaciones mantenidas vía WhatsApp, puesto que son fácilmente manipulables, además también hace referencia a dos características que posibilitan el que el usuario puede fingir conversar con alguien cuando en realidad se está relacionando consigo mismo, como son el anonimato que permite el sistema y la libre creación de cuentas con una identidad falsa[87].

El TS concluyó que "si bien la valoración de la prueba en estos casos de mensajería instantánea debía ser abordada con todas las cautelas precisamente por la posibilidad real de manipulación, en este caso se debían valorar otras pruebas circunstanciales como era el hecho de que la propia víctima hubiera puesto a disposición del Juez de Instrucción su contraseña de Tuenti con el fin de que se pudiera solicitar un informe pericial, así como que hubiera obtenido los pantallazos también en presencia de la guardia civil, o la circunstancia de que el otro interlocutor de los mensajes hubiera acudido como testigo al juicio"[88].

86 STS 300/2015, de 19 de mayo de 2015, en Tirant on line, TOL5.002.579.

87 En esta sentencia el Tribunal Supremo establece que cualquier persona puede crear pruebas electrónicas falsas específicamente para conseguir un fallo a su favor, más aún cuando la misma se puede capturar mediante un pantallazo e incorporarlo con una imagen digital fija y que se puede incorporar a la causa como documento digitalizado o incluso en papel impreso.

88 Ibídem.

Por tanto, una de las características principales de la prueba electrónica que la diferencia de la prueba tradicional es la volatilidad o fragilidad de la misma[89]. En este sentido, la prueba electrónica es fácilmente manipulable sin que sea fácil detectar la alteración o modificación, en algunos casos incluso será imposible detectar las modificaciones llevadas a cabo.

Si bien, aunque es fácil la manipulación de este tipo de prueba, la línea jurisprudencial seguida desde la sentencia de 2015 comentada es que tales mensajes enviados vía WhatsApp son fácilmente manipulables, pero si existen circunstancias que excluyen razonablemente la duda de su alteración, no es necesario acudir a la prueba pericial[90].

---

89 Señala la doctrina que la prueba electrónica tiene las siguientes características: a) Intangibles; b) Volátiles; c) Delebles o destruibles; d) Parciales; e) Intrusivas. Véase a PÉREZ PALACI, José Enrique, "Las pruebas electrónicas: Consideraciones", op. cit., pág. 13.

90 STS 754/2015, de 27 de noviembre, en Tirant on line, DOCUMENTO TOL5.602.357. En esta sentencia, el TS manifiesta citando la STS 300/2015, de 19 de mayo , que "*las conversaciones mantenidas entre el acusado y Cristina, incorporadas a la causa mediante "pantallazos" obtenidos a partir del teléfono móvil de la víctima, no son propiamente documentos a efectos casacionales. Se trata de una prueba que ha sido documentada a posteriori para su incorporación a la causa. Y aquéllas no adquieren de forma sobrevenida el carácter de documento para respaldar una impugnación casacional. Así lo ha declarado de forma reiterada esta Sala en relación, por ejemplo, con las transcripciones de diálogos o conversaciones mantenidas por teléfono, por más que consten en un soporte escrito o incluso sonoro (por todas, SSTS 956/2013 de 17 diciembre ; 1024/2007 , 1157/2000, 18 de julio y 942/2000, 2 de junio).*

Ahora bien, respecto a la queja sobre la falta de autenticidad del diálogo mantenido a través del sistema chino "We Chat", que es un modo comunicación basado en los mensajes cortos, bidireccionales, tipo "Whatsapp" , la Sala quiere reiterar una idea básica, que ya fue declarada por la STS 300/2015, de 19 de mayo , y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido".

En el plano internacional[91], la norma ISO/IEC 27037:2012 "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence" viene a configurar unos principios generales para lograr la mayor fiabilidad de estas pruebas. Esta norma dirigida a recopilar evidencias digitales viene a sustituir a las ya antiguas directrices RFC 3227[92] estando las recomendaciones de la ISO 27037

En este caso, sí se aceptan los mensajes porque la propia defensa del recurrente admitió su remisión.

También la STS 375/2018, de 19 de julio, en Tirant on line, DOCUMENTO TOL6.677.063. El Tribunal Supremo viene a manifestar que *"no es posible entender, como se deduce del recurso, que estas resoluciones establezcan una presunción iuris tantum de falsedad de estas modalidades de mensajería, que debe ser destruida mediante prueba pericial que ratifique su autenticidad y que se debe practicar en todo caso; sino que, en el caso de una impugnación (no meramente retórica y en términos generales) de su autenticidad –por la existencia de sospechas o indicios de manipulación– se debe realizar tal pericia acerca del verdadero emisor de los mensajes y su contenido. Ahora bien, tal pericia no será precisa cuando no exista duda al respecto mediante la valoración de otros elementos de la causa o la práctica de otros medios de prueba. En el presente caso, no hay razones para mantener una duda al respecto. En primer lugar, porque la propia víctima pone a disposición del Juez de Instrucción su teléfono móvil, del que directamente se consultan y transcriben los mensajes por el Letrado de la Administración de Justicia. Éste, como indica la sentencia recurrida, realiza una transcripción, que obra al folio 19 y siguientes del Tomo II de la causa en instrucción, y en ella se recoge íntegramente el contenido de los mensajes cruzados, el teléfono donde se encuentran y aquel del que proceden, que es número NUM000.*

Además, el uso de este número es atribuido a la acusada. Con todo ello, se garantiza, en primer lugar, que si las conversaciones hubieran llegado a ser cuestionadas en cuanto a su origen y/o contenido se hubiera podido asegurar su autenticidad mediante el correspondiente informe pericial; y, en segundo lugar, la forma y modo en que los mensajes se obtuvieron despeja cualquier duda sobre tales extremos, que no surgen por el mero hecho de que el recurrente indique que pudieron haber sido objeto de manipulación o que existen serias dudas sobre la cadena de custodia de los mensajes, ya que se trata de argumentos puramente retóricos y no sustentados en un indicio mínimamente objetivo sobre que ello hubiera sucedido así".

91 Véase toda la información referida al ámbito internacional en https://www.iso-27001security.com/html/27043.html.

92 Los RFC «Request For Comments» son catalogados con "documentos que recogen propuestas de expertos en una materia concreta, con el fin de establecer por ejemplo una serie de pautas para llevar a cabo un proceso, la creación de estándares o la implantación de algún protocolo. El RFC 3227 es un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento, y puede llegar a servir como estándar de

más enfocadas a dispositivos actuales y que son más acordes con la técnica utilizada actualmente.

Así, esta norma establece una serie de instrucciones de carácter general para los forenses informáticos. La norma no trata el análisis de las evidencias digitales, sino que se circunscribe a regular el procedimiento del peritaje en las fases de identificación, recopilación y conservación de estas[93]. La finalidad principal es la de configurar un contexto general de actuación o protocolo que permita garantizar que los procedimientos aplicados en la pericia forense son los adecuados y que se realizan con arreglo a la normativa legal.

La tipología de dispositivos tratados en la norma, son los siguientes:

a) Equipos y medios de almacenamiento y dispositivos periféricos

b) Sistemas de navegación móvil

c) Ordenadores y dispositivos conectados en red

d) Dispositivos móviles

e) Sistemas de circuito cerrado de televisión digital[94]

Aunque la norma establece unos principios básicos aplicables a toda la tipología de dispositivos tratados, sin embargo, para cada uno de ellos establece un tratamiento diferente en cada una de las fases reguladas por la norma, es decir, tanto en la identificación, como en la recopilación y conservación.

Los principios que deben regir las evidencias digitales son tres: a) relevancia; b) fiabilidad y; c) suficiencia. La norma determina que estos tres principios fijan los requisitos necesarios para que los peritos forenses puedan acceder, asegurar y conservar los elementos materiales probatorios sobre medios digitales, los cuales podrán ser examinados y analizados por terceros interesados y sometidos posteriormente a contradicción según el ordenamiento jurídico donde se encuentren[95].

Además de la norma comentada, posteriormente se han dictado otras que

---

facto para la recopilación de información en incidentes de seguridad". Véase con mayor profundidad en https://www.incibe-cert.es/blog/rfc3227.

93 Señala PÉREZ PALACI, José Enrique, que "Los principios básicos en los que se basa la norma son: a) Aplicación de métodos; b) Proceso auditable; c) Proceso reproducible; d) Proceso defendible; e) La identificación; f) La recolección y/o identificación; g) La conservación/preservación". En "La prueba electrónica: Consideraciones", op. cit., págs. 18 y 19.

94 ISO/IEC 27037:2012.

95 Véase PALAZZI, PABLO A., *Los Delitos Informáticos en el Código Penal Análisis de la ley 26.388*, Buenos Aires, 2016, en https://www.academia.edu/37287925/Los_Delitos_Informaticos_en_El_Pablo_a_Palazzi_2_pdf?auto=download.

completan el tratamiento pericial de las evidencias digitales. En concreto, serían las siguientes:

– La ISO/IEC 27041:2015 Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method.

Esta norma pretende orientar sobre los mecanismos de garantía de la ciencia forense digital, por ejemplo, asegurando que los métodos y herramientas que se utilizan sean los apropiados.

Esta norma, que completaría la inmediatamente anterior, sirve como directriz para establecer unos estándares en el análisis e interpretación de las evidencias digitales cuando estas han sido recogidas. Pretende ser una guía para asegurar la idoneidad y adecuación del método de investigación de los incidentes que puedan darse.

El propósito fundamental de los estándares forenses digitales ISO27k es promover métodos y procesos de buenas prácticas para la captura forense y la investigación de la evidencia digital. El enfoque principal de esta norma es asegurar los procesos periciales forenses y las herramientas utilizadas en la investigación de las evidencias digitales. La autenticidad, la fiabilidad y la integridad son requisitos fundamentales para todos los métodos forenses: esta norma pretende asegurar los aspectos de idoneidad y adecuación en el proceso de investigación de los incidentes digitales.

Si bien tanto los investigadores privados como las organizaciones y los estados pueden llevar a cabo sus propios métodos, procedimientos y controles, se espera que la estandarización conduzca a la eventual adopción de enfoques similares, si no idénticos, a nivel internacional, lo que hará que sea más fácil comparar, combinar y contrastar los resultados de tales investigaciones incluso cuando seann realizadas por diferentes personas u organizaciones y potencialmente en diferentes jurisdicciones.

– Por su parte, la norma ISO/IEC 27042:2015, Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence, establece el procedimiento de análisis e interpretación de las evidencias digitales.

La norma ofrece la orientación necesaria sobre el análisis e interpretación de la evidencia digital englobando las cuestiones de custodia, validez, reproducibilidad y repetibilidad. Recoge las mejores prácticas para la selección, el diseño y la implementación de procesos analíticos y el registro de información necesaria para permitir que dichos procesos estén sujetos a una compro-

bación independiente cuando sea necesaria. Esta norma ofrece las pautas que deben seguirse en relación con los mecanismos adecuados para demostrar el dominio y la competencia del equipo de investigación.

La norma ISO 27042 al igual que la ISO 27037 proporcionan un marco común para los elementos analíticos e interpretativos del manejo de incidentes de seguridad de sistemas de información, que pueden ser de utilidad para la implementación de nuevos métodos y proporcionar un estándar mínimo común para el tratamiento de las evidencias digitales recogidas a partir de tales actividades.

– La norma ISO/IEC 27043: 2015, Information technology – Security techniques – Incident investigation principles and processes, trata las actividades más amplias de investigación de incidentes, dentro de las cuales generalmente se realizan los análisis periciales.

La norma se refiere tanto a los principios que subyacen en los procesos de análisis forense como al propio proceso de investigación de incidentes con evidencias digitales.

El objetivo principal de esta norma es establecer la base de un modelo general idealizado aplicable a diferentes escenarios de incidentes de seguridad informática que contengan evidencias digitales. Esto incluye todas las fases del proceso de investigación: desde la preparación previa al incidente hasta que concluye la misma, así como consejos generales y advertencias. Hay que resaltar que esta norma proporciona unos principios y procesos generales aplicables a diferentes escenarios, pero no contempla particularidades, remitiendo a otras normas internacionales con contenido más específico sobre los procesos.

– La norma ISO/IEC 27050:2016+ – Information technology – Security techniques – Electronic discovery, se compone de 4 partes.

Esta norma, que se compone de varias partes, se refiere en concreto a la fase de descubrimiento electrónico que incluye las siguientes fases, aunque estas no son excluyentes:

a) Identificación: se identifica el ESI (información almacenada electrónicamente) que es potencialmente relevante para un determinado caso, junto con sus ubicaciones, almacenajes, tamaños / volúmenes, etc. Nota: esto puede ser más complejo de lo que puede parecer, por ejemplo, obteniendo datos que pertenecen no solo a los individuos sospechosos sino también a otras personas de su entorno como, por ejemplo, organizaciones, compañías telefónicas y proveedores de servicios como correo electrónico y acceso a Internet

(ISP), incluso las redes sociales. A menudo, esta fase es crítica y es importante el tiempo que transcurra puesto que la potencial prueba (especialmente los datos operacionales efímeros) se puede perder o destruir antes de que se haya obtenido y preservado;

b) Conservación: el ESI identificado y potencialmente relevante se coloca bajo custodia legal, comenzando el proceso pericial diseñado para garantizar la protección en todo momento de posibles pérdidas, robos, daños accidentales, interferencias, manipulación, reemplazo y sustitución que puede llevar a devaluar esta información con la potencial inadmisión o inutilización del ESI.

c) Recopilación: el ESI se obtiene del dispositivo de custodia original separando los medios de almacenamiento digital originales (discos duros, tarjetas y tarjetas de memoria, CD, DVD, etc) y la posible evidencia física asociada (huellas dactilares o evidencia de ADN) que puedan vincular a un sospechoso del delito y custodiándolos de una forma más segura.

En algunos casos (Internet, la nube, la RAM, etc.) puede llegar a ser imposible proteger los datos mediante la captura u obtención de los medios físicos. Por ello, estos datos en algunos casos deben capturarse directamente en una forma forense de sonido[96].

d) Procesamiento: las copias forenses de bits se almacenan de tal forma que les permite buscar o analizar información relevante para el caso, utilizando herramientas y plataformas forenses adecuadas. La importancia de esta fase es separar los pocos datos relevantes de un volumen mucho más grande que normalmente se ha recopilado;

e) Revisión: se buscan o analizan copias de bits forenses para obtener información relevante para el caso;

f) Análisis: la información se analiza y evalúa en cuanto a su relevancia, idoneidad, volumen, significado, implicaciones, etc. La información útil se obtiene de los datos seleccionados;

g) Incorporación al proceso: la información relevante del análisis, más los medios de almacenamiento originales, etc., se presentan formalmente ante el

96 Si existe alguna duda razonable sobre la posible devaluación de los datos obtenidos es posible presentar ante el tribunal el análisis de las copias de bits realizadas con las herramientas y métodos forenses adecuados, en lugar de la evidencia original en sí. Además, hay que tener en cuenta también que eliminar físicamente los sistemas y los medios de comunicación bajo la custodia de un tercero podría clasificarse como un incidente de seguridad de la información con claras implicaciones sobre la confidencialidad, integridad y disponibilidad de la información, particularmente porque, en esta etapa, el caso no está probado.

tribunal como prueba. Esto inevitablemente implica demostrar y explicar el significado de la evidencia en términos que tengan sentido para el tribunal[97].

En concreto, las cuatro partes que componen la ISO/IEC 27050 son las siguientes:

1. ISO / IEC 27050-1: 2019 Tecnología de la información - Técnicas de seguridad - Descubrimiento electrónico - Descripción general y conceptos

– Descripción general de eDiscovery;

– Define los términos, conceptos, procesos, etc., tales como información almacenada electrónicamente;

– Presenta y define el alcance y el contexto de este estándar de varias partes;

– Estado: la parte 1 se publicó en 2016 y se actualizó en 2019.

2. ISO / IEC 27050-2: 2018 Tecnología de la información - Técnicas de seguridad - Descubrimiento electrónico - Orientaciones para la gobernanza y gestión del descubrimiento electrónico

– Guía de gestión para identificar y tratar los riesgos de información relacionados con la exhibición de documentos electrónicos, por ejemplo, estableciendo e implementando políticas relacionadas con eDiscovery y cumpliendo con las obligaciones (mayoritariamente legales) y expectativas relevantes;

– Proporciona orientación sobre la buena gobernanza para el trabajo forense, es decir, el marco o estructura general dentro del cual se llevan a cabo las actividades forenses digitales y se gestionan a través de un conjunto de actividades controladas, repetibles y confiables;

– Sugiere algunas métricas posibles.

– Estado: la parte 2 se publicó en 2018.

3. ISO / IEC 27050-3: 2017 Tecnología de la información - Técnicas de seguridad - Descubrimiento electrónico - Código de prácticas para descubrimiento electrónico

– Identifica los requisitos y ofrece orientación sobre los siete pasos principales de eDiscovery mencionados anteriormente (identificación, preservación, recolección, procesamiento, revisión, análisis y producción de ESI);

97 Con suerte, algo parecido a "Declaro, bajo juramento, que cumplimos plenamente con ISO/ IEC 27050", en el futuro, -evitará una serie de desafíos relacionados con los procesos de descubrimiento electrónico-.

– Esencialmente, una guía básica y genérica de cómo hacerlo que presenta los elementos clave que, sin duda, formarán la base de muchos manuales forenses digitales a su debido tiempo;

– Estado: la parte 3 se publicó en 2017.

– Una revisión "básica" está en la etapa de FDIS y, por lo tanto, debe publicarse a principios de 2020.

4. ISO / IEC 27050-4 (BORRADOR) Tecnología de la información - Descubrimiento electrónico - preparación técnica

– Orientación sobre la tecnología de descubrimiento electrónico, es decir, las herramientas y sistemas forenses que respaldan la recopilación, el almacenamiento, la búsqueda, el análisis y la producción de ESI, además de los procesos relacionados;

– Estado: el proyecto que desarrolla la parte 4 se reinició en 2017. La Parte 4 se encuentra actualmente en la etapa de borrador del Comité y se publicará en 2021.

– Finalmente, debo hacer referencia a la British Standard BS 10008:2008 "Evidential weight and legal admissibility of electronic information. Specification."

Encontramos también la normativa British Standard BS 10008 que, si bien es menos conocida, está siendo cada vez más introducida en las organizaciones. La importancia y utilidad de esta directriz no debe ser infravalorada, puesto que, si bien pone el foco en las exigencias del mercado británico, es aplicable más allá de sus fronteras, en cualquier país y puede ser de gran utilidad a ciertas organizaciones y empresa.

Al igual que las normas internacionales que han sido previamente analizadas, la BS 10008 establece un sistema de control de calidad y riesgos que permite probar la calidad y fiabilidad de la información electrónica. La principal diferencia que presenta esta norma frente a la ISO 27001 es que la directriz británica limita su alcance a la información electrónica, que es, en ocasiones, difícil de obtener a través de las ISO dado el amplio alcance que presenta la norma internacional. Por el contrario, la BS 10008 está diseñada para que las organizaciones, corporaciones y empresas reduzcan o incluso eliminen por completo el papel físico deviniendo apropiada su aplicación en los siguientes casos:

– En el caso de documentos escaneados o firmados electrónicamente en los que la autenticidad es necesaria para demostrar la calidad y fiabilidad de los datos.

– Cuando una organización no quiere incluir todos los activos de información en toda la empresa.

– Cuando una organización desea limitar el ámbito de aplicación a determinada información electrónica contenida en dispositivos electrónicos concretos.

– Cuando se pretende un rápido cumplimiento de la normativa: la capacidad de limitar el ámbito de aplicación acelera su acreditación.

– Para salvaguardar información electrónica durante años, incluida la originada de forma digital, que puede convertirse en evidencia ante una disputa.

En definitiva, el propósito principal de las normas relativas al tratamiento forense de las evidencias digitales comentadas (ISO/IEC 27037, 27041, 27042, 27043 y 27050) es promover métodos y procesos de buenas prácticas para la obtención, conservación, análisis, etc, forense y la investigación de la evidencia digital. Como se advirtió anteriormente, si bien los investigadores privados, las organizaciones y los Estados pueden aplicar sus propios métodos, procesos y controles, se espera que la estandarización de estas normas suponga un marco común a nivel internacional que facilite la investigación entre los diferentes países.

d.4 Autenticidad

En relación con la autenticidad de la prueba electrónica, muchas de las veces, como ya he mencionado anteriormente, será necesario un informe pericial que acredite la autenticidad de aquella teniendo en cuenta la facilidad que existe a la hora de manipularlas y la complejidad técnica de dichas pruebas. En este sentido, se puede practicar una prueba pericial informática.

La labor del perito informático forense estribará fundamentalmente en el desarrollo de procedimientos dirigidos a "preservar" o "conservar" las evidencias digitales que se puedan extraer del contenido electrónico con la finalidad de que se pueda aportar en el juicio correspondiente. Esta "conservación" se realiza mediante la creación de copias forenses "exactas" de la información digital que está almacenada, proporcionando un código alfanumérico de dicha información (código *hash*). Para este tipo de pericias se utilizan programas como FtkImager, Encase, etc. Es necesario que la copia se realice por duplicado, de manera que una copia se deposite ante Notario, y la otra se quede en poder del perito para su posterior análisis técnico. Las técnicas que utiliza el perito forense son de carácter selectivo ya que sólo debe buscar aquella infor-

mación que resulte necesaria para la investigación, a través, por ejemplo, de las denominadas búsquedas "ciegas", evitando con ello posibles injerencias en datos o informaciones de carácter íntimo o privado del sujeto investigado garantizando así la no vulneración de sus derechos fundamentales, por ejemplo, en el ámbito laboral garantizando la no injerencia en datos de carácter privado del trabajador[98].

Por último, los resultados que arroje la investigación serán trasladados al informe que el perito técnico realice y que será aportado al proceso. Además, para evitar posibles impugnaciones de las partes, el perito puede ser llamado a la vista para que ratifique el informe presentado y se le pueda preguntar.

En definitiva, el informe del experto informático garantiza en el proceso la originalidad, autenticidad e integridad de la evidencia o información digital de manera que se pueda valorar como prueba digital. En la práctica es habitual realizar este tipo de informes cuando hay que registrar el disco duro de un ordenador, donde existe gran cantidad de información que analizar y es fácilmente manipulable. También, como se ha puesto de manifiesto, es aconsejable utilizar este tipo de informes en los casos en los que se constate que ha existido un uso abusivo o indebido de navegación en internet, o averiguación de identidades en redes sociales a través de complejos sistemas de patrones comunes de actuación, debido a que en muchos casos se utilizarán distintos perfiles o "avatares" que no se corresponden fácilmente con la identidad del investigado[99].

También es posible que la parte que vea impugnada su prueba proponga cualquier otro medio de prueba que acredite la autenticidad de la misma, como puede ser, por ejemplo, solicitar al juez que libre un requerimiento al prestador de servicios de comunicaciones electrónicas para que indique el contenido del mensaje. Esta posibilidad se puede dar por la vía del artículo 326 de la Ley de Enjuiciamiento Civil[100], ya que se permite acreditar la au-

98 Véase a ROJAS ROSCO, Raúl, "La prueba digital en el ámbito laboral ¿son válidos los pantallazos?", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016, págs. 95 y 96.

99 Ibídem.

100 En dicho artículo se regula la fuerza probatoria de los documentos privados y se indica literalmente que: "1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.

2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya pre-

tenticidad del documento privado cuando ha sido impugnado por cualquier medio de prueba que resulte útil y pertinente al efecto, por tanto, es posible que para acreditar la autenticidad del contenido de un WhatsApp se solicite al juzgado que requiera a un tercero, en concreto al prestador de servicios de esta comunicación electrónica, para que indique el contenido exacto del mensaje y, de esta forma, acreditar su autenticidad e integridad. Así, de acuerdo al artículo 42 de la Ley General de Telecomunicaciones[101]: "*la conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*". Por tanto, en relación a la cesión de los datos es la Ley 25/2007 la que resulta aplicable también en estos supuestos.

Sin embargo, a día de hoy hay que tener en cuenta que los mensajes enviados vía Whatsapp son fácilmente manipulables por lo que es difícil acreditar la autenticidad e integridad de un mensaje debido a debilidades de seguridad de la propia aplicación, lo que hace imposible acreditar la cadena de custodia. A diferencia de los correos electrónicos, los mensajes de Whatsapp no se almacenan en un servidor online, sino que el terminal envía y recibe los datos directamente, y es factible editar la información sin dejar ningún rastro lo que conlleva la dificultad de contrastarlos. WhatsApp guarda la información en una base de datos sin cifrar dentro del terminal móvil, pudiendo accederse a los mismos como usuario administrador del terminal[102].

---

sentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.

Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

3. Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica".

101 Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. Publicado en el «BOE» núm. 114, de 10/05/2014.

102 De acuerdo al artículo 43 de la Ley General de Telecomunicaciones: "1. Cualquier

En 2019, con la finalidad de disminuir el número total de denuncias de abuso sexual infantil no sólo en la UE sino en el resto del mundo, la empresa Facebook manifestó la intención de implementar por defecto el cifrado de extremo a extremo en su servicio de mensajería instantánea. Se calculó que ello supondría rebajar las denuncias entre el 50% y el 67%, puesto que las herramientas de detección utilizadas hasta entonces no eran válidas en comunicaciones cifradas de extremo a extremo[103]. Facebook valoró la importancia de la implementación de esas medidas dada la ausencia de nuevas medidas técnicas complementarias.

El cifrado de extremo a extremo está activo por defecto en WhatsApp y no hay forma de desactivarlo.

d.5 Integridad del contenido

Como indicaba anteriormente, la volatilidad de estas aplicaciones es tal que es fácil manipular el contenido de los mensajes. En relación con los WhatsApp, a diferencia de otros sistemas de comunicación, es especialmente significativo, porque esta aplicación no conserva en un servidor externo perteneciente al administrador el contenido de los mensajes, sólo se conserva en el dispositivo de quienes se están comunicando, por lo que es fácilmente manipulable por cualquiera de ellos. Por ello es fundamental que el perito informático haga su informe lo más rápido posible, aunque es cierto que siempre dejará un rastro que podrá ser analizado por el perito informático. Por tanto, ni siquiera el servicio externo puede acceder al contenido cifrado.

Como indica el Tribunal Supremo en la ya comentada sentencia 300/2015, "*la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de*

---

tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente".

103 Véase a ALONSO LECUIT, Javier, "El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea", en *Estudios Internacionales y Estratégicos*", ARI 4/2021 – 14/1/2021, en http://www.realinstitutoelcano.org/.

las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido".

Aunque no voy a profundizar en cuestiones relativas a la manipulación de las aplicaciones informáticas por ser una cuestión que deriva muy compleja por su carácter técnico sí quisiera apuntar, aunque fuera someramente, que es bastante factible manipular datos de contenido[104]. Así, cualquier archivo informático cuenta con una serie de datos "ocultos" que describen el contenido informativo de un objeto al que se le denomina recurso, son los denominados metadatos[105]. A todos estos datos "ocultos" o metadatos se acceden mediante el software, y este software también puede ser manipulado, ya que existen herramientas de software que pueden modificarlos o suprimirlos. Sin entrar en profundidad en ello, solo mencionar que existe una herramienta de software, llamada "Exiftool" que precisamente sirve para ello[106]. Ahora bien, al igual que es posible modificar o suprimir datos, a sensu contrario, también existen instrumentos y herramientas que sirven para garantizar y proteger el contenido de los soportes informáticos o automatizados, aunque esta protección va dirigida más a los terceros puesto que es posible que los autores del documento digital modifiquen su propio archivo[107].

En definitiva, la misma facilidad que existe para comunicarnos existe para manipular la información. Aunque se ha avanzado mucho en los sistemas de comunicación, sin embargo, la seguridad que ofrecen en cuanto a su acceso como prueba en el proceso es todavía cuestionable dada la facilidad de la manipulación. Es necesario extremar todas las cautelas posibles para proteger el contenido de la información y no todo el mundo está familiarizado con el

104 Los datos de contenido junto con los datos de tráfico son datos informáticos.

105 Véase a PERALES CAÑETE, Rafael, "Exiftool: Los metadatos sirven de algo", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016, págs. 110 y ss.

106 Ibídem, pág. 111.

107 Una de las herramientas que se utilizan para encriptar el archivo es la denominada "Foxit Reader", véase a PERALES CAÑETE, Rafael, "Exiftool…", op. cit., pág. 113.

mundo informático. Por ello, la prueba digital o tecnológica ha de ser valorada con mucha cautela y siempre en conjunto con los demás medios de prueba practicados en el proceso.

d.6 Idoneidad, pertinencia y necesidad de la prueba electrónica en los delitos cometidos a través de las nuevas tecnologías

En el Capítulo IV y siguientes del Título VIII del Libro II de la LECrim se regulan las medidas de investigación tecnológica que fueron introducidas por la Ley Orgánica 13/2015. Como señala PÉREZ GIL, "era necesario un reconocimiento legal de la especificidad de la información en formato electrónico, la singularidad de la regulación de esta materia debe venir por la atención al formato en el que se encuentra la información electrónica en forma de datos y la especificidad que de ello se deriva"[108].

La LO 13/2015, estableció unos principios rectores aplicables a todas las medidas de investigación tecnológica que vienen a recoger toda la doctrina jurisprudencial recaída durante muchos años dada la insuficiencia de regulación legal sobre dicha materia. Por tanto, esta ley viene a plasmar el principio de legalidad que necesariamente debe imperar con carácter primordial antes de fijar los principios rectores. En concreto, es en el artículo 588 bis a de la Ley de Enjuiciamiento Criminal donde se fijan estos principios, entre otros, el de judicialidad, especialidad, idoneidad, excepcionalidad, necesidad, etc., como a continuación pasaré a comentar[109].

Posteriormente, el legislador establece con el mismo tratamiento común una serie de disposiciones generales relativas al procedimiento de adopción y ejecución de todas las medidas como son: la necesidad de autorización judicial, los requisitos de la resolución, el secreto de las actuaciones, la duración, las posibilidades de prórroga, el control judicial, la posible afectación de terceras personas, etc.

Y, finalmente, el legislador regula de forma diferenciada las cinco medidas tecnológicas de investigación.

---

108 Véase PÉREZ GIL, Julio, "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal", en *Justicia: ¿Garantías versus eficiencia?*, (Dir. JIMÉNEZ CONDE y BELLIDO PENADÉS), Tirant lo Blanch, 2019, pág. 423.

109 Véase el trabajo de CASTILLEJO MANZANARES, Raquel, "Alguna de las cuestiones que plantean las diligencias de investigación tecnológica", en *Revista Aranzadi de Derecho y Proceso Penal*, número 45, enero-marzo 2017.

En este sentido, en el Artículo 588 bis a de la LECRim se establecen los Principios rectores y se establece que:

"*1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.*

2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.

4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:

a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o

b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

Sin entrar en profundidad a analizar estos principios quisiera apuntar brevemente su significado[110].

a) En relación con el principio de especialidad, este principio implica que las medidas de investigación tecnológica sólo podrán adoptarse para la investigación de un concreto delito sin posibilidad de llevar a cabo investigaciones prospectivas. Este principio conllevaría:

a. la exclusividad jurisdiccional

b. concreción de las medidas

c. resolución judicial

110 Véase al respecto a AÑÓN CALVETE, JUAN, *Diligencias de Investigación Tecnológica y Derechos Fundamentales*, 2015, Tirant on line, DOCUMENTO TOL5.429.306.

d. existencia de indicios objetivos y suficientes
e. temporalidad de la medida
f. control judicial.

Por tanto, la motivación para llevar a cabo esta clase de diligencias de investigación tecnológicas limitadoras de derechos fundamentales del artículo 18 de la CE no puede estar dirigida a la prevención, el descubrimiento de delitos o las simples sospechas sin una base objetiva, por más que la primera y la segunda de esas actividades sí puedan ser llevadas a cabo por los Cuerpos y Fuerzas del Estado en cumplimiento de sus funciones, como sabemos en espacios públicos y entorno virtuales de acceso libre[111].

b) Por otro lado, el principio de excepcionalidad supone la elección de esas medidas cuando no existan otras menos graves tanto para los derechos fundamentales de las personas investigadas como o para el descubrimiento o la comprobación del hecho investigado, la determinación de su autor, la averiguación de su paradero, o la localización de los efectos del delito. Es decir, el logro de estas finalidades se vería impedida sin el recurso a esta medida.

c) En relación con el principio de necesidad, la valoración que debe efectuar el órgano judicial en relación con la práctica de unas pruebas que, por sus características, suponen invasión en derechos fundamentales tales como la intimidad y la libertad informática, las cuales, a falta de cobertura legal y del debido cumplimiento de las garantías que han de presidir su ejecución, deben ser sustituidas por otras alternativas[112].

d) El principio de idoneidad, sirve para definir el ámbito objetivo, subjetivo y la duración de la medida en virtud de su utilidad.

e) Y, finalmente, el principio de proporcionalidad que implica una ponderación de los intereses en juego teniendo en cuenta que pueden verse afecta-

111 Véase a SANCHIS CRESPO, Carolina (con VELASCO, Eloy), *Delincuencia informática…*, op. Cit., pág. 274.

112 Véase la STSJ 1450/2006, de 12 de septiembre, de la Sala de lo Social del País Vasco. En los hechos que se enjuician se trataba de la intervención de ordenador y pericial informática, que se consideraron nulas. En esta circunstancia, el Tribunal Superior de Justicia del País Vasco consideró que atendiendo a la doctrina fijada por el Tribunal Constitucional en relación con los requisitos necesarios para validar tales pruebas que los mismos no se daban ya que podían adoptarse medidas alternativas a las adoptadas puesto que fue posible solicitar el consentimiento del actor desde un primer momento y en caso de negarse, haber instado la autorización judicial correspondiente.

dos derechos fundamentales[113]. En la ponderación de los intereses en juego habrá que considerar la gravedad del hecho, su transcendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho[114].

En este sentido, la regulación que se contiene en la Ley de Enjuiciamiento Criminal, tras la reforma llevada a cabo por la Ley Orgánica 13/2015, de 5 de octubre, responde plenamente a los *principios* y requisitos que venían exigiéndose por vía jurisprudencial dado el vacío legal.

Los artículos 588 bis a a 588 bis k de la Ley de Enjuiciamiento Criminal regulan con vocación de generalidad para todas las diligencias de investigación tecnológicas que afectan a los derechos a la intimidad, al secreto de las comunicaciones y al secreto informático, amparados en el artículo 18.1, 3 y 4 de la Constitución Española, las "Disposiciones comunes".

Así, en el primero de los artículos mencionados de la Ley de Enjuiciamiento Criminal, art. 588 bis a, se establece, por un lado, la necesidad de que cualquier medida de investigación tecnológica por limitar los derechos fundamentales del sujeto sea autorizada por el juez y por otro, en atención al principio de especialidad que la medida se dirija al esclarecimiento de un hecho punible concreto. Además de estos principios se deben satisfacer también los *principios* de *idoneidad,* excepcionalidad, necesidad y proporcionalidad[115].

Por tanto, la solicitud destinada a la práctica de dichas medidas, de acuerdo al artículo 588 bis b de la Ley de Enjuiciamiento Criminal, debe contener lo siguiente:

"1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.

3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.

---

113 Véase a GONZÁLEZ-CUELLAR SERRANO, Nicolás, *Proporcionalidad y derechos fundamentales en el proceso penal*, Ed. Colex, Madrid, 1990.

114 Véase a SANCHIS CRESPO, Carolina (con VELASCO, Eloy), *Delincuencia informática*..., op. cit., pág. 281.

115 STS de 12 de febrero de 2019, número 77/2019, ECLI: ES:TS:2019:473, en Tirant on line, TOL7.065.911.

4.º La extensión de la medida con especificación de su contenido.
5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.
6.º La forma de ejecución de la medida.
7.º La duración de la medida que se solicita.
8.º El sujeto obligado que llevará a cabo la medida, en caso de conocerse".

Por su parte, el Juez, según el artículo 588 bis c de la Ley de Enjuiciamiento Criminal, en un auto motivado y previa audiencia del Fiscal detallará de forma minuciosa:

"a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.
b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.
c) La extensión de la medida de injerencia, especificando su alcance, así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.
d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.
e) La duración de la medida.
f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.
g) La finalidad perseguida con la medida.
h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia".

En relación con la sustanciación de las medidas, se exige su tramitación en una pieza separada y secreta (artículo 588 bis d de la Ley de Enjuiciamiento Criminal).

Además de estos requisitos comunes a todas las medidas de investigación, en relación a las diligencias de investigación de interceptación de las comunicaciones telefónicas y telemáticas reguladas en los artículos 588 ter a a 588 ter i de la Ley de Enjuiciamiento Criminal, se añaden otros requisitos complementarios a los anteriores, en concreto, indica el Tribunal Supremo en la STS 77/2019, 12 de febrero de 2019[116], los siguientes:

1º) La concreción de los concretos delitos para los cuales se pueden acordar dichas medidas, como: a) los delitos dolosos con pena con límite máximo de, al menos, tres años de prisión; b) los delitos cometidos en el seno de un

116 https://vlex.es/vid/769623469.

grupo u organización criminal; c) los delitos de terrorismo; y d) los delitos cometidos por medio de instrumentos informáticos o de cualquier otra *tecnología* de la información o la telecomunicación (artículo 588 ter a de la Ley de Enjuiciamiento Criminal).

2°) La intervención acordada judicialmente podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación (artículo 588 ter b de la Ley de Enjuiciamiento Criminal).

3°) La solicitud de autorización judicial debe reunir, además de los requisitos del artículo 588 bis b de la Ley de Enjuiciamiento Criminal, los siguientes contenidos en el artículo 588 ter d de la Ley de Enjuiciamiento Criminal: i) el número; ii) la conexión; o iii) los datos para la identificación del medio de telecomunicación. Y atendiendo al mismo precepto, la solicitud deberá precisar el alcance de la injerencia que pretende, que podrá ser: i) el contenido de la comunicación; ii) su origen o destino; iii) localización geográfica; y iv) otros datos de tráfico.

4°) Por lo que respecta a la Policía Judicial, ésta aportará al juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes de interés y las grabaciones íntegras (artículo 588 ter f de la Ley de Enjuiciamiento Criminal).

5°) La duración de la medida será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses (artículo 588 ter o de la Ley de Enjuiciamiento Criminal).

En relación con la motivación, conforme se indica en la sentencia del Tribunal Supremo núm. 413/2015, de 30 de junio[117], la motivación por remisión no es una técnica jurisdiccional modélica, pues la autorización judicial debería ser autosuficiente (STS núm. 636/2012, de 13 de julio). Sin embargo, la doctrina constitucional admite que la resolución judicial pueda considerarse suficientemente motivada si, integrada con la solicitud policial, a la que se remite o con el informe o dictamen del Ministerio Fiscal en el que solicita la intervención (STS núm. 248/2012, de 12 de abril), contiene todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad (STC 72/2010, de 18 de octubre). Es evidente, que en la mayoría de las ocasiones resulta redundante que el Juzgado se dedique a copiar y reproducir literalmente la totalidad de lo narrado extensamente en el oficio o dictamen policial que

117 En Tirant on line, TOL5.211.585, ECLI: ES:TS:2015:3177.

obra unido a las mismas actuaciones, siendo más coherente que extraiga del mismo los indicios especialmente relevantes (STS núm. 722/2012, de 2 de octubre)[118].

El Tribunal Supremo en sentencia núm. 86/2018, de 19 de febrero[119], que a su vez recoge los criterios sentados en las sentencias de esta misma Sala núm. 426/2016, de 19 de mayo, 373/2017, de 24 mayo, 720/2007, de 6 noviembre, y 2/2018, de 9 enero, especifica que "en la motivación de los autos de intervención de las comunicaciones deben ser superadas las meras hipótesis subjetivas o la simple plasmación de la suposición o, incluso, de la convicción de la existencia de un delito o de la intervención en él de una determinada persona, pues de considerar suficiente tal forma de proceder, resultaría que la invasión de la esfera de intimidad protegida por un derecho fundamental vendría a depender, en la práctica, exclusivamente de la voluntad del investigador, sin exigencia de justificación objetiva de ninguna clase, lo que no es admisible en un sistema de derechos y libertades efectivos, amparados en un razonable control sobre el ejercicio de los poderes públicos"[120].

Por tanto, para apreciar los indicios como fundamento para acordar una intervención telefónica u otra cualquier medida de investigación tienen que ser considerados como verdaderos datos objetivos y no meras sospechas. Estos datos por su naturaleza deben ser susceptibles de verificación posterior con la finalidad, como reiteradamente establece el Tribunal Supremo, de que "*permitan concebir sospechas que puedan considerarse razonablemente fundadas acerca de la existencia misma del hecho que se pretende investigar y de la relación que tiene con él la persona que va a resultar directamente afectada por la medida*[121]".

Señala la jurisprudencia de forma reiterada que "*han de ser objetivos en un doble sentido. En primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control. Y, en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o se va a cometer el delito sin que puedan consistir en valoraciones acerca de la persona*"[122].

---

118 STS 159/2020, 18 de mayo de 2020, en https://vlex.es/vid/845816996.

119 En Tirant on line, TOL6.525.968, ECLI: ES:TS:2018:569.

120 Sentencias del Tribunal Supremo núm. 1363/2011, de 15 de diciembre y núm. 635/2021, de 17 de julio, citadas por la sentencia núm. 86/2018, de 19 de febrero.

121 STS 635/2012, de 17 de julio. En https://vlex.es/vid/-395385858.

122 STC 184/2003, de 23 de octubre.

Por lo que respecta a su contenido, ha de ser de tal naturaleza que "*permitan suponer que alguien intenta cometer, está cometiendo o ha cometido una infracción grave o en buenas razones o fuertes presunciones de que las infracciones están a punto de cometerse" (Sentencias del Tribunal Europeo de Derechos Humanos de 6 de septiembre de 1978, caso Klass , y de 15 de junio de 1992, caso Ludí) o, en los términos en los que se expresa el actual artículo 579 de la Ley de Enjuiciamiento Criminal), en "indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa" (artículo 579.1 de la Ley de Enjuiciamiento Criminal) o "indicios de responsabilidad criminal" (artículo 579.3 de la Ley de Enjuiciamiento Criminal*"[123].

En definitiva, la jurisprudencia manifiesta que el control que se debe efectuar sobre la decisión del juez a la hora de acordar la medida para ver si esta era necesaria y por tanto estaba justificada es que tuviese a su alcance datos objetivos sobre la existencia del delito y la participación del sospechoso como la utilidad de la intervención telefónica. Juez debe controlar una vez que la medida ha sido acordada que este tenía a su alcance datos objetivos sobre la existencia del delito y de la participación del sospechoso[124].

Además, como reitera la jurisprudencia, la ilegitimidad constitucional de la primera intervención contamina a las prórrogas y a las posteriores intervenciones acordadas sobre la base de datos obtenidos en la primera[125]. Hay

123 STC 167/2002, de 18 de septiembre.

124 STS núm. 635/2012, de 17 de julio. ECLI: ES: TS: 2012: 5606, Id Cendoj: 28079120012012100670.

125 STS 77/2019, 12 de Febrero de 2019, en https://vlex.es/vid/769623469, donde el Tribunal Supremo indica que: "*Bien entendido -como se indica en las SSTS 645/2010 de 14 de mayo y 413/2015 de 30 de junio ,- que la intervención de un nuevo teléfono del mismo titular o la prórroga temporal de una intervención telefónica que inicialmente ha sido autorizada por concurrir motivos justificados, solo tiene de específico la prolongación en el tiempo de esa intervención ya ordenada legítimamente, lo que es necesario entonces justificar y lo que se exige en tal caso es motivar en la nueva resolución decisoria que no se extiende a lo que se justificó, ponderó y valoró en el auto originario habilitante, sino la ampliación temporal de lo mismo más allá del periodo inicialmente concedido cuando lo que apoya la nueva intervención o prórroga no es propiamente un cúmulo de indicios nuevos o diferentes de los que fueron expresados y valorados en la intervención, sino estrictamente la subsistencia de aquéllos, es decir el mantenimiento, la mera vigencia en el tiempo de la misma necesidad. Si la una y otra en cuanto tales ya se sometieron al control judicial no es preciso ponderar de forma redundante lo ya ponderado antes y será únicamente objeto del control la justificación de la prórroga en lo que supone*

que ser verdaderamente escrupulosos con la práctica ajustada a derecho de la primera intervención telefónica puesto que aunque ofrezca datos objetivos indicativos de la existencia de un delito grave, sin embargo, contamina irremediablemente las posteriores prórrogas que se deriven de ella (SSTC 171/99 del 27 septiembre, 299/2000 de 11 diciembre, 184/2003 del 23 octubre, 165/2005 de 20 junio, 253/2006 de 11 septiembre)[126].

El Tribunal Supremo ha establecido reiteradamente[127], que "en los autos en los que se restringen derechos fundamentales, el tipo de juicio requerido cuando aparece cuestionada por vía de recurso la existencia de los presupuestos habilitantes de la medida limitativa y la corrección jurídica de su autorización ha de operar con rigor intelectual con una perspectiva ex ante, o lo que es lo mismo, prescindiendo metódicamente del resultado realmente obtenido como consecuencia de la actuación policial en cuyo contexto se inscribe la medida cuestionada. Porque este resultado, sin duda persuasivo en una aproximación extrajurídica e ingenua, no es el metro con el que se ha de medir la adecuación normativa de la injerencia. De otro modo, lo que coloquialmente se designa como éxito policial sería el único y máximo exponente de la regularidad de toda clase de intervenciones; cuando, es obvio, que tal regularidad depende exclusivamente de que éstas se ajusten con fidelidad a la Constitución y a la legalidad que la desarrolla. Lo contrario, es decir, la justificación ex post, sólo por el resultado, de cualquier medio o forma de actuación policial o judicial, equivaldría a la pura y simple derogación del artículo 11.1 de la Ley Orgánica del Poder Judicial e, incluso, de una parte, si no todo, del artículo 24 de la Constitución Española (STS 926/2007, de 13 de noviembre)"[128]. Continua el Tribunal Supremo manifestando que "esa obligada disociación del resultado finalmente obtenido de sus antecedentes para analizar la adecuación de éstos, considerados en sí mismos, al paradigma constitucional y legal de pertinencia en razón de la necesidad justificada, es, precisamente lo que tiñe de dificultad la actividad de control jurisdiccional y, con frecuencia, hace difícil también la acepta-

---

de concesión de un nuevo período temporal para una intervención ya justificada STS 1008/2013 de 8 de enero de 2014".

126 STS 77/2019, 12 de Febrero de 2019, en https://vlex.es/vid/769623469.

127 STS 974/2012, de 5 diciembre en Tirant on line, TOL2.721.470, DOCUMENTO TOL2.721.470; STS 83/2013, de 13 febrero, en Tirant on line, TOL3.054.768, DOCUMENTO TOL3.054.768; STS 877/2014, de 22 diciembre, en Tirant on line, TOL4.609.985, DOCUMENTO TOL4.609.985.

128 STS 77/2019, 12 de febrero de 2019, en https://vlex.es/vid/769623469.

ción pública de eventuales declaraciones de nulidad. Por ello, el auto inicial de la intervención telefónica debe valorarse a la vista de los elementos y datos disponibles en el momento de su adopción, sin que la insuficiencia de los resultados obtenidos o la existencia posterior de otras pruebas, que desvirtúen su contenido incriminador o incluso su misma relevancia jurídica, afecten a la legitimidad inicial de la medida restrictiva del derecho fundamental"[129].

Como vemos, toda esta doctrina jurisprudencial en relación con los principios y requisitos necesarios para acordar medidas restrictivas de derechos fundamentales ha sido recogida expresamente por nuestro legislador en la Ley de Enjuiciamiento Criminal dando cobertura legal donde hasta ahora existía un vacío normativo.

e. La licitud de la prueba electrónica

La obtención y análisis de evidencias electrónicas en el ámbito del proceso está sujeta a un tratamiento, procesal y técnico muy riguroso[130], que en el caso de no cumplimentarse[131], podrá dar lugar a la discusión del resultado probatorio que, en función del tipo de vulneración producida, nos encontraremos ante meras irregularidades subsanables, o bien, ante la nulidad en supuestos de que se hayan violado derechos fundamentales.

De esta forma, la prueba obtenida de forma ilícita, es decir, vulnerando derechos fundamentales es prueba nula de pleno derecho y, por tanto, no puede ser utilizada contra ninguna persona dentro del proceso. Su desarrollo legal está contemplado en el artículo 11.1 de la Ley Orgánica del Poder Judicial donde se indica que lo obtenido de forma directa o indirecta violando derechos fundamentales es nulo de pleno derecho. En un sentido amplio, la doctrina entiende que la prueba es ilícita tanto si se produce una vulneración directa de una norma o principio constitucional como si se trata de una irregularidad que causa una indefensión efectiva, puesto

129 STS de 12 de febrero de 2019, citada anteriormente.

130 Véase el trabajo de SANZ-GADEA GÓMEZ, Juan Bautista, *Los informes periciales informáticos en el ámbito*..., op. cit.

131 El forense informático debe documentar el proceso realizado en todas sus fases y con todos los pasos realizados, las herramientas utilizadas (versiones, licencias, etc.), incluido los resultados obtenidos del análisis de los datos, de tal manera que puede confrontarse por terceras personas la validez del proceso de análisis. SANZ-GADEA GÓMEZ, Juan Bautista, *Los informes periciales informáticos*..., op. cit.

que el proceso no puede llegar a su fin a costa del derecho de defensa de las partes[132].

e.1 La ilicitud probatoria basada en la vulneración del derecho al secreto de las comunicaciones y del derecho a la intimidad

Una vez considerada que la prueba es pertinente, necesaria y útil, la misma ha debido de obtenerse de forma lícita, es decir, sin vulnerar ningún derecho fundamental ya que, de otra forma, como hemos visto, sería declarada nula. Por tanto, la incorporación de los hechos en el proceso debe hacerse con un escrupuloso respeto a los derechos fundamentales y a las normas y garantías procesales.

En concreto, la ilicitud probatoria puede venir por la vulneración de los derechos contemplados en los artículos 18.1 y 18.3 de la Constitución. En relación con el derecho al secreto de las comunicaciones la norma constitucional protege la impenetrabilidad de los terceros en la comunicación puesto que esta es secreta. El concepto de secreto, por consiguiente, abarcaría tanto el contenido de la comunicación como también la identidad subjetiva de los interlocutores. El Tribunal Constitucional ha señalado a este respecto que "*el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas*"[133].

Por tanto, este derecho garantiza la comunicación en sí, la cual no puede ser observada o escuchada por terceros ajenos, por tanto, cuando la comunicación es desvelada por alguno de los interlocutores, o alguno de ellos permite que sea observada o escuchada no opera el derecho al secreto de las comunicaciones sino más bien el derecho a la intimidad personal cuando lo comunicado incide en el ámbito de la vida privada. En el artículo 18.1 de la Constitución se establece un "deber de reserva" atendiendo al contenido mismo de la comunicación, puesto que se vería vulnerado el derecho a la intimi-

132 Véase a DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba*..., op. cit., págs. 40-43.

133 STC 114/1984. Como se indica en la STC 123/2002, este Tribunal recogiendo la doctrina emanada del TEDH en la sentencia de 2 de Agosto de 1984, caso Malone, ha afirmado que el concepto de secreto de la comunicación cubre, no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores.

dad cuando se invade la esfera íntima del interlocutor. Es necesario proteger este espacio de intimidad personal y familiar de las personas dado el creciente y vertiginoso desarrollo de los medios tecnológicos.

Si bien, el derecho a la intimidad se puede considerar desde dos vertientes diferentes, aunque las dos integran el contenido de dicho derecho. Por un lado, una vertiente positiva, donde el acento se pone en el acervo de las facultades de su titular, y por otro lado, la vertiente negativa, donde el acento se pone en las facultades de exclusión de su titular. En este sentido, el sujeto puede decidir desde la vertiente negativa que determinadas informaciones o datos que forman parte del núcleo básico de la personalidad sean excluidos del conocimiento de terceros ajenos[134]. La vertiente positiva del derecho en su dimensión informativa, también conocida como autodeterminación informativa, cobijada bajo el art. 18.4 de la CE. Esta vertiente positiva o activa concede al titular del derecho un poder de decidir que quiere y que no quiere compartir, es decir, le otorga un auténtico y ejercitable poder de control de los datos e informaciones que le atañen[135].

El Tribunal Constitucional ha venido manifestando, ya desde su STC 110/1984, de 26 de noviembre, que *"la inviolabilidad del domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida" (FJ 3). En el mismo sentido, en la STC 119/2001, de 24 de mayo, afirmábamos que "estos derechos han adquirido también una dimensión positiva*

134 Véase a LÓPEZ ORTEGA, Juan José, y ALCOCEBA GIL, Juan. Manuel, "De la intimidad territorial a la informativa: la defensa de la intimidad a través de sus manifestaciones constitucionales", en *Foro. Revista de Ciencias Jurídicas y Sociale*s, Nueva Época, Universidad Complutense de Madrid, vol. 22, núm. 1 (2019), págs. 94-95, en https://dx.doi.org/10.5209/foro.66635.

135 PÉREZ CONCHILLO, Eloísa, *Intimidad y difusión de sexting no consentida*, op. cit., pág. 33.

en relación con el libre desarrollo de la personalidad, orientada a la plena efectividad de estos derechos fundamentales. En efecto, habida cuenta de que nuestro texto constitucional no consagra derechos meramente teóricos o ilusorios, sino reales y efectivos ..., se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada. A esta nueva realidad ha sido sensible la jurisprudencia del Tribunal Europeo de Derechos Humanos, como se refleja en las Sentencias de 21 de febrero de 1990, caso Powell y Rayner contra Reino Unido; de 9 de diciembre de 1994, caso López Ostra contra Reino de España, y de 19 de febrero de 1998, caso Guerra y otros contra Italia" (FJ 5)"[136].

También el Tribunal Supremo, en la Sentencia 97/2015, de 24 febrero de 2015, Rec. 1774/2014[137] ha señalado que:

"En STC. 142/2012 de 2 de junio*, se precisa que debe delimitarse es si el acceso a los datos del ordenador es un acto con solo incidencia en el derecho a la intimidad (*art. 18.1 CE*) o alcanza también al derecho al secreto de las comunicaciones (*art. 18.3 CE*), lo que, en última instancia, tiene relevancia por el diferente régimen constitucional de protección de ambos derechos. A esos efectos, cabe recordar que este Tribunal ha señalado que si bien, de conformidad con el* art. 18.3 CE*, la intervención de las comunicaciones requiere siempre resolución judicial, no existe en el* art. 18.1 CE *esa misma garantía de previa resolución judicial respecto del derecho a la intimidad personal, de modo que excepcionalmente se ha admitido la legitimidad constitucional de que en determinados casos y con la suficiente y precisa habilitación legal la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas,* STC 281/2006, de 9 de octubre*, FJ 9).*

El Tribunal Constitucional analizando si los datos contenidos en un ordenador pueden afectar a la intimidad o no de una persona ha indicado que: "*Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su*

136 STC 173/2011, sentencia citada.

137 En Tirant on line, DOCUMENTO TOL4.776.958. ECLI:ES:TS: 2015: 823.

titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información"[138].

Debido a la ingente cantidad de datos personales que los usuarios publican en sus perfiles, éstos se convierten en auténticas "identidades digitales" o "huellas digitales" que facilitan un rápido conocimiento de datos de contacto, preferencias y hábitos del usuario[139].

Se indica en la Sentencia del Tribunal Supremo, de 14 de octubre de 2019,

138 STC 173/2011, citada anteriormente.

139 Véase *Estudio sobre la privacidad de los datos y la seguridad de la información…*, op. cit., pág. 82.

que: "*Las especiales características del instrumento técnico sobre el que se asentó la investigación judicial (smartphone) que, por un lado, permite la comunicación telemática en sus distintas modalidades de conversación oral o escrita y, aun en esta, por distintos instrumentos como son los mensajes electrónicos por emails, o la mensajería instantánea sms (short message service, por sus siglas en inglés), o a través de plataformas de comunicación específicas como WhatsApp o telegram, y que por otro lado realiza un registro de todos los datos referidos a estas conversaciones, además de otras circunstancias que dependen de la configuración personal del usuario, tales como fotografías, vídeos, historial de geolocalización, navegación por internet, o el rastro de las distintas iniciativas que haya impulsado el usuario durante la utilización de las distintas utilidades o aplicaciones informáticas que tenga instaladas, justifica principiar por la aclaración, ya reiterada en numerosas sentencia de esta Sala, que distingue entre las comunicaciones en marcha, de aquellos otros procesos de correspondencia o de relación que ya están cerrados. Solo las primeras se encuentran afectadas por el derecho al secreto de las comunicaciones, mientras que aquellas que terminaron y cuya existencia presente deriva de un proceso técnico o electrónico de conservación o documentación, a lo que conciernen es al derecho a la intimidad y/o, en su caso, a la autodeterminación informativa mediante el control de datos personales. Así lo recoge reiterada jurisprudencia de esta Sala (SSTS 1235/2002, de 27 de junio; 1647/2002, de 1 de octubre; 528/2014; 864/2015, de 10 de diciembre o 849/2018, de 23 de octubre), y lo plasma una estable doctrina constitucional que, entre otras en su sentencia 70/2002, de 3 de abril, expresaba que: "... La protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos*"[140].

Tal es el avance de las nuevas tecnologías que se ha llegado incluso a crear una aplicación que puede leer los mensajes borrados en Whatsapp. Ello es verdaderamente peligroso por la incidencia que pueden tener en la privacidad de las personas. Esta posibilidad depende de si se eres un usuario de un Iphone u otro Android; en los primeros la única posibilidad es utilizando la copia de seguridad de WhatsApp, sin embargo con los usuarios de Android aumentan las posibilidades gracias a unas aplicaciones que recuperan los

140 ECLI: ES:TS:2019:3123 en Tirant on line, TOL7.531.381.

mensajes de las notificaciones, por lo que si se tiene el chat abierto no se puede recuperar. Para ello, las aplicaciones más usadas son dos: la Whats-Removed+ y la WAMR, las cuales se encuentran en Play Store y tienen un funcionamiento muy similar, registran el texto de las notificaciones recibidas en los móviles. Todas las notificaciones que son enviadas al WhatsApp son guardadas por dichas aplicaciones.

Es evidente que el uso inadecuado de todo este tipo de aplicaciones puede conllevar un doble riesgo: por un lado, puede vulnerar o transgredir la privacidad de la persona que borró o eliminó el mensaje y, además, puede ser incluso más peligroso al poder acceder a datos personales, contactos e información contenida en el teléfono. Eso sí, ninguna de estas dos aplicaciones podrá recuperar los mensajes borrados antes de su instalación.

e.2 La ilicitud probatoria basada en la vulneración del derecho fundamental a la protección de datos

Un aspecto importante a tratar es la ilicitud probatoria basada en la vulneración del derecho fundamental a la protección de datos, por tanto, ilicitud probatoria por vulnerar el artículo 18.4 de la Constitución. Aunque este derecho fundamental a la protección de datos generalmente se utiliza como apoyo de otros derechos fundamentales, especialmente el derecho a la intimidad, sin embargo, puede tener carácter autónomo sin tener que estar integrado dentro de ningún otro derecho fundamental y, en concreto, dentro del derecho a la intimidad contemplado en el párrafo tercero del mismo artículo 18 de la Constitución.

A este respecto mencionaba en otro epígrafe que la regulación de las diligencias de investigación tecnológica aumenta la sensación de seguridad jurídica a la hora de poder incorporar la prueba electrónica en el proceso penal, sin embargo, suponen un mayor riesgo en la lesividad de los derechos fundamentales de las personas investigadas y fundamentalmente en el derecho a la protección de datos personales. Ahora bien, si se analizan las sentencias que tratan la ilicitud de la prueba obtenida vulnerando derechos fundamentales, se incide en el riesgo de vulnerarse el derecho al "propio entorno virtual", y no tanto al derecho a la protección de datos de carácter personal ni tampoco a los otros derechos afectados.

e.3 El principio de no indagación como excusa para admitir la prueba ilícita

En la práctica, muchas veces se necesita obtener información o fuentes de prueba que no están en nuestro territorio nacional o al revés, otro Estado necesita que el nuestro le preste la ayuda requerida con miras a que la investigación pueda avanzar. Ello se lleva a cabo a través de la cooperación judicial internacional y hay que tener en cuenta que en esta cooperación entre Estados en algunas ocasiones para obtener esta información transfronteriza necesaria para el proceso penal se realizan actuaciones restrictivas de derechos fundamentales. En este sentido, lo verdaderamente relevante no es el mecanismo que se utilice para prestar la ayuda requerida, aunque también, sino cuáles son los requisitos que han de darse para que el resultado de esas investigaciones pueda tener eficacia probatoria, es decir, que puedan utilizarse válidamente como prueba para fundamentar legítimamente una condena penal[141]. Así, cuando un juez español *solicita la asistencia de las autoridades de otro Estado en la investigación necesaria para la obtención de pruebas penales, lo que de verdad importa es que* sepa cuáles son las garantías realmente esenciales según el sistema español, que supeditan la eficacia posterior de las pruebas, fundamentalmente esos mínimos que necesariamente han de haberse respetado en el extranjero para que el resultado de la investigación sirva posteriormente como prueba en España[142]. Sin embargo, esta premisa por lo menos hasta hace muy poco se ha revelado incorrecta, puesto que nuestro Tribunal Supremo considera que todo vale si se respeta la *lex loci*, y no la *lex fori*, es decir, las pruebas que han sido el resultado de investigaciones transfronterizas serán válidas y eficaces en los procesos penales españoles si las actuaciones que se han desarrollado en el extranjero se han efectuado de conformidad con la legislación vigente en su lugar de práctica. Es lo que se denomina principio de no indagación, que significa la admisibilidad de la prueba llevada a cabo en el extranjero sin necesidad de analizar previamente el contenido de la actividad procesal desarrollada en el extranjero. Supone un reconocimiento del valor primordial de la *lex loci*[143].

---

141 GASCÓN INCHAUSTI, Fernando, *Orden Europea de Investigación y Prueba Transfronteriza en la Unión Europea*, (coord. GONZÁLEZ CANO, María Isabel), Tirant lo Blanch, 2019, en Tirant on line, DOCUMENTO TOL7.558.495.

142 Ibídem.

143 Ibídem.

En el ámbito de la Unión Europea se ha avanzado considerablemente pues, partiendo del principio de reconocimiento mutuo[144], se han ido promulgando instrumentos jurídicos cuyo fin es el de garantizar que se puedan solicitar y obtener de forma más rápida las evidencias del delito, incluso de naturaleza electrónica. Estos instrumentos jurídicos tienen como finalidad última la de aproximar las legislaciones nacionales para adaptarlas a los nuevos retos que plantea esta nueva era digital. En este contexto es donde se enmarca la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes de entrega y conservación de pruebas electrónicas que nacen como instrumentos adicionales completando la orden de investigación europea en materia de prueba electrónica[145]. Es evidente que el principio de reconocimiento mutuo tiene su fundamento en la confianza mutua entre los Estados y ello es posible si existe una mínima armonización de los derechos y garantías procesales. La efectividad del principio de no indagación tendrá lugar cuando los Estados tengan la confianza de que entre los Estados miembros se respetan los derechos y garantías procesales esenciales. A ello, evidentemente tienden todos estos instrumentos.

La jurisprudencia ha indicado que*: "Cuando se trata de fijar los límites de la licitud probatoria y de definir las reglas de exclusión, no puede operarse con soluciones miméticas, la doctrina sobre la prueba obtenida con vulneración de derechos fundamentales no responde a una fotografía estática, antes al contrario, ha experimentado una más que apreciable evolución desde su formulación inicial por la jurisprudencia del Tribunal Constitucional español.*

Esta doctrina, con enunciado normativo propio en el art. 11 de la LOPJ ("…no surtirán efectos las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales") aconseja huir de interpretaciones rígidas, sujetas a reglas estereotipadas que impidan la indis-

144 El principio de reconocimiento mutuo fue reconocido en el Consejo Europeo de Tampere como la "piedra angular" de la cooperación judicial civil y penal en la Unión Europea, basada en la confianza mutua entre los Estados miembros. Este principio supuso una verdadera transformación en el ámbito de la cooperación entre los Estados miembros puesto que implica que una resolución emitida por una autoridad judicial de un Estado miembro sea reconocida casi automáticamente por otro Estado miembro, a excepción de los supuestos en los que se den alguno de los motivos de denegación del reconocimiento.

145 Véase mi trabajo, "El nuevo marco jurídico transfronterizo de las pruebas electrónicas. Las órdenes de entrega y conservación de las pruebas electrónicas", en *Revista General de Derecho Europeo*, noviembre, número 49, 2019.

pensable adaptación al caso concreto. Y esa rigidez despliega similar efecto pernicioso, tanto cuando se erige en injustificada regla de exclusión, como cuando se convierte en una tolerante fórmula para incorporar al arsenal probatorio lo que debió haber sido excluido"[146].

Hace referencia la sentencia citada al principio de no indagación para matizarlo, y así se manifiesta que: *"Es cierto que algunos precedentes de esta Sala sugieren su vigencia. Así en la STS 456/2013, 9 de junio, recordábamos que "... la pretensión de que los Tribunales españoles se conviertan en custodios de la legalidad de actuaciones efectuadas en otro país de la Unión Europea deviene inaceptable. Existe al respecto ya una consolidada doctrina de esta Sala que en general, y más en concreto, en relación a los países que integran la Unión Europea, tiene declarado que no procede tal facultad de "supervisión"". Y en la STS 1521/2002 de 25 de Septiembre, apuntábamos que "…. en el marco de la Unión Europea, definido como un espacio de libertad, seguridad y justicia, en el que la acción común entre los Estados miembros en el ámbito de la cooperación policial y judicial en materia penal es pieza esencial (…), no cabe efectuar controles sobre el valor de los realizados ante las autoridades judiciales de los diversos países de la Unión, ni menos de su adecuación a la legislación española cuando aquellos se hayan efectuado en el marco de una Comisión Rogatoria y por tanto de acuerdo con el art. 3 del Convenio Europeo de Asistencia Judicial en materia Penal". En la misma línea, la STS 340/2000, 3 de Marzo, precisaba que "…la incorporación a causa penal tramitada en España de pruebas practicadas en el extranjero en el marco del Convenio Europeo de Asistencia Judicial (…) no implica que dichas pruebas deban ser sometidas al tamiz de su conformidad con las normas españolas"; mientras que la STS 947/2001 , 18 de Mayo, concluía que "….no le corresponde a la autoridad judicial española verificar la cadena de legalidad por los funcionarios de los países indicados, y en concreto el cumplimiento por las autoridades holandesas de la legalidad de aquel país ni menos sometidos al contraste de la legislación española…". Esa no indagación por las autoridades jurisdiccionales españolas del grado de cumplimiento en otro Estado de las garantías propias de nuestro sistema, está también presente en la STS 556/2006, 31 de mayo. En el apartado 2º de su FJ 7º puede leerse lo siguiente: "…la posible existencia de irregularidades en la detención y ejecución de la misma en el extranjero no tendría consecuen-*

146 Sentencia de la Audiencia Provincial de las Palmas de 5 de noviembre de 2018, en Tirant on line, DOCUMENTO TOL 7.067.587.

cias respecto de la validez de las actuaciones policiales y procesales desarrolladas en España, pues el control de legalidad constitucional y ordinaria que efectúa este Tribunal ha de referirse a la actuación de las autoridades españolas dentro del marco del proceso penal, en sentido amplio, seguido en nuestro país. Y ello no supone la aplicación del principio "male captus bene detentus", según el cual, cuando la detención está acordada en legal forma, las irregularidades en la ejecución de la misma no constituyen una excepción procesal que pueda afectar a la validez del proceso en su conjunto.

Pues, aunque de alguna forma se alegue, no se ha acreditado ninguna infracción cometida en el apresamiento del recurrente. Y por otra parte, como se ha dicho, esta regla no exige una excepción cuando la infracción no ha sido cometida por las autoridades españolas".

Sin embargo, el principio de no indagación no puede convertirse en la pieza maestra con la que resolver las dudas de ilicitud cuando los documentos bancarios ofrecidos por las autoridades policiales de un Estado extranjero han podido obtenerse con vulneración de algún derecho fundamental. De entrada, porque las citas jurisprudenciales a que hemos hecho referencia tienen en común el venir referidas a sentencias dictadas cuando la queja sobre su validez constitucional se produce en el marco de un acto de cooperación jurídica internacional y lo que se cuestiona es la falta de semejanza entre los requisitos que en uno y otro sistema disciplinan la práctica de ese acto probatorio. Es lógico que la validez en el proceso penal español de actos procesales practicados en el extranjero no se condicione al grado de similitud entre las reglas formales que, en uno y otro Estado, singularizan la práctica de esa prueba. Al juez español no le incumbe verificar un previo proceso de validación de la prueba practicada conforme a normas procesales extranjeras. Pero la histórica vigencia del principio locus regit actum, de dimensión conceptual renovada a raíz de la consolidación de un patrimonio jurídico europeo, no puede convertirse en un trasnochado adagio al servicio de la indiferencia de los órganos judiciales españoles frente a flagrantes vulneraciones de derechos fundamentales. Incluso en el plano semántico la expresión principio de no indagación, si se interpreta desbordando el ámbito exclusivamente formal que le es propio, resulta incompatible con algunos de los valores constitucionales comprometidos en el ejercicio de la función jurisdiccional.

Esta idea tampoco es ajena a la jurisprudencia de esta Sala. De hecho, en la STS 829/2006, 20 de julio, en una causa incoada por delito de terrorismo,

negábamos validez a la valoración de una "entrevista policial" de dos agentes españoles a un preso interno en la base militar de Guantánamo, cuyo testimonio fue recuperado como indicio probatorio de refuerzo de la declaración prestada por el acusado. Decíamos entonces que "...la detención de cientos de personas, entre ellas el recurrente, sin cargos, sin garantías y por tanto sin control y sin límites, en la base de Guantánamo, custodiados por el ejército de los Estados Unidos, constituye una situación de imposible explicación y menos justificación desde la realidad jurídica y política en la que se encuentra enclavada. Bien pudiera decirse que Guantánamo es un verdadero "limbo" en la Comunidad Jurídica". La cita de este fragmento sugiere una doble reflexión. De una parte, se opone de manera frontal a la proclamación del principio de no indagación como una regla de valor apodíctico en nuestra jurisprudencia. La Sala indagó y lo hizo para concluir la falta de virtualidad probatoria de un testimonio de referencia, por más que procedía de agentes de la autoridad españoles expresamente desplazados a territorio estadounidense para la práctica de un interrogatorio que fue ajeno a los principios estructurales de contradicción y defensa y que, por si fuera poco, se practicó en el entorno de coacción moral que es imaginable en un centro de reclusión concebido en los términos en los que aquél fue diseñado. De otra parte, la lectura de ese razonamiento es bien expresiva de la necesidad de no fijar reglas generales que en su inflexibilidad no tomen en consideración la rica variedad de supuestos que nos ofrece la práctica. La intensidad de la vulneración de derechos denunciada admite matices de los que no puede prescindirse en el momento de fijar el alcance de la regla de exclusión.

En definitiva, el principio de no indagación no puede interpretarse más allá de sus justos términos"[147].

f. La valoración de la prueba electrónica

En relación con la valoración de la prueba electrónica, en nuestro Ordenamiento no existe un procedimiento probatorio específico para valorarla[148]. A

147 Sentencia de la Audiencia Provincial de las Palmas de 5 de noviembre de 2018, en Tirant on line, DOCUMENTO TOL7.067.587.

148 Como señala DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba*..., op. cit., pág. 93, a los efectos valorativos hay que tener en cuenta "la naturaleza de las distintas pruebas, ya que el recurso a la analogía interpretativa, es indispensable en los casos en que no existe legislación y/o jurisprudencia suficiente al respecto, como sucede, precisamente en relación a la prueba electrónica o tecnológica".

mi parecer, ello obedece, a dos razones: en primer lugar, a que como tampoco existe una definición legal de qué se entiende por prueba electrónica es difícil que se puede llegar a regular o establecer un procedimiento para su valoración, por tanto, tenemos que remitirnos a la regulación existente para la prueba tradicional, y; en segundo lugar, también es cierto que la prueba tecnológica no es diferente a la prueba tradicional en lo que se refiere a probar los hechos, aunque se haga a través de medios electrónicos o informáticos, por lo tanto, en este sentido, tampoco tendría que fijarse un procedimiento específico.

A mi juicio, la diferencia que puede existir entre las distintas modalidades no es tanto en lo relacionado a la valoración de la prueba sino en relación a la admisión de la misma por su facilidad a la hora de manipularla. Por tanto, una vez determinado qué se entiende por prueba electrónica, la valoración de la misma ser hará tal y como está prevista para la prueba tradicional, teniendo en cuenta igualmente si nos referimos a documento electrónico o medios de reproducción de la palabra, el sonido o la imagen, o cualquier otro medio de prueba que sirva para acreditar esos hechos electrónicos en el proceso.

La base de la que se debe partir estriba en la posible impugnación de la prueba por las partes, en el sentido de que si estas no llevan a cabo la impugnación de la prueba electrónica cualquier soporte o medio es válido para acreditar hechos o circunstancias relevantes en el proceso. Por tanto, si no se impugna no existe controversia sobre su validez sí sobre su naturaleza como documento o como otro medio de prueba, pero no sobre su validez en sí.

A este respecto el Tribunal Constitucional nos advierte que "*el derecho a la presunción de inocencia se configura como el derecho a no ser condenado sin pruebas de cargo válidas, lo que exige una mínima actividad probatoria, realizada con las garantías necesarias, referida a todos los elementos esenciales del delito, y que de la misma quepa inferir razonablemente los hechos y la participación del acusado en los mismos; así, sólo cabrá constatar la vulneración del derecho a la presunción de inocencia cuando no haya pruebas de cargo válidas, es decir, cuando los órganos judiciales hayan valorado una actividad probatoria lesiva de otros derechos fundamentales o carente de garantías, o cuando no se motive el resultado de dicha valoración, o, finalmente, por ilógico o por insuficiente no sea razonable el iter discursivo que conduce de la prueba al hecho probado*"[149].

En definitiva, acreditada la validez del medio de prueba en el proceso pe-

149 STC Sala 2ª, S 14 de marzo de 2011, nº 25/2011, rec. 1131/2009. En Tirant on line, Documento TOL2.068.799.

nal la valoración sería factible. Y en materia de prueba electrónica la validez de la misma tiene que atender a lo exigido anteriormente en relación con la integridad, autenticidad, fiabilidad, etc.

f.1 Valoración conforme a la sana crítica

La regla general en materia de valoración de la prueba, en el proceso penal, sea esta electrónica o no, es su valoración libre conforme a las reglas de la sana crítica o máximas de experiencia. El artículo 741 de la LECrim configura el principio de libre valoración probatoria al establecer que el Tribunal dictará sentencia apreciando según su conciencia las pruebas practicadas en el juicio. Si bien, como indica la doctrina "la valoración libre de la prueba debe ser una valoración racional no arbitraria que debe justificarse y expresarse en las decisiones que se tomen en cada caso concreto, sabiendo que estas decisiones son objeto de control incluso por el tribunal de casación"[150]. Por ello, en la sentencia y en concreto en la fundamentación jurídica se debe incluir el análisis de los elementos probatorios que fundamentan su convicción fáctica. El control de la valoración probatoria por parte del Tribunal Supremo, vendrá estrictamente referido a la comprobación de la existencia de prueba, si es de contenido incriminatorio, si en su obtención se han observado las garantías constitucionales, si es suficiente para enervar el derecho a la presunción de inocencia y si ha sido valorada racionalmente por el tribunal sentenciador, sin infracción evidente de las reglas de la sana crítica, las máximas de la experiencia o los principios científicos, y que en lo relativo a su impugnación, deberá atenderse al resultado del test de admisibilidad[151].

En este sentido, el juez valorará libremente, conforme a su conciencia, la prueba electrónica sin que el carácter técnico de dicha prueba implique que el juez deba valorarla de forma tasada. Ahora bien, en la mayoría de los casos, debido al carácter técnico y complejo de estas pruebas, el juez se verá auxiliado por un perito informático que le garantice que la prueba electrónica no ha sido manipulada o que explique las cuestiones más técnicas, pero ello no supone que no pueda realizar una valoración libre.

Por tanto, en el proceso penal a diferencia del proceso civil todos los me-

150 DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba*..., op. cit., pág. 23.

151 Véase la STS 1143/2018, de 8 de marzo, ECLI:ES:TS:2018:1143, en https://www.poderjudicial.es/search/openDocument/d7b2698688481 2c2.

dios de prueba son de valoración libre, de acuerdo al artículo 741 de la LECRim, no existe priorización ninguna entre los distintos medios probatorios y, por tanto, la consideración de documento electrónico o instrumento tecnológico no tendrá ningún tipo de consecuencias en materia de valoración probatoria. Ello difiere del proceso civil en el que el documento electrónico, al igual que el documento en formato papel, conlleva una valoración tasada.

f.2 Valoración legal

En el proceso penal, como comenté anteriormente, todos los medios de prueba son de valoración libre, conforme a las reglas de la lógica o de la experiencia, es decir, ningún medio de prueba se valora de forma tasada. En el proceso civil, en cambio, existen dos medios de prueba que en determinados casos conllevan una valoración legal o tasada como son el interrogatorio de partes, cuando es el único medio de prueba y se declara sobre hechos personales y perjudiciales, y también el documento público y el privado cuando se reconoce su autenticidad o no es impugnado.

Por tanto, en los supuestos en los que la prueba electrónica tenga la naturaleza de documento electrónico, debemos acudir necesariamente a su regulación, en concreto, a la Ley 59/2003, de 19 de diciembre de Firma Electrónica, donde se especifica la valoración que debe hacer el juez de estos instrumentos de prueba[152].

f.3 Especialidades valorativas

En relación con determinados tipos de prueba, o por decirlo de otra forma, atendiendo a la naturaleza de la prueba en cuestión se suele hablar de estándares de valoración, como guías o pasos a seguir para valorar una prueba. En este sentido, se suele hacer referencia a estos estándares valorativos cuando se habla de la prueba científica, es lo que TARUFFO llama "discrecionalidad

152 Señala ROUANET MASCARDÓ, Jaime, "Valor probatorio procesal del documento electrónico", op. cit., pág. 175, que: "Según el Código Civil, el documento auténtico (sea normal o electrónico), público o privado, produce la misma eficacia probatoria, en cualquier caso impuesta por la Ley. Es un medio de prueba tasado, en principio, que el Juez debe valorar de acuerdo con lo establecido en las normas legales, aunque la jurisprudencia del Tribunal Supremo y la regulación del recurso de casación han hecho de esta prueba una más de valoración libre".

guiada" por las reglas de la ciencia, la lógica y la argumentación racional[153]. No son exactamente reglas de valoración sino una guía o una serie de pautas que proporciona el criterio de la probabilidad probable y que se da fundamentalmente en las pruebas científicas. Esta guía es perfectamente aplicable a la prueba tecnológica o electrónica[154].

De hecho, la reforma llevada a cabo en 2002 sobre el párrafo 2º del artículo 788.2 de la LECrim mediante la Disposición Adicional Tercera de la LO 9/2002, de 10 de diciembre, sobre sustracción de menores introduce una pauta de valoración cambiando la naturaleza del medio de prueba. Así en relación con el procedimiento abreviado dicha reforma dispone que «tendrán carácter de prueba documental los informes emitidos por laboratorios oficiales sobre la naturaleza, cantidad y pureza de sustancias estupefacientes cuando en ellos conste que se han realizado siguiendo los protocolos científicos aprobados por las correspondientes normas»[155]. Por tanto, convierte la prueba pericial en una prueba documental con lo que ello supone en el proceso.

Señala la doctrina a este respecto que es necesario "*la adecuación de ciertas reglas procesales ya existentes y la creación de otras nuevas que permitan la entrada del conocimiento científico en el proceso, manteniendo el respeto a todas las garantías -presunción de inocencia, derecho de defensa, derecho a los medios de prueba pertinentes y, en definitiva, el derecho a la tutela judicial efectiva*"[156].

Aunque cada clase de prueba electrónica o tecnológica tiene características propias, en general, se puede decir que en el ámbito de la prueba tecnológica, además del contenido de la misma, los temas de autenticidad, integridad y autoría, resultan más o menos problemáticos en casi todos los casos. Como

153 TARUFFO, M, "Conocimiento científico y estándares de prueba judicial", en Revista *Jueces para la Democracia*, nº 52, marzo 2005.

154 DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba*..., op. cit., págs. 60 y 61.

155 Véase a SÁNCHEZ RUBIO, Ana, *La prueba científica en la justicia penal*, Tirant lo Blanch, 2019, en Tiran on line, DOCUMENTO TOL7.571.683, quien indica que "respecto a ello surgen varios interrogantes: ¿Estamos ante una prueba documental o ante una prueba documentada?, ¿Es éste un medio de prueba idóneo para cualquier prueba científica o solo para algunas? Siendo así, ¿para cuáles? ¿Existe, tal vez, otro medio distinto a la pericial capaz de trasmitir los conocimientos científicos al proceso de un modo eficiente?, etc".

156 SANCHEZ RUBIO, Ana, *La prueba científica en la justicia penal*, Tirant lo Blanch, 2019, en Tiran on line, DOCUMENTO TOL7.571.683.

ya he puesto de manifiesto en repetidas ocasiones las posibles manipulaciones de este tipo de pruebas, requieren de ese "plus" de garantía para el juicio de autenticidad que sólo puede aportar un experto[157]. En este sentido, la integridad, autenticidad y licitud serían las tres garantías esenciales que deben observarse en el *iter* procesal de la prueba electrónica. Si bien estas garantías son esenciales en materia de validez de la prueba como condición necesaria para entrar a valorarla, sin embargo, cuando de prueba electrónica o científica hablamos son insuficientes para determinar si el método utilizado descansa sobre fundamentos verdaderamente científicos o se sustenta en teorías carentes de verificación[158].

En definitiva, dadas las características de la prueba científica han de fijarse, por tanto, ciertos estándares de valoración, común a todas ellas, que faciliten la labor de evaluación de sus resultados. Al respecto manifiesta LAUDAN que "dicho estándar sirve como regla de decisión para que el juzgador de los hechos alcance el veredicto del caso. Sin un estándar de prueba el veredicto mismo no estaría justificado y cualquier declaración de culpabilidad será injusta"[159].

g. La dimensión extraterritorial de Internet

FLORES PRADA indica que las redes digitales y fundamentalmente Internet plantean, como mínimo, tres grandes dificultades para su regulación por los modernos derechos nacionales: la universalidad, la horizontalidad, y la dependencia del código técnico[160].

Aunque el uso de Internet conlleva muchas ventajas y nos facilita la comunicación a nivel global, sin embargo, una de las cuestiones más problemáticas que siempre se pone de manifiesto es precisamente esa dimensión extraterritorial de Internet puesto que en la Red el territorio físico no tiene importancia, sino que lo que cuenta en la Red son los terminales, los servidores, los

157 DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba*..., op. cit., pág. 70.

158 SANCHEZ RUBIO, Ana, *La prueba científica*..., op. cit., DOCUMENTO TOL7.571.685.

159 LAUDAN, L., «La elemental aritmética epistémica del derecho II: los inapropiados recursos de la teoría moral para abordar el derecho penal», en VÁZQUEZ, C., *Estándares de prueba y prueba científica*, Marcial Pons, Madrid, 2013, pág. 121.

160 Véase "Prevención y solución...", op. ci., pág. 7.

proveedores, las conexiones y la información circulante por todo el mundo[161]. Esta dimensión espacial complica mucho la labor de rastreo de la información cuando se ha cometido un hecho delictivo. Hay que tener en cuenta que en relación con la criminalidad organizada uno de sus rasgos característicos es la transnacionalidad, es un fenómeno global que supera los límites de las fronteras territoriales de los Estados y si añadimos además a la criminalidad organizada el uso de las nuevas tecnologías conlleva la dificultad de investigar y enjuiciar dichas conductas delictivas dada la dimensión extraterritorial. En este sentido, existe una íntima conexión entre la delincuencia organizada y las nuevas tecnologías por la capacidad que éstas tienen de potenciar y facilitar el desarrollo de las actividades criminales de dichas estructuras organizativas[162]. La combinación de dichos factores – transnacionalidad y rapidez- potencia considerablemente la comisión de determinados hechos delictivos.

Como ya he comentado anteriormente, Internet es un sistema de redes conectados a nivel mundial, la información y, por tanto, la comunicación de la misma se hace a través de conexiones extraterritoriales. Es una estructura mundial, cuyos canales de comunicación no son físicos sino digitales, lo que dificulta el control fronterizo y la ubicación territorial de actividades, conexiones y operaciones[163]. Si ya es difícil el rastrear la información a nivel interno mayores dificultades se plantean a nivel internacional, no sólo en cuanto a descubrir la autoría de los delincuentes sino también en lo relativo al enjuiciamiento de sus conductas puesto que, aunque no existen barreras en la comunicación vía Internet sí existen fronteras a la hora de investigar, enjuiciar y castigar las conductas de los delincuentes en el ciberespacio. En este sentido, la nueva dimensión espacial de Internet actualmente no se ajusta a la dimensión territorial en la persecución y enjuiciamiento de los delitos por los agentes encargados de los mismos y ello, evidentemente, plantea dificultades añadidas. En definitiva, el principio de territorialidad en el cual se basa el principio de lugar de comisión del hecho delictivo no opera en los delitos cometidos en el ciberespacio[164], en este mundo digital

161 FLORES PRADA, I., "Prevención y solución…", op. cit., pág. 8.

162 DEL ROSAL BLASCO, *Criminalidad organizada y nuevas tecnologías: Algunas consideraciones fenomenológicas y político-criminales*, 2001, en Tirant on line, DOCUMENTO TOL163.240.

163 Véase a FLORES PRADA, I., *Criminalidad informática. Aspectos sustantivos y procesales*, Tirant lo Blanch, 2012.

164 En estos supuestos independientemente de la ubicación física de los servidores, lo que se tiene en cuenta, es el lugar desde el que se tiene acceso a la información. Puesto

las fronteras físicas no existen y, por tanto, se plantean problemas de jurisdicción y competencia.

g.1 Ámbito europeo

Esta cuestión tan problemática se ha puesto de manifiesto en todos los países de nuestro entorno por lo que, como se ha señalado, hay más que sobrados motivos para encontrar cauces de regulación común en materia de pruebas electrónicas[165]. De hecho, en el ámbito de la Unión Europea se han propuesto dos instrumentos jurídicos dirigidos precisamente a regular esa materia como es la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, de 17 de abril de 2018 y la Propuesta de Directiva por la que se establecen normas armonizadas para la designación de representantes legal a efectos de recabar pruebas para procesos penales, de la misma fecha[166].

Como complemento de estos dos instrumentos se encuentra la Orden de investigación europea, regulada por la Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, implementada en nuestro Ordenamiento por la Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales, para regular la Orden de Investigación Penal[167].

Como se indica en la Propuesta de Reglamento europeo citado la finalidad principal de aquellos instrumentos jurídicos es que los órganos competentes de los Estados miembros puedan acceder a datos que sirvan como prueba y que están almacenados fuera de su país o por proveedores de servicios de otros Estados miembros o de países terceros. De esta forma, se hace realidad la cooperación judicial en materia penal a través de un instrumento de reconocimiento mutuo que posibilita la obtención de prueba electrónica en

---

que podría darse el caso de que se no se conociera la ubicación física de las instalaciones o que los servidores se encuentren dispersados por varios países, y en consecuencia la impunidad de conductas delictivas.

165 PÉREZ GIL, Julio, "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal", op. cit., págs. 423 y 424.

166 COM/2018/226 final- 2018/0107 (COD) de 17 de abril de 2018, véase en https://eur-lex.europa.eu/legal-contest/ES/TXT/

167 BOE número 142, de 12 de junio.

todas las fases del proceso penal y además en cualquier Estado miembro de la Unión Europea[168].

En este sentido, los anteriores instrumentos jurídicos que regulaban la obtención de pruebas en el ámbito penal han ido quedando obsoletos por no adaptarse a las exigencias de las nuevas tecnologías, así ocurrió con la Decisión Marco 2008/978/JAI, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal que fue derogado por el Reglamento (UE) 2016/95, del Parlamento Europeo y del Consejo, de 20 de enero de 2016, por el que se derogan determinados actos en el ámbito de la cooperación policial y judicial en materia penal[169]. Ha ocurrido también con la Orden europea de investigación[170] que vino a sustituir determinadas disposiciones relativas a la prueba tanto del Convenio Europeo de Asistencia judicial en materia penal del Consejo de Europa de 20 de abril de 1959, así como sus dos protocolos adicionales y los acuerdos bilaterales celebrados de acuerdo a su artículo 26, como el Convenio relativo a la aplicación del Acuerdo Schengen, y también el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea y su Protocolo del 2001[171].

La Propuesta de Reglamento sobre órdenes europeas de entrega y conservación de pruebas electrónicas ofrece instrumentos adicionales a las autoridades de investigación para que obtengan pruebas electrónicas sin limitar las competencias ya previstas por la legislación nacional[172]. Sin entrar en profundidad en el procedimiento a seguir en este ámbito, una de las características fundamentales de este nuevo instrumento de reconocimiento mutuo es la agilización a la hora de obtener los datos electrónicos. El procedimiento es relativamente sencillo y si no existe ningún impedimento formal o material el proveedor de servicios a través de su representante legal ejecutará directamente las órdenes sin necesidad de que intervenga ninguna autoridad más del Estado miembro de ejecución.

---

168 LÓPEZ JIMÉNEZ, Raquel, "El nuevo marco jurídico transfronterizo de las pruebas electrónicas, las órdenes de entrega y conservación de las pruebas electrónicas", en *Revista General de Derecho Europeo,* noviembre, número 49, 2019, véase en https://www-iustel-com.biblioteca5.uc3m.es//v2/revistas/detalle_revista.asp?id_noticia=421898&texto=

169 Publicado en el Diario Oficial de la Unión Europea, el 2 de febrero de 2016, L 26/9.

170 Publicada en el DOUE el 1 de mayo de 2014, L 130.

171 Véase mi trabajo "El nuevo marco jurídico transfronterizo de las pruebas electrónicas. Las órdenes de entrega y conservación de las pruebas…", op. cit.

172 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52018PC0225.

En definitiva, todos estos instrumentos procesales van dirigidos a facilitar la investigación y persecución de los delitos a través de la creación de herramientas adecuadas para la obtención y aportación de datos en el proceso penal más allá de las barreras nacionales.

g.2 Ámbito internacional: especial referencia a EE.UU.

Ahondando en lo dicho, uno de los problemas principales con los que se encuentran los órganos encargados de la investigación de los hechos delictivos es la localización precisamente de los datos, puesto que estos se encuentran localizados muchas de las veces en servidores informáticos fuera del territorio español y primordialmente en Estados Unidos.

Por ello, he decidido hacer una referencia especial a EE.UU. porque una buena parte de los grandes proveedores de servicios de Internet a nivel global se encuentran en Estados Unidos, o por lo menos sus casas matrices se hallan radicadas en dicho país[173]. Por tanto, junto a los marcos jurídicos internacionales de referencia, hay que tener también en cuenta algunos aspectos del derecho de los Estados Unidos que, evidentemente, tienen una importante incidencia práctica en este tipo de asuntos.

A mayor abundamiento, desde el plano penal sustantivo, Estados Unidos es el país pionero en materia de delitos cibernéticos, de hecho, el concepto de "delito cibernético" tiene origen en ese país. Estados Unidos acuñó el término de *cybercrime*, en una acepción amplia del mismo, la que comprende tanto aquellas situaciones en que el elemento informático se encuentra en el objeto de la conducta penada (vg. intromisión ilegal a bancos de datos), como aquellas en que dicho elemento es el medio para realizar un fin ilícito (vg. estafa vía Internet).

Partiendo de estas premisas, la cooperación judicial internacional con EE.UU. se puede hacer efectiva a través de la asistencia judicial internacional. En este sentido, las solicitudes de auxilio judicial dirigidas a Estados Unidos tienen su base legal tanto en el Convenio sobre Cibercrimen, como el Texto integrado de las disposiciones del Tratado de Auxilio Judicial en Materia Penal entre los EEUU y España de 20 de noviembre de 1990 y el Acuerdo de Asistencia Judicial entre la Unión Europea y EEUU de 2003.

El Acuerdo establece las condiciones relativas a la prestación de asistencia

173 Por ejemplo, en relación con las redes sociales Facebook, Twitter, Youtube, tienen su sede en Estados Unidos.

judicial mutua en materia penal entre la UE y los EE.UU. Por tanto, su objetivo es mejorar la cooperación entre los países de la UE y los EE.UU., como complemento a los tratados bilaterales celebrados entre los países de la UE y los EE.UU. Atendiendo al Acuerdo, la UE y los EE.UU. deberán permitir el establecimiento y el funcionamiento de equipos conjuntos de investigación para facilitar las investigaciones o causas penales entre uno o más países de la UE y los EE. UU.

La normativa de referencia en Estados Unidos para la cesión o intervención de los datos es la contenida en la *Electronic Communications Privacy Act* (ECPA) de 1986 donde se distingue cuando es necesaria la comisión rogatoria o no para la cesión de los datos.

Por tanto, de acuerdo a esta normativa para obtener de las ISP (proveedores de servicios de Internet) alojadas en EE.UU., datos de registro de conexión o suscriptores se puede llevar a cabo de dos formas distintas: a) a través de una solicitud de auxilio judicial, o; b) directamente del ISP cuando se refieran a determinados datos[174].

Aunque la política de los ISP está cambiando súbitamente y sin previo aviso, es siempre muy recomendable que, tal y como se indica en el Compendio de Guías prácticas para asuntos de auxilio judicial internacional entre España y los Estados Unidos, cuando una autoridad española desee hacer una preservación (conservación rápida) o un pedido directo de datos en relación con una cuenta de un proveedor estadounidense consulte antes con la Magistratura de enlace[175]. La conservación rápida de datos informáticos almacenados, de acuerdo al artículo 16 del Convenio de Budapest, posibilita que se pueda pedir posteriormente una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos (artículo 29 del Convenio). La conservación rápida de datos es una medida previa y obligatoria a la solicitud de acceso a esos datos para evitar que dicha información sea borrada o alterada. No se llevará a cabo ninguna comisión rogatoria si antes no se ha solicitado la preservación

174 Véase a SÁNCHEZ SISCART, José Manuel, "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU.", en *Revista del Poder Judicial*, número 91, año 2011, págs. 38 y ss.

175 Dirección General de Cooperación Jurídica Internacional, Relaciones con las Confesiones y Derechos Humanos, Magistratura de enlace de España ante los Estados Unidos, 2019, pág. 63, véase en https://www.mjusticia.gob.es/ca/AreaInternacional/CooperacionJuridicaInternacional/Documents/1292429588802-Compendio_de_guias_practicas_para_asuntos_de_Auxilio_Judicial_I.

de los datos. Es importante solicitar antes la preservación o conservación de datos puesto que en Estados Unidos los proveedores de servicios de Internet no están obligados a guardar datos y generalmente borran los registros de transmisión, así como el contenido de los mensajes de correo electrónico cuando ya no son necesarios desde el punto de vista comercial[176].

Dada la ingente cantidad de peticiones de asistencia a través de comisiones rogatorias que recibe Estados Unidos, en relación a datos de cuentas de Internet ubicados en servidores o redes propiedad de multinacionales con sede en el país, se han generado dificultades en su gestión. Por ello, el Departamento de Justicia ha decidido, en relación con la conservación de datos, instar a los diferentes actores a que dirijan directamente sus solicitudes a las empresas interesadas, las que en no pocos casos requieren que los pedidos se encaminen a la casa matriz en Estados Unidos[177].

Las solicitudes de acceso a los datos se llevan a cabo a través del auxilio judicial, en concreto a través de comisiones rogatorias. No obstante, excepcionalmente, sin necesidad de la comisión rogatoria puede pedirse directamente a través de la Magistratura de enlace a los proveedores o prestadores de servicios de Internet los datos de suscriptores[178] y datos transaccionales[179], nunca los datos de contenido de comunicaciones[180]. En definitiva, es posible esta cooperación directa precisamente para agilizar el procedimiento y con ello la efectividad de las medidas ya que una comisión rogatoria puede alargarse más de 10 meses y de la otra forma 1 o 2 semanas. Ahora bien, la entrega de los datos por parte de las empresas proveedoras de servicios es voluntaria, de manera de serán ellas las que decidan, atendiendo a su política de privacidad, la entrega o denegación de los datos y contra esta decisión no cabe ningún tipo de recurso. Al margen de esta política de privacidad, existen determinadas barreras legales en Estados Unidos que imposibilitan la entrega de datos, entre ellas se encuentra la necesidad de que el delito que se investiga

176 Véase a SÁNCHEZ SISCART, JOSÉ MANUEL, "Cibercrimen y cooperación judicial…", op. cit., pág. 41.

177 Ibídem.

178 Son datos de suscripción: el nombre del usuario, la dirección física y otros datos de contacto, así como los datos de facturación si el servicio es de pago.

179 Son datos transaccionales o técnicos: todos aquellos datos relativos a la comunicación generados por el sistema y que indican el origen, destino, ruta, hora, fecha, tamaño, duración de la comunicación o tipo de servicio subyacente.

180 Son datos de contenido: todos aquellos datos relativos a los mensajes que las partes se transmiten entre sí en el seno de una comunicación.

por el cual es solicitan los datos no sea un delito que se refiera a la libertad de expresión, puesto que es Estados Unidos no pueden perseguirse penalmente las opiniones, ideas, pensamientos, etc. Por tanto, no se permite la entrega de datos cuando el delito que se investiga se refiera al derecho a la libertad de expresión, entre estos delitos estarían el delito de injurias, calumnias, odio, apología del terrorismo y revelación de secretos. Si se dan los presupuestos correspondientes se puede reclamar civilmente pero nunca penalmente.

En nuestro Ordenamiento jurídico, de acuerdo al artículo 588 octies de la LECrim, tras la reforma efectuada por la Ley Orgánica 13/2015, se permite además de al órgano judicial también al Ministerio Fiscal y a la Policía Judicial que requieran "*a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes*".

En relación con los datos de contenido, que necesariamente deben solicitarse a través de comisión rogatoria y nunca directamente a los ISP, se requiere que en la solicitud se indique la "causa probable" que justifique su admisión, de manera que a los ojos de un "ciudadano medio" deben existir elementos de convicción suficientes como para entender que esos datos están claramente vinculados con la actividad presuntamente delictiva objeto del proceso[181]. Hay causa probable en relación con los registros o accesos a comunicaciones cuando se dispone de información suficiente, debidamente obtenida y acreditada, de tal manera que una persona prudente llegaría a la conclusión de que, efectivamente, a través de dicho registro o acceso podrán obtenerse evidencias sobre la comisión del presunto delito[182]. La razonable sospecha no sería causa probable.

Por tanto, en la comisión rogatoria deberá indicarse detalladamente, de forma clara y precisa, los hechos delictivos objeto de enjuiciamiento. No vale con una somera indicación, sino que es necesario que se acrediten los hechos que sean relevantes junto con la fundamentación jurídica. Además, es fundamental que se indique la conexión que existe entre los hechos que se investigan y la concreta comunicación que se quiere investigar, bien sea esta una cuenta de internet, correo, etc. Esa conexión debe ser de igual forma relevante. De otra forma, lo más probable es que se deniegue la orden.

181 Compendio de guías prácticas para asuntos de auxilio judicial..., op. cit., pág. 71.
182 Ibídem, pág. 127.

La "causa probable" deriva de la Cuarta Enmienda de la Constitución estadounidense, la cual establece que "*El derecho del pueblo a sentirse seguro en sus personas, hogares, papeles y efectos, frente a pesquisas y aprehensiones no razonables, será inviolable, y no se expedirán al efecto mandamientos sino bajo causa probable, apoyados bajo juramento o protesta, y particularmente describiendo el lugar que debe ser registrado y las personas o cosas que deben ser detenidas o embargadas*". Esta causa probable no rige para todo lo que tiene que ver con el acceso a datos de comunicaciones en sentido amplio, sino que hay que ver en concreto qué tipo de información se quiere solicitar. Así, determinados datos pueden ser enviados directamente por las proveedoras de servicios sin necesidad de hacerlo a través de una comisión rogatoria.

En definitiva, los datos que se podrían mandar directamente a España sin necesidad de comisión rogatoria serían:

1. Datos de suscripción: datos del titular de una cuenta de Internet, es decir, los datos con los que se abrió la cuenta o su actualización (nombre, dirección, teléfono, dirección de correo electrónico).

2. Datos de transacción o metadatos: direcciones IP, registros de conexión, registros de sesión o logs, etc.,

En estos dos tipos de datos no hay que acudir al estándar de la causa probable. Bastará con alegar y justificar que esos datos son, además de relevantes, importantes para la investigación o el proceso[183].

Finalmente, en casos de urgencia los proveedores de servicios de Internet pueden entregar datos tanto los relativos a transacciones, de suscripción como de contenido, directamente a través del representante del *law enforcement* federal estadounidense. Muchos proveedores admiten pedidos directos del *law enforcement* de otros países, y en los casos de urgencia o emergencia puede operarse a través del agregado local del FBI o directamente con el proveedor. El Departamento de Justicia ha ofrecido un canal de comunicación oficial especialmente rápido que se concreta en el agregado local del FBI. En el caso español, el agregado del FBI en la Embajada de los Estados Unidos en Madrid[184].

Debe existir un peligro inminente para la vida o para la integridad física de las personas: *imminent danger of death or serious physical injury requiring disclosure without delay*. (18 U.S. Code § 2702 - Voluntary disclosure of

183 Véase el Compendio de guías prácticas, op. cit., págs. 126 y ss.

184 Compendio guías prácticas..., pág. 139.

customer communications or records). Más concretamente, lo que se establece en 18. U.S. Code § 2702, en su apartado 8, es que "un proveedor puede voluntariamente entregar datos a una entidad gubernamental si, de buena fe, entiende que existe una emergencia vital o relacionada con un riesgo grave de daño físico para una persona que conlleva la necesidad de dar a conocer sin dilación comunicaciones relacionadas con dicha emergencia"[185]. Hay que recalcar que, aunque se pueden entregar datos de las tres clases (de suscripción, transaccionales y de contenido), sin embargo, son entregas voluntarias en las que el proveedor determina la extensión y límites de los datos que va a entregar.

Hay que tener en cuenta que "*las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado*". Aunque parezca baladí el primer momento crítico o más peligroso para resguardar la protección de los datos personales se encuentra precisamente cuando el usuario procede a registrarse, esto es, cuando este proporciona la información personal requerida y necesaria para poder operar en la red social, desde este momento los datos personales pueden verse sometidos a diferentes riesgos, uno de estos riesgos es el relativo a la transferencia internacional de datos. Como sabemos, muchas de estas plataformas *on line* se encuentran ubicadas fuera de Europa, mayoritariamente en EE.UU., lo que implica que, en el mismo instante en que se registra el usuario, los datos son trasladados a los servidores y oficinas ubicados en ese país. En consecuencia, resulta primordial que las políticas de privacidad del proveedor de servicios aseguren un nivel adecuado de protección. Como se indica en el Estudio citado puede ocurrir, con los problemas que ello supone, que las plataformas cedan sus bases de datos a terceras organizaciones, con la finalidad de que se realicen campañas de envío de comunicaciones comerciales no autorizadas (spam) o realicen otro tipo de tratamiento que goce de menor protección en el país en el que se tratan los datos[186].

En 2017 en EE.UU., la protección de los datos personales sufrió un re-

185 Ibídem.

186 Véase el Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, Instituto Nacional de Tecnologías de la Comunicación (INTECO) y a la Agencia Española de Protección de Datos (AEPD), pág. 96, febrero de 2009, en https://www.uv.es/limprot/boletin9/inteco.pdf.

vés cuando el expresidente Donald Trump publicó una ley que permitía a los proveedores de servicios de Internet (ISP) comerciar con los datos de los consumidores sin requerir el consentimiento previamente, invalidando así una norma impulsada bajo la presidencia de Barak Obama que establecía lo contrario[187]. Es cierto que las empresas de Internet como Facebook y Google ya tenían acceso a este tipo de información y recopilaban datos de los consumidores sin tener que pedir permiso, lo que añade esa norma además es que los ISP pueden ir más allá y acceder a la información completa sobre todos los sitios web que visita un consumidor. Por tanto, esta nueva norma posibilita que las empresas de telecomunicaciones puedan vender cualesquiera datos de los usuarios de Internet, partiendo de los que se refieren a su historial de navegación, hasta su localización, el registro del uso de aplicaciones o incluso el tipo de dispositivo desde el que usan la red, entre otros.

g.3 Dificultades de determinar la jurisdicción y competencia en los delitos cometidos a través de las nuevas tecnologías

Uno de los principales problemas que se plantean a la hora de investigar y enjuiciar estos delitos cometidos a través de la red, u *on line*, es determinar la jurisdicción y el órgano competente para su conocimiento puesto que muchos de los efectos del delito pueden tener lugar en diferentes territorios. En este sentido, determinar el lugar desde donde se produce la comunicación es complicado puesto que en ocasiones se lleva a cabo desde un equipo informático o cualquier otro equipo con acceso a Internet que no está fijo y que puede redireccionar a través de diversos servidores que pueden estar ubicados en diferentes territorios nacionales o extranjeros.

Nuestra Ley Orgánica del Poder Judicial, en su artículo 23, tras la reforma introducida por la Ley Orgánica 1/2014, de 13 de marzo, de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, relativa a la justicia universal[188], se modifica e introduce en su apartado k) los delitos contra la libertad e indemnidad sexual, cometidos sobre víctimas menores de edad, entre los que se encuentra el delito de "grooming", objeto de nuestro estudio.

187 El *Privacy Shield* (Escudo de Privacidad*),* un nuevo marco legal que permitía a las empresas enviar y almacenar información personal de ciudadanos europeos sin comprometer su seguridad. Este fue declarado inválido por el Tribunal de Justicia de la Unión Europea el 16 de julio de 2020.

188 BOE número 63, de 14 de marzo de 2014, páginas 23026 a 23031 (6 págs.).

Así, en dicho apartado se indica que "será competente la jurisdicción española para conocer de los hechos cometidos por españoles o extranjeros fuera del territorio nacional susceptibles de tipificarse, según la ley española, como alguno de los siguientes delitos, -entre los que se encuentran el comentado-, cuando se cumplan las condiciones expresadas:

1º El procedimiento se dirija contra un español;

2º El procedimiento se dirija contra ciudadano extranjero que resida habitualmente en España;

3º el procedimiento se dirija contra una persona jurídica, empresa, organización, grupos o cualquier otra clase de entidades o agrupaciones de personas que tengan su sede o domicilio social en España; o,

4º el delito se hubiera cometido contra una víctima que, en el momento de comisión de los hechos, tuviera nacionalidad española o residencia habitual en España".

En el mismo artículo 23 de la LOPJ se indica que: "asimismo, la jurisdicción española será también competente para conocer de los delitos anteriores cometidos fuera del territorio nacional por ciudadanos extranjeros que se encontraran en España y cuya extradición hubiera sido denegada por las autoridades españolas, siempre que así lo imponga un Tratado vigente para España".

Además, la persecución de los delitos cometidos fuera de España por la jurisdicción española exige la previa interposición de la querella por el agraviado o por el Ministerio Fiscal.

Tal y como se indica en la Exposición de Motivos de la Ley Orgánica 1/2014, de justicia universal "también se delimita con carácter negativo la competencia de los tribunales españoles, definiendo con claridad el principio de subsidiariedad. En ese sentido, se excluye la competencia de los tribunales españoles cuando ya se hubiese iniciado un procedimiento en un Tribunal Internacional o por la jurisdicción del país en que hubieran sido cometidos o de la nacionalidad de la persona a la que se impute su comisión, en estos dos últimos casos siempre que la persona a que se imputen los hechos no se encuentre en España o, estando en España vaya a ser extraditado a otro país o transferido a un Tribunal Internacional, en los términos y condiciones que se establecen".

En todo caso, la jurisdicción española se reserva la posibilidad de continuar ejerciendo su jurisdicción si el país extranjero que la ejerce no está dispuesto a llevar a cabo la investigación o no puede realmente hacerlo. En

este sentido, corresponde a la Sala 2ª del Tribunal Supremo valorar estas circunstancias de acuerdo a los criterios recogidos en el Estatuto de la Corte Penal Internacional.

Una de las modalidades de comisión de delitos contra la libertad e indemnidad sexual contra menores de edad se encuentra en el delito de "grooming" que, como vimos en un apartado anterior, la comisión de ese hecho delictivo se lleva a cabo a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación.

La tipificación del delito de "grooming" llevada a cabo por la Ley Orgánica 1/2015, de 30 de marzo del Código Penal, se encuadra dentro de los delitos tipificados en el Código Penal como delitos contra la libertad e indemnidad sexual. Por tanto, dentro de la previsión efectuada por el artículo 23 de la Ley Orgánica del Poder Judicial, modificada por la Ley Orgánica 1/2014, se incluiría, en su apartado k) el delito conocido como "grooming". La Ley 1/2014, de justicia universal es anterior a la reforma efectuada en el Código Penal por la Ley Orgánica 1/2015, donde se introducen esa modalidad delictiva dado el avance de las nuevas tecnologías, por ello, dentro de los delitos contra la libertad e indemnidad sexual debe incluirse la modalidad especificada en el artículo 183 ter del Código Penal.

En cambio, en relación con el delito de "sexting" encuadrado dentro del Título X del Código Penal que regula los delitos contra la intimidad, el derecho a la propia imagen, la inviolabilidad del domicilio, en concreto, dentro del Capítulo I, "Del descubrimiento y revelación de secretos", artículo 197 del CP, no se hace referencia a él en el artículo 23 apartado 4 de la LOPJ. Por tanto, la competencia para que conozca la jurisdicción española se atribuye en los apartados 1 y 2 del mismo artículo 23 conforme a los siguientes criterios:

"1. En el orden penal corresponderá la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en que España sea parte.

2. También conocerá la jurisdicción española de los delitos que hayan sido cometidos fuera del territorio nacional, siempre que los criminalmente responsables fueren españoles o extranjeros que hubieran adquirido la nacionalidad española con posterioridad a la comisión del hecho y concurrieren los siguientes requisitos:

a) Que el hecho sea punible en el lugar de ejecución, salvo que, en virtud de un Tratado internacional o de un acto normativo de una Organización internacional de la que España sea parte, no resulte necesario dicho requisito, sin perjuicio de lo dispuesto en los apartados siguientes.

b) Que el agraviado o el Ministerio Fiscal interpongan querella ante los Tribunales españoles.

c) Que el delincuente no haya sido absuelto, indultado o penado en el extranjero, o, en este último caso, no haya cumplido la condena. Si sólo la hubiere cumplido en parte, se le tendrá en cuenta para rebajarle proporcionalmente la que le corresponda".

h. La creación de nuevas herramientas o instrumentos para la investigación, persecución y enjuiciamiento de los autores de los hechos delictivos

La aparición de estas nuevas figuras delictivas cometidas a través de la red conlleva necesariamente la creación de nuevas herramientas que posibiliten la investigación y seguimiento de los autores de esos delitos. Los delincuentes han aprovechado la facilidad del uso de las nuevas tecnologías para la comisión de hechos delictivos y ello ha supuesto que se hayan generado nuevas herramientas también digitales para la lucha de esa nueva criminalidad.

Sin embargo, no es correlativa la facilidad del uso de las nuevas tecnologías con la facilidad de la averiguación de los delitos cometidos a través de las redes. Al contrario, cuanto más fácil es el uso de las nuevas tecnologías de la información y comunicación más difícil es el descubrimiento de los hechos cometidos *on line*. Además de necesitar instrumentos legales suficientes son necesarios conocimientos técnicos, forenses especializados y procedimientos adecuados para conseguir averiguar al autor y las condiciones de su comisión. Precisamente por ello, dentro de las Fuerzas y Cuerpos de Seguridad del Estado se han creado dotaciones específicas para llevar a cabo tal función, cuerpos especializados en nuevas tecnologías con los recursos materiales apropiados para la persecución y resolución de los delitos con esas características[189]. Ade-

189 Dentro de la Unidad Central Operativa de la Guardia Civil, se creó el Grupo de Delitos telemáticos precisamente para investigar todos aquellos delitos que se cometen a través de Internet. Hay que remontarse al año 1996, cuando se constituyó el Grupo de Delitos Informáticos (GDI) para atender a las denuncias que hasta entonces no eran muchas por los llamados delitos informáticos. Como se indica en la página de la Guardia Civil "su buen hacer y el crecimiento exponencial de usuarios de la red, propiciaron el crecimiento del grupo, que pasó a llamarse Departamento de Delitos de Alta Tecnología (DDAT), asumiendo como nueva competencia el fraude en el sector de las telecomunicaciones. Con la socialización de Internet y el crecimiento de los hechos delictivos, se amplía el abanico de competencias de investigación, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como el cibercrimen. Posteriormente, el departamento cambia de nombre por el actual, Grupo de Delitos Telemáticos (GDT). Estos cambios se acompañaron de la creación de los

más, también dentro de la estructura del Ministerio Fiscal se han creado fiscales especializados en criminalidad informática[190].

Muchas de estas medidas han sido incorporadas por primera vez a nuestro Ordenamiento por la LO 13/2015 como medidas de investigación tecnológica, precisamente con la finalidad de investigar la comisión de hechos delictivos[191], por tanto, la regulación legal de estas medidas de investigación refuerza la seguridad jurídica que se necesita en la obtención de la prueba electrónica. Pero además el Derecho penal tiene que actuar no sólo frente a la comisión del delito, sino antes de ello impedirlo, de forma que junto con la función de represión que tiene el Derecho penal se asigna al sistema de justicia criminal una función de carácter anticipativo[192]. El Derecho penal ya no sólo se utiliza como reacción ante el delito sino como prevención al mismo. Se produce, por una parte, un adelantamiento en la intervención punitiva que pasa a guiarse

---

Equipos de Investigación Tecnológica (EDITE,s) en cada uno de las provincias de España", véase https://www.gdt.guardiacivil.es/webgdt/la_unidad.php.

Por lo que respecta al Cuerpo de Policía Nacional, dentro de la estructura de la Dirección General de la Policía se ha creado la Unidad de Investigación Tecnológica (UIT). Esta nueva Unidad dentro de la Comisaría General de Policía Judicial se dirige a reforzar la presencia de la Policía Nacional en este escenario virtual en el que se difuminan las fronteras.

La Unidad de Investigación Tecnológica (UIT) actúa como Centro de Prevención y Respuesta E-Crime de la Policía Nacional y cuenta con dos brigadas: la Brigada Central de Investigación Tecnológica y la Brigada Central de Seguridad Informática. Véase en https://www.ccn-cert.cni.es/g

190 Véase la Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías, en https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-I-2011-00002.pdf

191 La Fiscalía General del Estado ha publicado un conjunto de cinco circulares relativas a todas las medidas de investigación tecnológica: 1) Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal; 2) Circular 2/2019, sobre interceptación de comunicaciones telefónicas y telemáticas; 3) Circular 3/2019, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; 4) Circular 4/2019, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; 5) Circular 5/2019, sobre registro de dispositivos y equipos informáticos.

192 Véase a LÓPEZ ORTEGA, Juan José y ALCOCEBA GIL, Juan Manuel, "Prevenir y evitar: consideraciones en torno a un modelo de intervención penal anticipativa", en *Derechos del condenado y necesidad de pena*, (Obra Colectiva: Carmen Juanatey Dorado (dir.), y Natalia Sánchez-Moraleda Vilches (dir)), Aranzadi Thomson Reuters, 2018, pág. 90.

por criterios estratégicos dirigidos a la neutralización de riesgos y, por otra parte, se incorporan al proceso no sólo las herramientas para llevarlo a cabo sino también la metodología propia de los servicios de inteligencia basada en la recolección de información[193], y es precisamente aquí donde las nuevas tecnologías cobran verdadero protagonismo[194].

La lucha contra la criminalidad organizada está en el origen de la transformación del modelo de proceso penal, la finalidad de la investigación penal se modifica precisamente para perseguir las conductas delictivas de estructuras organizadas, la necesidad de obtener información subrepticia y en secreto se abre paso en el proceso penal y se empiezan a utilizar herramientas hasta entonces desconocidas, como son el agente encubierto o la prueba pericial de inteligencia, dentro del proceso penal, o fuera de este, el ciberpatrullaje, como habituales. Por tanto, se amplían las funciones a los servicios de inteligencia para reprimir el crimen organizado.

Pero junto con la lucha contra la criminalidad organizada la aparición de nuevos delitos, como el "sexting", el "grooming", "satalking", entre otros, surgidos como consecuencia del fenómeno tecnológico ha supuesto que se abra un nuevo método de investigación donde la utilización de las nuevas tecnologías desempeña un papel fundamental en la averiguación de la comisión de estos hechos delictivos.

---

193 LÓPEZ ORTEGA, Juan José y ALCOCEBA GIL, Juan Manuel, "Prevenir y evitar: consideraciones en torno a un modelo de intervención…, op. cit. págs. 90 y 91.

194 Señala LÓPEZ ORTEGA, Juan José y ALCOCEBA GIL, Juan Manuel, "Prevenir y evitar…", op. cit., pág. 91, que "la tecnológica se convierte en el medio posibilitador de la evitación. En este sentido, la acumulación y tratamiento automatizado de la información obrante en bases de datos y, mas recientemente, el uso de algoritmos basados en el Big data como mecanismo predictivo, son claros ejemplos del paralelismo existente entre el surgimiento de la evitación del delito como principal finalidad del sistema de justicia criminal y la revolución tecnológica".

Señala DELGADO MARTÍN, Joaquín, "Protección de datos personales en el proceso penal (II), en ELDERECHO.COM, Tribuna, 30-4-2019, que "nos encontramos con el llamado *big data*, que puede definirse como aquel conjunto de nuevas tecnologías que permiten analizar ágilmente, a través del uso extenso de algoritmos, cantidades masivas de datos provenientes de fuentes dispares con el objetivo de crear valor. Su rasgo esencial radica en que el análisis y tratamiento de enormes cantidades de datos permite comprender elementos que no se pueden abordar con el análisis de cantidades reducidas de información".

h.1 Ámbito nacional

1. El ciberpatrullaje

Hasta no hace mucho tiempo era habitual hablar de que la policía estaba patrullando las calles, sin embargo, en la actualidad, dadas las nuevas figuras delictivas que han surgido precisamente por la aparición de las nuevas tecnologías de la información, se suele hablar del ciberpatrullaje para referirnos al patrullaje que se hace en la red como prevención del delito. Como se ha señalado, "*si en un primer momento el medio de investigación por excelencia era la vigilancia física, característico de una concepción pretecnológica de la investigación criminal, pronto se completará con la vigilancia de las comunicaciones*"[195]. Ello como medida de investigación dentro del proceso penal pero también se van a utilizar herramientas propias de las Fuerzas y Cuerpos de Seguridad del Estado para prevenir la comisión de los delitos precisamente para evitar que se incoe un proceso penal.

Como es bien sabido, la posibilidad de obtener ingente o masiva información a través de las redes posibilita a su vez que la policía sea capaz de generar inteligencia ya que con todos los datos obtenidos se pueden extraer patrones de conducta delictiva con anterioridad a la comisión de los hechos. En definitiva, es posible a través de esos patrones de conducta predecir los actos delictivos y posibilita neutralizar el riesgo con el fin de garantizar la seguridad. La seguridad juega un importante papel en la actual política criminal, fundamentalmente a partir de los atentados yihadistas del 11 de septiembre de 2001 en Nueva York, tal es así, que un sector doctrinal ha llegado a reconocer la existencia de un derecho fundamental a la seguridad con nuevos perfiles, como derecho de nuevo cuño del que gozaría toda persona consistente en que los poderes públicos actúen con diligencia para prevenir grandes riesgos[196].

La acción policial a través de Internet busca garantizar la seguridad y evitar la alarma social que pueden provocar las diferentes conductas delictivas, es este sentido, muchas de las conductas que ahora están criminalizadas ya eran objeto de persecución policial a través de las redes con anterioridad a su tipificación penal, en especial en materia de pornografía infantil. En este ámbito lo que se perseguía fundamentalmente era evitar la creación de material

195 LÓPEZ ORTEGA, J.J. y ALCOCEBA GIL, J.M., "Prevenir y evitar…", op. cit., pág. 95.

196 Véase LÓPEZ ORTEGA, J.J. y ALCOCEBA GIL, J.M., "Prevenir y evitar…", op. cit., pág. 104.

pornográfico infantil. De hecho, ya en 1995 el Cuerpo Nacional de Policía creó el Grupo de Delitos informáticos y en 1996 se estableció el Grupo de delitos telemáticos por parte de la Guardia Civil y a medida que las comunidades autónomas fueron asumiendo competencias en esta materia fueron creando sus propios grupos. Además, dentro del propio Cuerpo de Policía Nacional se han creado grupos especializados periféricos que actúan de manera coordinada, fomentando y desarrollando herramientas conjuntas de inteligencia y análisis.

Es evidente que este fenómeno adquiere características y consecuencias completamente nuevas y conlleva una atención y tratamiento policial que necesariamente pasa por el uso de estructuras de cooperación internacional eficaces[197], puesto que Internet traspasa fronteras con una facilidad abismal. La mayoría de las acciones, fundamentalmente dentro del crimen organizado, tienen una proyección internacional.

En este sentido, el ciberpatrullaje, consistente en un rastreo en la red, permite la investigación del tráfico delictivo, visto potencialmente, es decir, se utiliza para prevenir conductas delictivas, no tanto para la investigación de los hechos delictivos. La actuación policial a través del ciberpatrullaje se sitúa en los lugares abiertos de Internet, lugares públicos, por lo que no necesita autorización judicial que le habilite a rastrear la Red. Es lo que se conoce por el acrónimo anglosajón OSINT (Open Source Intelligent). Sin embargo, precisamente esta limitación en los lugares en los que puede rastrear conlleva que muchas de las veces la labor policial sea infructuosa especialmente en los delitos de pornografía infantil en los que existen grupos cerrados de usuarios en los que se transmiten material pornográfico infantil que es de difícil acceso. Al no ser el ciberpatrullaje un medio de investigación, se encuentra limitado en su actuación a los lugares abiertos, por ello, esta frontera infranqueable por el rastreo policial puede ser franqueada por el agente encubierto virtual o informático[198], como veremos, diligencia de investigación prevista en el proceso penal.

197 LÓPEZ, Antonio, "La investigación policial en Internet: estructuras de cooperación internacional", en *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, Número 5 (2007) I ISSN 1699-8154, pág. 66. Véase en http://idp.uoc.edu.

198 CAROU GARCÍA, Sara, "El agente encubierto como instrumento de lucha contra la pornografía infantil en Internet. El guardián al otro lado del espejo", en *Cuadernos de la Guardia Civil*, nº 56, 2018, pág. 27.

Así, la Policía puede rastrear la Red si es un canal de comunicación abierto, es decir, es público, por tanto, estaría legitimado sólo con la habilitación legal sin necesidad de ningún otro requisito adicional. Esta facultad de rastreo estaría comprendida dentro de las facultades atribuidas por la Ley de Fuerzas y Cuerpos de Seguridad del Estado (artículo 11) y por el artículo 282 de la LECRim[199].

Por ejemplo, la Policía puede rastrear sin necesidad de autorización judicial que le habilite para ello la red P2P (Peer to Peer). Es una de las redes más importantes y utilizadas de intercambio de todo tipo de material entre usuarios de Internet, independientemente de la plataforma de software utilizada ni el lugar o momento en que se encuentren. Esta red de intercambio de archivos puede ser rastreada por la Policía sin necesidad de autorización judicial puesto que es abierta. Como señala ZARAGOZA TEJADA, "es decir utilización de sistemas de rastreo que debidamente programados y a partir de voces o de conceptos realizan búsquedas en foros abiertos"[200]. En este sentido, el Tribunal Supremo ha afirmado sobre la validez de los rastreos informáticos policiales sin autorización judicial que "quien utiliza un programa P2P, en nuestro caso EMULE, asume que muchos de los datos se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos públicos en internet, no se hallaban protegidos por el art. 18-1º ni por el 18-3 C.E" [201].

---

199 Como refleja la jurisprudencia "el derecho comparado muestra modalidades muy diversas de regulación. Doctrinalmente, se diferencia entre lo que se conoce como *ciber patrulleo* (el agente realiza exploraciones o indagaciones por canales abiertos de comunicación) y el estricto agente encubierto *online* que opera en canales cerrados. Solo en este segundo caso la legislación reformada en 2015 requiere autorización judicial, lo que no inexorablemente habría de proyectarse a casos como el ahora examinado en que no estamos ante una infiltración policial en la red, sino ante el uso por la policía del canal creado por quien ha sido detenido, valiéndose de su *nickname*", véase la STS de 11 de abril de 2018, núm. 173/2018, en *Tirant on line*, DOCUMENTO TOL6.586.812.

200 Véase "El agente encubierto "online: la última frontera de la investigación penal", en *Revista Aranzadi Doctrinal*, nº 1, 2017, pág. 7.

201 STS 236/2008, de 9 de mayo, en Tirant on line, DOCUMENTO TOL1.320.850. El Tribunal Supremo ha manifestado que "los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet Protocols) que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. 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

En este supuesto resuelto por el Tribunal Supremo en el que el objeto a enjuiciar eran delitos de pornografía infantil, una de las diligencias tenía como finalidad descubrir a los usuarios que descargaban o compartían archivos con contenido pornográfico de menores para ello se llevaron a cabo los correspondientes rastreos policiales sin autorización judicial. El resultado de estos rastreos fue un listado de IPS, claves de acceso que los proveedores de servicios de Internet asignan a cada ordenador en el momento en el que se conecta a Internet, lo que permite identificar de forma indubitada a través de dichos proveedores el número de telefono desde el que se produce la conexión. Ello es posible sin autorización judicial.

Dentro de los proveedores de Internet (ISP) hay que diferenciar entre los proveedores de acceso y los proveedores de servicios[202]. Entre los primeros se encuentran las compañías que proporcionan el acceso a Internet que habitualmente suelen ser operadoras de telecomunicaciones, como son Movistar, Orange, Vodafone, etc., mientras que entre los segundos se encuentran las empresas que ofrecen ciertos servicios de uso común como por ejemplo el correo electrónico, con son Hotmail, Gmail, etc.; redes sociales como Twitter, Facebook; almacenamiento de archivos como Dropbox, Googledrive; publicación de videos y fotos como Youtube, Panoramio, flickr o; mensajerías como whatsApp, Line, etc[203].

Dentro de las técnicas que la Policía puede utilizar está la del "hacking legal" o intrusismo informático que sirve para introducirse en el disco duro sin alterar los archivos que este contenga. Tradicionalmente lo que se hacía era descubrir las medidas de seguridad que usaba el usuario, tales como las cla-

---

huella de la entrada - como puntualiza con razón el Mº Fiscal- queda registrada siempre y ello lo sabe el usuario".

202 El término "proveedores de servicios" está definido en el Informe explicativo del Convenio de Ciberdelincuencia de Budapest abarcando a una amplia categoría de personas que desempeñan un papel particular con respecto a la comunicación o el tratamiento de los datos a través de los sistemas informáticos. En el numero i) de la definición, se aclara que quedan comprendidas todas las entidades tanto públicas como privadas que ofrecen a los usuarios la posibilidad de comunicarse entre sí, ya sea que ofrezcan su servicio gratuitamente o a cambio de un arancel. En el numero ii) de la definición se aclara que el término "proveedor de servicios" abarca también a aquellas entidades que procesen o almacenen datos en nombre de las personas mencionadas en el inciso i y para los usuarios. En este concepto se incluyen ambas definiciones, véase en https://rm.coe.int/16802fa403.

203 Véase a QUEVEDO GONZÁLEZ, Josefina, *Investigación y prueba del ciberdelito*, op. cit., pág. 125.

ves de acceso, contraseñas, o passwords, para poder acceder a la información, sin embargo, dado el gran avance que están teniendo las nuevas tecnologías, actualmente existen programas para interceptar las comunicaciones, denominados e-blasters, o programas para grabar esas comunicaciones y reproducirlas en otro ordenador (keyloggers)[204].

Otra técnica que pueden utilizar es la de *sniffers* o programas de rastreo informático que filtran toda la información que circula por un sistema, recogiendo aquella que le interesa, como claves y contraseñas, y enviándola seguidamente a aquella persona que colocó el *sniffer*[205]. Esta técnica permite interceptar los correos electrónicos del delincuente y su grabación automática en el disco duro de un ordenador habilitado para este fin[206].

Otra técnica es la del *cracker* o *cracking*, que simplemente podemos denominar como piratería informática, en la que el sujeto activo se dedica a realizar copias no consentidas de programas informáticos[207].

Pues bien, conforme a la LECrim si los agentes de la Policía Judicial en el ejercicio de las funciones de prevención y/o descubrimiento de los delitos cometidos en Internet tienen acceso a una dirección IP que estuviera siendo utilizada para la comisión de algún delito y no constara la identificación y localización del equipo o dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, de acuerdo al artículo 588 ter k de la LECrim, deberán solicitar del juez de instrucción que requiera a los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

2. El agente encubierto informático o virtual

La nueva forma de actuar de los criminales ha llevado a que los Cuerpos y Fuerzas de Seguridad del Estado tengan que estar permanentemente en alerta, vigilantes, para intentar atajar estos fenómenos. En la consecución de este

204 PÉREZ ESTRADA, Miren Josune, "La investigación del delito a través de las nuevas tecnologías. Nuevos medios de investigación en el proceso penal", (dir. DE LA CUESTA ARZAMENDI), en *Derecho Penal informático*, Thomson Reuters, 2010, pág. 314.

205 Véase a DEL ROSAL BLASCO*, Criminalidad organizada y nuevas tecnologías: algunas consideraciones fenomenológicas y político-criminales*, 2001, en Tirant on line, Documento TOL163.240.

206 ALONSO, Adolfo, "La investigación policial de los delitos…", op. cit., pág. 61.

207 Ibídem.

objetivo, cada vez más preocupante por el avance de las nuevas tecnologías, es necesario, como se indica en el Estudio sobre la Ciberdelincuencia ya citado, la conjunción tanto de una cualificada preparación como la dotación de herramientas legales y materiales, con la finalidad de llevar a cabo la detección de estos tipos de conductas. En este sentido, la figura del agente encubierto informático o virtual se erige como una nueva herramienta para responder a la criminalidad, figura legal que fue aprobada tras la reforma de la Ley de Enjuiciamiento Criminal en el año 2015 (art. 282 bis apartado 6 LEC), como medida de investigación delictiva.

Es la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la ley de Enjuiciamiento Criminal la que regula en el apartado 6 del artículo 282 bis de la Ley de Enjuiciamiento Criminal la figura del agente encubierto informático o virtual. En este apartado se indica literalmente que:

"*El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.*

El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos"[208].

208 En STS de 13/03/2019, DOCUMENTO TOL7.118.521, el Tribunal Supremo indica que: "*La reforma de LO 13/2015 ha introducido los apartados 6 y 7 del art. 282 de la LECrim. El apartado 6 introduce la novedosa figura del agente encubierto informático, tratando el legislador, una vez más, de adaptar el texto legal a la sociedad digitalizada en la que nos encontramos inmersos. Su previsión se ve enfocada a la investigación de los delitos llevados a cabo por la delincuencia organizada dispuestos en el apartado 4, antes mencionados; de los designados en el art. 579 LECrim,, a saber, delitos de terrorismo, delitos cometidos en el seno de una organización criminal o delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; o cualquier otro delito cometido a través de medios informáticos. Además, se prevé que este agente encubierto podrá intercambiar o enviar archivos ilícitos, por razón de su contenido, para poder conseguir con ello algoritmos que le permitan conocer la identificación del investigado, siempre contando con la autorización judicial pertinente.*

Por último, el apartado 7 regula la posibilidad de que el agente pueda filmar imágenes y grabar las conversaciones que éste mantenga con el investigado, incluso si se desarrollan en el interior de un domicilio. Para ello y en todo caso, el agente deberá contar con una autorización previa otorgada por el Juez competente. Esta posibilidad podría quedar amparada por el art. 282 bis 3 LECrim., en el cual se prevé que cuando las actua-

Esta figura se presenta como una técnica de investigación utilizada por la Policía Judicial a medio camino entre la infiltración física policial y la intervención de las comunicaciones telemáticas. Una de las diferencias con el ciberpatrullaje es que a través de esta técnica de investigación la Policía puede acceder tanto a canales abiertos como cerrados de Internet. En este sentido, sólo cuando se trate de actuación en canales cerrados, se precisa la condición de agente encubierto informático o virtual. Al ser un medio de investigación con autorización judicial es posible acceder a lugares cerrados de comunicación, de difícil acceso. Si bien, antes de la infiltración la Policía lleva a cabo a través de los servicios de inteligencias estudios y análisis previos que aseguren el éxito de la investigación[209].

En este sentido, el agente se infiltra en la Red bajo una identidad falsa que le permite acceder a los grupos cerrados de criminales con la finalidad de tener relación de confianza con alguno de ellos con el propósito final de que le inviten a integrar esas comunidades virtuales delictivas. Los dos medios de investigación son perfectamente compatibles. A este respecto, señala el Tribunal Supremo que: "*La actuación del agente encubierto con la oportuna autorización judicial es una medida apta y hábil en estos casos para conseguir la información de la autoría, no siendo un delito provocado en modo alguno, sino una medida reconocida legalmente para la obtención de pruebas con respecto a los hechos que son objeto de investigación, y en donde, al igual que en las medidas de limitación de derechos fundamentales se llega a un punto en la investigación en donde ya no se puede continuar, precisando la introducción de medidas de investigación, como la del agente encubierto, para acceder a esa información de la que no podría accederse de otra manera; y más en circuitos informáticos de comunicación cerrados que requieren de claves o accesos de amistad entre los partícipes. La intervención del agente encubierto no provoca en estos casos el delito, sino que el delito ya se ha cometido, o se está cometiendo, y la actuación del agente lo que hace es conseguir pruebas acerca de la comisión del delito, pero no provoca que el delito se cometa; de ahí, su legitimidad de intervención*"[210].

---

ciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las correspondientes autorizaciones".

209 Véase a este respecto a ZAFRA ESPINOSA DE LOS MONTEROS, Rocío, "El ciberagente en la lucha de la pornografía infantil", en *Libro Homenaje al profesor MARTÍN OSTOS*, pág. 1974.

210 STS de 7 de febrero de 2019, núm. 65/2019, en Tirant on line, DOCUMENTO TOL7.059.509.

Es importante saber en qué consisten los lugares abiertos o cerrados de comunicación, puesto que la ley no establece o define qué se entiende por canales cerrados de comunicación. El Tribunal Supremo ha indicado que se "*caracterizan por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación*"[211], por tanto, la característica es precisamente la ocultación a terceros de lo comunicado, y por ende, sólo es posible que el tercero lo conozca si es aceptado por el comunicante.

Sin entrar en profundidad a estudiar la figura del agente encubierto virtual, quisiera apuntar algunas cuestiones relevantes para nuestro estudio[212]. En este sentido, esta técnica de investigación sólo sería viable para determinados delitos, que como veremos es mucho más amplia que la lista de delitos en los cuales puede investigar el agente encubierto físico. Así, de acuerdo al apartado 4 del mismo artículo 282 bis de la LECrim comprendería los siguientes delitos:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.

e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.

f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.

g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.

h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.

i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.

---

211 STS 249/2008, de 20 de mayo, RJ 2008/4387. En https://vlex.es/vid/drogas-penas-complice-368-369-6-40562210.

212 Para una mayor profundización sobre las características del agente encubierto virtual véase a ZAFRA ESPINOSA DE LOS MONTEROS, Rocío, "El ciberagente en la lucha de la pornografía infantil", op. cit., págs. 1975 a 1982.

j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.

k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.

n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.

o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.

Además, de acuerdo al artículo 588 ter a de la LECrim: "*La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*"[213].

En el artículo 579.1 de la LECrim, a su vez, se contemplan:

1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2.º Delitos cometidos en el seno de un grupo u organización criminal.

3.º Delitos de terrorismo.

En relación con estos delitos, tanto los del art. 579.1 de la LECrim como los delitos cometidos a través de instrumentos informáticos o de cualquier otra

213 La Ley Orgánica 13/2015 opta por un sistema mixto a la hora de determinar los delitos cuya concurrencia estima necesaria para que el órgano jurisdiccional pueda autorizar la medida. Por un lado, la referencia a un criterio cuantitativo: el límite máximo de la pena prevista para el delito doloso investigado deberá ser de al menos tres años de prisión. Por otro lado, el legislador parece recurrir -aunque solo de forma muy genérica, sin especificar tipos penales concretos incluidos en el Código penal- a un criterio cualitativo o de listado, que es lo que ocurre cuando alude a los delitos cometidos en el seno de un grupo u organización criminal, delitos de terrorismo y, específicamente para la intervenciones telefónicas y telemáticas, los delitos cometidos a través de instrumentos informáticos o de tecnologías de la información o comunicación. Véase GONZÁLEZ, NAVARRO, Alicia, *El proceso penal. Cuestiones fundamentales,* (coord. FUENTES SORIANO, Olga)*,* 2017, en Tirant on line, DOCUMENTO TOL6.080.359.

tecnología de la información o la comunicación o servicio de comunicación, señala la doctrina que "aunque en principio una interpretación excesivamente literal de ambos preceptos permitiría inferir que podría autorizarse este tipo de medidas para la investigación de cualquier delito cometido a través de las nuevas tecnologías, es razonable entender que en atención a los bienes jurídicos en juego y a los derechos que pueden quedar afectados con la decisión sobre la utilización del agente encubierto han de ponderarse criterios como la especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad a los que se hace expresa referencia en el art. 588 ter a de la Ley de Enjuiciamiento Criminal (...). De seguirse la interpretación contraria, podría darse cabida a la utilización del agente encubierto en la investigación de delitos de poca gravedad o con poca trascendencia social, como delitos leves de estafa cometidos a través de internet o coacciones cometidas a través de las redes sociales lo que puede resultar en algunos casos absolutamente desproporcionado teniendo en cuenta los derechos e intereses en juego"[214].

Por tanto, el apartado 6 del artículo 282 bis de la LECrim permite utilizar esta técnica de investigación en los delitos apuntados sin necesidad de que se comentan dentro de una organización criminal, como necesariamente ha de darse en la figura del agente encubierto físico.

Si las Fuerzas y Cuerpos de Seguridad del Estado entienden que es necesario para la investigación de los delitos infiltrar en las redes a un agente virtualmente solicitarán al órgano judicial su autorización. La autorización es exclusividad judicial sin posibilidad de otorgarla el Ministerio Fiscal. Esta autorización judicial es necesaria puesto que la infiltración policial virtual supone una injerencia en los derechos fundamentales de las personas inmersas en la investigación, fundamentalmente, el derecho al secreto de las comunicaciones. Por tanto, en el auto se debe hacer constar los requisitos contenidos en el artículo 588 bis c de la LECrim para la interceptación de las comunicaciones telemáticas.

En concreto, en el auto el juez debe motivar:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La extensión de la medida de injerencia, especificando su alcance, así

214 ZARAGOZA TEJADA J. I., "El agente encubierto "online: la última frontera de la investigación...", op. cit., págs. 6 y 7.

como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.

d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.

e) La duración de la medida.

f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

g) La finalidad perseguida con la medida.

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

Quisiera resaltar en relación con la identidad de los investigados y de cualquier otro afectado por la medida, que la misma se plantea difícil de conocer en el momento de autorizar la infiltración. Es posible que el agente lleve operando en la Red con un alias, por lo que es difícil saber la identidad real. En este sentido, la doctrina viene interpretando el concepto de identidad en sentido amplio, considerando que sería suficiente con la indicación del Nick con el que el investigado opera en la Red[215].

Por otro lado, en relación con la necesidad de auto judicial, que es insoslayable[216], se ha propugnado que, en casos excepcionales, en casos de urgencia y para supuestos de averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas, no se exija desde el inicio la autorización para interceptar las comunicaciones, puesto que de otra forma es difícil que dé fruto la investigación llevada a cabo por el agente de las Fuerzas y Cuerpos de Seguridad del Estado[217]. Una de las características de la Ciberdelincuencia precisamente es la volatilidad y facilidad de manipular los datos en la Red, por tanto, para luchar contra ella es necesario que la actuación de la Policía sea lo más rápida y flexible posible. En este sentido, es preciso que la actuación llevada a cabo por el agente infiltrado durante la investigación, pueda dar fruto en el acto del juicio oral, es decir, es necesario que pueda ser llevada al juicio como material probatorio y, para ello, es imprescindible que

215 CAROU GRACÍA, Sara, "El agente encubierto como instrumento de lucha contra la pornografía infantil en Internet", op. cit., pág. 30.

216 El Tribunal Supremo en la STS de 11 de abril de 2018, DOCUMENTO TOL6.586.812, ha manifestado que: "*No es una exigencia necesariamente constitucional. Se mueve más bien en el plano de la legalidad y no es universal en el sentido de que no se exige para cualquier actividad de investigación policial en la red*".

217 Ibídem.

las actuaciones llevadas a cabo antes de la autorización judicial sean consideradas válidas[218]. La figura del agente encubierto tiene precisamente de especialidad que de su actuación se generen unos vínculos de confianza con los delincuentes que sirvan precisamente para penetrar y descubrir el entramado delictivo descubriendo pruebas.

En este sentido, el Tribunal Supremo ha señalado que: "*Por las defensas se alega que este contacto previo, que consideramos irrelevante a los efectos de la validez de la prueba practicada, cobra especial importancia porque quieren vincularlo a que es el mismo agente quien intervino. Y éste, cuando declara como testigo, indica que solo interviene una vez tiene la autorización. La Sala concluye que esto no es determinante, si el primer contacto fue con la persona que luego fue agente encubierto, u otro policía, el que hizo ese contacto, o lo mantenía, o fue a través de confidentes, queda en el ámbito del actuar policial, y lo que se acredita por la prueba es que la concreción de las actuaciones del agente Bucanero, el método de contacto mediante la cuenta de correo, lo que de él esperan, lo que quieren del mismo, el precio que cobrara y como lo cobrara, lo fijan en las reuniones que se tienen una vez que ya está vigente el decreto. No puede considerarse esencial que el instructor en la declaración del juicio no haya sido más preciso en cuanto a quien concretamente se reunió antes de que se autorizara el agente encubierto.*

Lo que importa es que una vez que se dan las informaciones mínimamente consistentes, la policía actúa correctamente solicitando la autorización

218 El Tribunal Supremo en la STS de 5 de abril de 2017, núm. 250/2017, citada anteriormente, a este respecto ha declarado que: "*Como dice la STS 575/2013, de 28 de junio, la existencia de un contacto previo entre el recurrente y el agente encubierto, enmarcados en una relación derivada de las labores de prevención y captación de información propias de las Fuerzas y Cuerpos de Seguridad, en modo alguno conlleva una infracción de alcance constitucional. Carecería de sentido, con el fin de sostener la validez de la diligencia de prueba, la exigencia de que la autorización del agente encubierto se produzca a ciegas, con exclusión de cualquier contacto previo entre la persona que va a infiltrarse en la organización y quienes aparecen como miembros sospechosos de una red delictiva. Es contrario a elementales máximas de experiencia concebir la infiltración en un grupo criminal como la respuesta a una invitación formal a un tercero que, de forma inesperada, curiosea entre los preparativos de una gran operación delictiva. La autorización judicial, por sí sola, no abre ninguna puerta al entramado delictivo que quiere ser objeto de investigación. Antes al contrario, la cerraría de forma irreversible.*

De ahí que esa resolución tiene que producirse en el momento adecuado que, como es lógico, no tiene por qué ser ajeno a una relación previa que contribuya a asentar los lazos de confianza".

para intervenir. El propio " Bucanero" (agente encubierto de la GC) declara en el juicio que no se reunió antes con los investigados, pero, repetimos, ello en nada modifica el fondo del asunto, un aspecto es obtener y trabajar una información a través de la confidencia o los contactos, otro involucrarse en las actuaciones que para lo que se necesita la autorización"[219].

Además, hay que tener en cuenta que el ciberdelito no tiene fronteras físicas ello supone sino la mayor dificultad para poder obtener prueba de esos delitos, sí, una de ellas, por ello, ya desde el Convenio de Ciberdelincuencia de 2001 se introducen modalidades específicas de asistencia judicial dadas las características propias del fenómeno del cibercrimen, así como de la prueba electrónica relacionada con el resto de tipologías delictivas. La finalidad principal del Convenio es establecer una política penal común para proteger a la sociedad de la ciberdelincuencia configurando una legislación adecuada y reforzando la cooperación internacional. En concreto en los artículos 29, 30, 31, 32, 33 y 34 correlativamente del citado Convenio se habla de la preservación urgente de datos informáticos almacenados (art. 29); revelación urgente de datos de tráfico almacenados (art. 30); asistencia mutua en relación con el acceso a datos almacenados (art. 31); acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público (art. 32); asistencia mutua para la obtención en tiempo real de datos relativos al tráfico (art. 33); asistencia mutua en relación con la interceptación de datos relativos al contenido (art. 34); o creación de una red de puntos de contactos permanente[220]; etc[221]. Alguna de las disposiciones contenidas en el Convenio van dirigidas a el establecimiento de una serie de condiciones y salvaguardias con la finalidad de que cada estado parte se asegure de que los actos que se regulan en el Convenio y que están dirigidos a la obtención de evidencia digital respeten los preseupuestos y requisitos previstos en su ordenamiento jurídico interno, garantizando de esta forma los derechos y libertades de los investigados reconocidos precisamente en el CEDH y en el PIDCP así como

219 STS de 26 de noviembre de 2018, 591/2018, en Tirant on line, DOCUMENTO TOL6.940.627.

220 En España, de acuerdo al Instrumento de ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest, concretamente el artículo 35 del Convenio, se declara que la autoridad central designada es la Comisaría General de Policía Judicial del Ministerio del Interior. En https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221.

221 Véase sobre ello, a SÁNCHEZ SISCART, José Manuel, "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU.", en *Revista del Poder Judicial*, número 91, año 2011, págs. 33 a 37.

en otros tratados internacionales partiendo del cumplimiento del principio de proporcionalidad[222].

En relación con la naturaleza de esta prueba elaborada por la Policía, en concreto el informe de inteligencia, se incluye dentro de la categoría mixta de pericial/testifical. Así, el Tribunal Supremo ha manifestado en una reciente sentencia, donde recoge el tratamiento que se le da a este tipo de pruebas, y sobre el cual no existe objeción a su admisión ni valoración, que: "*cabe entender que dichos informes sí incorporan razón de ciencia, pues sus autores, en cuanto tienen una larga experiencia adquirida durante los muchos años de investigación de las Fuerzas de Seguridad, en el transcurso de los cuales han ido acumulando datos sobre el funcionamiento del crimen organizado y sus miembros, pueden ser calificados como peritos*.

En este sentido se ha pronunciado esta Sala del Tribunal Supremo, en varias sentencias (SSTS de 31 de marzo de 2010; de 1 de octubre de 2010; de 29 de mayo de 2003; de 13 de diciembre de 2001 y de 17 de julio de 1998) señalando que "A este respecto debemos destacar nuestras sentencias..., que han declarado que tal prueba pericial de inteligencia policial cuya utilización en los supuestos de delincuencia organizada es cada vez más frecuente, está reconocida en nuestro sistema penal pues, en definitiva, no es más que una variante de la pericial a que se refieren tanto los arts. 456 LECrim como el 335 LEC, cuya finalidad no es otra que la de suministrar al Juzgado una serie de conocimientos técnicos, científicos, artísticos o prácticos cuya finalidad es fijar una realidad no constatable directamente por el Juez y que, obviamente, no es vinculante para él, sino que como el resto de probanzas, quedan sometidas a la valoración crítica, debidamente fundada en los términos del art. 741 LECrim .

La prueba pericial es una variante de las pruebas personales integrada por testimonios de conocimiento emitidos con tal carácter por especialistas del ramo correspondiente de más o menos alta calificación científica, para valorar por el Tribunal de instancia conforme a los arts. 741 y 632 LECrim y 117 CE. Dicho de otro modo: la prueba pericial es una prueba personal, pues el medio debe ser interrogado por la opinión o dictamen de una persona y al mismo tiempo, una prueba indirecta en tanto proporciona conocimientos técnicos para valorar los hechos controvertidos, pero no un conocimiento directo sobre cómo ocurrieron los hechos"[223].

---

222 Véase a RODRÍGUEZ RUBIO, Carmen, "Nuevas diligencias de investigación y de prueba: el registro...", op. cit., pág. 278.

223 STS de 7 de febrero de 2019, ya citada. El Tribunal Supremo en esta sentencia

Como expone el Tribunal Supremo, "*se trata de un medio probatorio que no está previsto en la Ley, siendo los autores de dichos informes personas expertas en esta clase de información que auxilian al Tribunal, aportando elementos interpretativos sobre datos objetivos que están en la causa, siendo lo importante si las conclusiones que extraen son racionales y pueden ser asumidas por el Tribunal, racionalmente expuestas y de forma contradictoria ante la Sala*"[224].

Finalmente, para concluir este apartado quisiera apuntar, tal y como se recoge en el *Estudio sobre la criminalidad informática del año 2018*, que en una de las operaciones realizadas el año pasado (se refiere al 2017), utilizando la figura del agente encubierto informático o virtual, se llegaron a detener a 19 personas por un presunto delito de tenencia y/o distribución de pornografía infantil. Las investigaciones comenzaron tras conocerse que, en determinados grupos cerrados o secretos de una conocida red social, se intercambiaban enlaces en los que, tras clicar en ellos, se accedía directamente a grupos de mensajería instantánea, que compartían abundantes archivos de pornografía infantil. Así, haciéndose pasar los agentes por usuarios normales, se averiguó

---

sigue indicando que "*Hay que destacar que tanto en delitos relacionados con terrorismo como en tráfico de drogas la articulación de la prueba Pericial de inteligencia ha sido configurada como pericial y testifical en razón a la duplicidad de quien así declara en juicio oral, ya que el agente policial que elabora el informe conoce del contenido de la materia y en consecuencia lo hace por sus conocimientos científicos, pero también actúa como testigo en razón de lo que sabe. Podría llegar a decirse que en estos casos la pericial de inteligencia se puede asemejar a la prueba del testigo-perito que fue incluida en la LEC en los artículos 370 y 380 por razón de la existencia de personas que podrían actuar en juicio de las dos maneras. En este sentido, la aplicación analógica nos permite llegar, frente a los detractores de considerar la pericial de inteligencia como una prueba mixta testifical/pericial, resolviendo el debate de las dudas que suscita su incardinación dentro del medio probatorio de la pericia en el proceso penal. De esta manera se le puede ubicar dentro de la prueba testifical sin olvidar la esencia de pericia de la que tampoco se puede olvidar su naturaleza en cuanto a que lo que el "testigo" declara lo es porque "lo sabe", y esto lo es por su preparación y conocimiento de este tipo de hechos, por lo que es preferible otorgarle un carácter mixto en orden a ubicarla dentro de los medios de prueba en el proceso penal. Así, se declara en la STS 1097/2011, de 25 de octubre, en la que tanto el MF como la propia Sala, reconocen la posibilidad de concurrencia en los funcionarios policiales que elaboran los informes de inteligencia de la doble condición de testigo, directo o de referencia, y perito, tal y como ocurre en los expertos en legislación fiscal o de aduana".*

224 Ibídem.

la existencia de estos grupos y se analizó que en varios de ellos se distribuía abundante pornografía infantil. En la operación se encontraron distintos números de teléfono localizados tanto en el territorio nacional como en el extranjero. A raíz de ello se llevó a cabo la operación, registrándose 20 domicilios situados en 14 localidades distintas y deteniéndose a 19 personas, como presuntos autores de un delito de tenencia y/o distribución de pornografía infantil[225].

En definitiva, como vemos, en la práctica la utilización de esta diligencia de investigación es bastante efectiva y los resultados son satisfactorios sobre todo en el descubrimiento de delitos cometidos a través de las redes. La preparación y profesionalidad de los agentes de la autoridad es pieza clave en la lucha o persecución de estos delitos cometidos en red, y fundamentalmente en la salvaguarda de los derechos de las víctimas especialmente vulnerables[226] en muchos de los delitos objeto de esta investigación, como son el delito de "sexting", "grooming", etc.

3. La interceptación de comunicaciones electrónicas o telemáticas

Otra de las diligencias de investigación previstas en nuestro Ordenamiento jurídico es la posibilidad de interceptar las comunicaciones cuando estas son electrónicas o telemáticas. Esta diligencia de investigación ha sido regulada también por primera vez en la Ley de Enjuiciamiento Criminal por la LO 13/2015.

Así, tras la reforma llevada a cabo por dicha LO 13/2015, se regula en el Capítulo V "La interceptación de las comunicaciones telefónicas y telemáticas". Este Capítulo está estructurado en tres Secciones: a) la Primera "Disposiciones Generales" que comprende los arts. 588 ter a) a 588 ter i); b) la Segunda "Incorporación al proceso de datos electrónicos de tráfico o asociados" que comprende el único artículo 588 ter j); y c) la Tercera "Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad"[227].

---

225 Véase www.interior.gob.es.

226 De la misma opinión es ZAFRA ESPINOSA DE LOS MONTEROS, Rocío, "El ciberagente en la lucha de la pornografía infantil", op. cit., pág. 1980.

227 Dentro del concepto de "terminales" y "dispositivos de conectividad" se incluyen tanto las tabletas, relojes inteligentes, etc., y medios de comunicación como el correo electrónico o servicios de mensajería electrónico como pueden ser sms, mms, whatsapp, line, etc.

El art. 588 ter a) respecto a los delitos que autorizan la interceptación de las comunicaciones telefónicas y telemáticas no contempla solamente los del art. 579.1 sino que utilizando la conjunción alternativa "o" la permite también para "los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la comunicación o servicio de comunicación" independientemente respecto a este segundo grupo de la pena con la que estén castigados, de manera que se viene a cercenar la impunidad que supone denegar tal medio de investigación cuando los medios tecnológicos son utilizados para cometer el delito.

Por otra parte, en las Secciones 2ª y 3ª se instaura un régimen específico para los supuestos en ellas contemplados. En la Sección 3ª en el art. 588 ter) k para la identificación del número de IP previendo únicamente la intervención judicial para que el Juez requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e) la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso y ello cuando esa dirección IP "estuviera siendo utilizada para la comisión de algún delito"; en el art. 588 ter i).1 se faculta a la policía a obtener el número IMSI o IMEI sin autorización judicial; y en el art. 588 ter m) se faculta al Ministerio Fiscal y a la Policía Judicial para dirigirse directamente a los prestadores de servicios para conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación o, en sentido inverso, para conocer el número de teléfono o los datos identificativos de cualquier medio de comunicación. Por tanto, en el ejercicio de sus funciones de investigación concreta de un determinado delito, el Ministerio Fiscal y la Policía judicial podrían requerir directamente a los proveedores de servicios de telecomunicaciones que les proporcionen aquellos datos que, sin embargo, no es posible cuando las funciones que llevan a cabo son las de prevención y descubrimiento de los delitos cometidos en Internet, en este supuesto sí es necesario solicitar la correspondiente autorización judicial. Es decir, no cabe en investigaciones prospectivas que la Policía se dirija directamente a las compañías de servicios de telecomunicaciones para solicitar datos personales, es preceptiva la previa autorización judicial. De hecho tal y como ha señalado repetidamente la jurisprudencia: "(...) *La prohibición de intervenciones prospectivas es consecuencia del principio de especialidad vigente en la materia, que significa que los poderes públicos no pueden inmiscuirse en la intimidad de los sospechosos, interceptando sus comunicaciones, con el exclusivo propósito u objeto de indagar a ciegas su conducta, por lo que*

la decisión jurisdiccional de intervención de las comunicaciones telefónicas tiene que estar siempre relacionada con la investigación de un delito concreto al menos en el plano indiciario (ver el vigente artículo 588 bis a 2 de la vigente LECrim), es decir, "no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva"[228].

En definitiva, la propia LECrim, en su artículo 588 ter m, está permitiendo al Ministerio Fiscal y a la propia Policía Judicial dirigir la solicitud directamente a las operadoras, sin necesidad de tutela o control judicial puesto que no afecta al derecho fundamental al secreto de las comunicaciones[229]. En este sentido, el legislador que modificó la LECrim mediante *LO 13/2015 incluyó explícitamente la titularidad de un número de teléfono entre los datos no vinculados a un proceso de comunicación y, por ende, descartó también* expresamente que su cesión exigiera autorización judicial[230]. La jurisprudencia ha señalado en relación a la diligencia de investigación solicitada al amparo de lo preceptuado en el artículo 588 ter m que: "*La diligencia de investigación que solicitó la fuerza actuante no alcanza al plano de la intimidad, o si la pudiera alcanzar, lo sería de forma tan irrelevante que la propia Ley de Enjuiciamiento Criminal está permitiendo al Fiscal y a la propia Policía Judicial solicitarlo directamente a las operadoras, sin necesidad de tutela o control judicial. Ahora bien, la argumentación del Fiscal choca contra el propio texto del invocado artículo 588 ter m, que dice textualmente: "Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia."; de lo que se deduce que el Ministerio Fiscal puede solicitar*

228 STS 272/2017, de 18 de abril, citada por una sentencia bastante reciente de la Audiencia Provincial de Barcelona del 15 de mayo de 2020, en Tirant on line, DOCUMENTO TOL8.012.597.

229 Sentencia de la Audiencia Provincial de Madrid, de 31 de marzo de 2017, en Tirant on line, DOCUMENTO TOL6.165.918.

230 Sentencia de la Audiencia Provincial de Araba/Álava de 8 de mayo de 2018, en Tirant on line, DOCUMENTO TOL6.735.137.

la información que menciona en su recurso sin necesidad de mediación por parte del juzgado de instrucción"[231].

Transcribo literalmente la argumentación dada por la jurisprudencia en relación a la diligencia de investigación vía artículo 588 ter m de la LECrim, donde se indica que: *"De interés resulta, para el presente caso, lo que refiere la Audiencia Provincial de Cádiz en auto de 17 de enero de 2017 para un supuesto similar: "Expuesto lo anterior diremos que lo que aquí se solicita por la policía no es propiamente una intervención judicial de un terminal móvil de telefonía, ni la observación ni la grabación de las conversaciones, ni tan siquiera la cesión de los datos asociados, llamadas, posición etc sino simplemente la identificación de los usuarios del IMEI correspondiente a un determinado teléfono sustraído y se hace como único medio posible para identificar a los autores de un delito de robo en el que dicho terminal se sustrajo. Los datos del terminal se obtienen por estar facilitados por su legítimo propietario interesado en su recuperación a quien le fue sustraído el 29 de mayo de 2016 y lo que se pretende es identificar al titular de la tarjeta SIM colocada en dicho terminal sustraído y para ello se solicita mandamiento a fin de que se faciliten todos los números de teléfono que se hayan asociados a dicho IMEI desde el 29 de mayo de 2016 e información de sus titulares, en ningún caso se interesan siquiera listados de llamadas, para con ello tratar de esclarecer el hecho.*

Es evidente que la injerencia que se solicita no afecta al contenido del secreto de las comunicaciones, ni tan siquiera creemos afecte materialmente al derecho a la intimidad, insistimos no se pide ningún dato asociado, los datos recabados no pueden permitir extraer conclusiones sobre la vida privada de las personas a las que afecten y de ahí que si la policía puede directamente conforme al art 588 bis m dirigirse a las operadoras para pedir

231 Sentencia de la Audiencia Provincial de La Coruña de 20 de octubre de 2018, en Tirant on line, DOCUMENTO TOL6.885.409. En la misma sentencia se indica que: "la Audiencia Provincial de Cádiz, Sección 3ª, en su Auto de 17 de enero de 2017, señala que "*tal injerencia no afecta al contenido del secreto de las comunicaciones, ni tan siquiera creemos afecte materialmente al derecho a la intimidad, insistimos no se pide ningún dato asociado, los datos recabados no pueden permitir extraer conclusiones sobre la vida privada de las personas a las que afecten y de ahí que si la policía puede directamente conforme al art 588 ter m dirigirse a las operadoras para pedir la identificación de un titular de un número, o el número de un terminal, cuanto más dicha diligencia podrá ser acordada por la autoridad judicial a solicitud policial, donde las garantías quedan reforzadas*".

la identificación de un titular de un número, o el número de un terminal, cuanto más dicha diligencia podrá ser acordada por la autoridad judicial a solicitud policial, donde las garantías quedan reforzadas, se trata de una injerencia mínima y conforme al principio de especialidad, precisa para la determinación de los autores de un delito, idónea además pues permite identificar al poseedor de un determinado terminal ilegítimamente arrebatado a su dueño y por ende necesaria, al no contar con otro medio alternativo para el esclarecimiento del hecho denunciado además de proporcionada, proporcionalidad que medimos considerando, insistimos en ello, la mínima injerencia que ocasiona"[232].

En relación con el número IMSI es el acrónimo de International Mobile Suscriber Identity (Identidad Internacional del Abonado a un Móvil). Este es el código de identificación único para cada dispositivo móvil, integrado en la tarjeta chip SIM (Subscriber Identy Module) que se inserta en el teléfono móvil para asignarle el número de abonado o MSISDN (Mobile Station Integrated Services Digital Network), que permite su identificación a través de las redes GSM y UMTS[233]. Proporciona una medida adicional de seguridad en la telefonía móvil y, sobre todo, facilita la prevención del fraude en la telefonía celular[234].

Por lo que respecta al IMEI o International Mobile Equipment Identy (Identidad Internacional del Equipo Móvil) identifica con su número de serie al equipo. Tal dato por, sí solo, *únicamente* permite diferenciar un determinado equipo del resto. Con el IMEI se puede solicitar al órgano judicial que ordene la identificación por el operador de los números de teléfono que corresponden a los datos obtenidos con el IMEI, y la correspondiente intervención de las comunicaciones[235]. El IMEI es el equivalente al número MAC en lo que hace referencia a móviles pues identifica ese número de serie al equipo. El término MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red, conocida también como dirección física y es única para cada dispositivo, en este sentido, las direcciones MAC son únicas a

232 Sentencia de la Audiencia Provincial de Pontevedra de 28 de julio de 2017, en Tirant on line, DOCUMENTO TOL6.359.343

233 Véase a HERNÁNDEZ DOMÍNGUEZ, Juan José, y MARTÍNEZ MARTÍN, José Israel, *Secreto de las comunicaciones. Alcance de protección constitucional de si interceptación y casuística*, DILEX, 2015, págs. 68 y 69.

234 STS 6389/2013 - ECLI: ES:TS:2013:6389. En https://www.poderjudicial.es/search/documento/TS/6939813/Dolo/20140127.

235 Ibídem.

nivel mundial y constituyen una huella digital que posibilitan saber desde qué dispositivo de red se ha emitido un determinado paquete de datos[236]. Aunque la LECRim no incluye en el artículo 588 ter) l, el identificador MAC, no obstante, la doctrina apunta la conveniencia de incluirlo, ampliando en este sentido la fórmula abierta y amplia de ese precepto[237].

Ni el MAC, ni el IMEI ni el IMSI proporcionan información sobre la identidad del usuario, por tanto, sólo tendrían valor si se asocia a otros datos en poder de las operadoras. Estos datos por sí solos no pueden integrarse en el concepto de datos de comunicación[238]. Para la obtención del número comercial del teléfono es necesario solicitarlo de las compañías proveedoras de servicios de telecomunicación y para ello se necesita la previa autorización judicial, de acuerdo a la Ley 25/2007, de 18 de octubre, de Conservación de Datos de las Comunicaciones Electrónicas, artículo 3.1. como al artículo 588 ter l, apartado 2 de la LECrim.

Señala el Tribunal Supremo que*: "A la vista de este régimen el art. 588 ter j), aplicable al caso que nos ocupa, establece igualmente un régimen específico, precepto que reza literalmente: "1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre la retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y se encuentren vinculados a procesos de comunicación, sólo podrán ser cedidos para su incorporación al proceso con autorización judicial.*

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación se solicit*ará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda automatizada o inteligente de datos, siempre que se precisen la naturaleza de los datos que han de ser conocidos y las razones que justifican la cesión".*

Como es de ver, no se trata de una interceptación o intervención de las comunicaciones telefónicas que como tales quedan sujetas a las exigencias contempladas en los artículos de la Sección 1ª en los cuales se hace continua referencia a la interceptación/intervención de las comunicaciones, sino del

---

236 QUEVEDO GÓNZALEZ, Josefina, *Investigación y prueba del ciberdelito*, op. cit., pág. 177.

237 Ibídem.

238 Ibídem.

supuesto más restringido y específico del citado art. 588 ter j, como ya hemos hecho mención".

La interceptación de las comunicaciones telefónicas y telemáticas es una diligencia de investigación que incide en el derecho al secreto de las comunicaciones. Este derecho tiene un carácter verdaderamente formal pues, como ha señalado el Tribunal Constitucional, "se predica de lo comunicado, sea cual sea su contenido"[239], es operativo "mientras el proceso de comunicación está teniendo lugar"[240]. En este sentido, es relevante señalar a estos efectos que una vez enviado por ejemplo un correo electrónico o un WhatsApp su acceso estaría protegido por el derecho al secreto de las comunicaciones, siempre y cuando no se haya leído[241].

En la Circular 1/2013, de la Fiscalía General del Estado se establece que: "*Debe considerarse la necesaria autorización judicial para acceder a cualquier mensaje enviado por correo electrónico, ya se trate de correo electrónico enviado y recibido pero no leído, correo en fase de transferencia o correo ya enviado, recibido y leído y que se encuentra almacenado*"[242].

Por tanto, a través de la correspondiente autorización judicial se podrá acceder tanto al contenido de las comunicaciones como a los datos de tráfico generados en dicha comunicación.

La jurisprudencia en este sentido ha manifestado que "*el derecho al secre-*

---

239 Sentencias del TC número 114/1984, de 29 de noviembre; número 34/1996, de 11 de marzo y número 70/2002, de 25 de abril.

240 STC n.º 137/2002, de 3 de junio.

241 Véase la Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas, publicado en el BOE» núm. 70, de 22 de marzo de 2019, donde se indica que, "por el contrario, no estarían comprendidas en la previsión constitucional las conversaciones grabadas o difundidas por uno de los interlocutores (SSTC n.º 175/2000, de 26 de junio y 56/2003, de 24 de marzo y STS n.º 421/2014, de 16 de mayo); las comunicaciones por radio (SSTS n.º 209/2007, de 9 marzo; 1397/2011 de 22 de diciembre y 695/2013, de 22 de julio); el acceso a la memoria o contactos de un teléfono móvil (SSTC n.º 70/2002, de 3 de abril y 142/2012, de 2 de julio y SSTS n.º 1273/2009, de 17 de diciembre); el visionado directo de un número de teléfono entrante (SSTS n.º 1040/2005, de 20 de septiembre y 1273/2009, de 17 de diciembre) o la conversación escuchada por agentes policiales a través del manos libres de uno de los interlocutores que accede a ello (STS n.º 589/2015, de 28 de septiembre)".

242 Circular 1/2013, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, en https://www.boe.es/buscar/doc.php?coleccion=fiscalia&id=FIS-C-2013-00001.

to es independiente del contenido de la comunicación, debiendo respetarse, aunque lo comunicado no se integre en el ámbito de la privacidad"[243].

La posibilidad de intervenir datos de tráfico o asociados al proceso de comunicación también conlleva que puedan verse afectados otros derechos diferentes al derecho al secreto de las comunicaciones como es el derecho a la intimidad (art. 18.1 CE) o el derecho a la protección de lo datos (art. 18.4 CE). La protección de estos últimos derechos, como veremos, es de menor intensidad que el derecho al secreto de las comunicaciones cuando se accede al contenido de lo comunicado, por tanto, deberá también ser menor el grado de exigencia de los principios rectores, recogidos en el artículo 588 bis a de la LECrim, para acordar su incorporación al proceso[244].

En definitiva, el derecho al secreto de las comunicaciones como manifestación concreta del derecho a la intimidad autoriza a su titular a mantener en secreto sus comunicaciones con sus interlocutores, excluyendo por tanto a cualquier tercero[245].

Ahora bien, de acuerdo al artículo 588 ter m de la LECrim, "*cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia*". Por tanto, la petición a las operadoras de la identificación del titular a partir de los datos de un dispositivo o precisar los dispositivos de los que es titular una persona concreta, realizada por el Ministerio Fiscal o la Policía Judicial no precisa de autorización judicial puesto que serían datos desvinculados de los procesos de comunicación. Ello puede tener repercusión en el derecho a la intimidad personal y no en el derecho al secreto de las comunicaciones que, como vimos, su protección es de menor intensidad, en este sentido, la jurisprudencia tanto del Tribunal Supremo como del Tribunal Constitucional han venido permitiendo que cuando concurran circunstancias de necesidad y urgencia las Fuerzas y Cuerpos de Seguridad del Estado puedan acceder a esa informa-

243 SSTC 70/2002 y 114/1984.

244 Véase la Circular 2/2019, ya citada supra.

245 STS 77/2019, 12 de Febrero de 2019, en https://vlex.es/vid/769623469.

ción en su función de prevención e investigación del delito, descubrimiento de los delincuentes y recogida de instrumentos, efectos y pruebas del delito. La LECrim, después de la reforma efectuada por la LO 13/2015 permite que, sin autorización judicial, la policía pueda requerir directamente a las empresas proveedoras de servicios de internet a la identificación de titulares o terminales o dispositivos de conectividad, apercibiéndoles en caso contrario de desobediencia.

Dejando a un lado esos supuestos, hay que tener en cuenta que la actuación de la Policía sin autorización judicial es muy excepcional, sólo por razones de necesidad y urgencia y siempre respetando los principios de proporcionalidad y razonabilidad. La Policía debe actuar con toda la cautela y precaución puesto que la práctica o adopción de diligencias de investigación relacionadas con las nuevas tecnologías, ya sea en el proceso penal o con anterioridad a la incoación del proceso penal, puede afectar a los derechos fundamentales reconocidos en el artículo 18 de la CE.

4. Registro de dispositivos de almacenamiento masivo

Otra de las herramientas que se pueden utilizar para investigar la comisión de hechos delictivos relacionadas con las nuevas tecnologías, es la del registro de dispositivos de almacenamiento masivo. Al igual que las medidas de investigación comentadas anteriormente, ésta se incorpora legalmente a nuestro Ordenamiento jurídico por primera vez mediante la LO 13/2015.

Esta Ley recoge la jurisprudencia existente hasta entonces danto cumplimiento a lo dispuesto en el Convenio sobre Ciberdelincuencia. Este tratado pretende que los actos procesales dirigidos a la obtención de la prueba digital respeten los presupuestos y requisitos de cada ordenamiento interno y al mismo tiempo se garanticen los derechos reconocidos internacionalmente y el principio de proporcionalidad[246].

Como preámbulo al análisis de su contenido, quisiera resaltar que una de las cuestiones importantes que la LO 13/2015 viene a destacar y de alguna manera a desterrar, es la consideración de que los dispositivos de almacenamiento masivo de información sean considerados simples piezas de convic-

246 Véase a RODRÍGUEZ RUBIO, Carmen, "Nuevas diligencias de investigación y de prueba: el registro de dispositivos de almacenamiento masivo de información", en https://dx.doi.org/10.5209/foro.74004,Foro, Nueva época, vol. 23, núm. 1 (2020): 267-304, ISSN:1698-5583.

ción y es que la importante tarea de recolección de datos a través del registro puede conllevar la vulneración de diferentes derechos fundamentales, dependiendo del carácter de la información a la que se accede, por ello, su naturaleza difiere de la simple pieza de convicción y la necesidad de una regulación exhaustiva, y es que los dispositivos de almacenamiento masivo que regula la ley comprenden no solo los instrumentos capaces de grabar, almacenar y posteriormente recuperar o leer información digital, sino también los soportes empleados para ello y que carecen de funcionalidad sin el dispositivo que en ellos escribe o lee[247].

Con anterioridad a la reforma operada por la comentada LO 13/2015, la jurisprudencia venía afirmando que "*el acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y a la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar -de hecho, normalmente albergará- información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones (…)*"[248].

Como se indica en la Exposición de Motivos de la Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos, "*al abordar el registro de dispositivos o equipos informáticos, el legislador ha optado por distinguir entre un registro estático, el de los dispositivos de almacenamiento masivo de información, y un registro dinámico, el registro remoto sobre equipos informáticos que, si bien presentan numerosas notas comunes, también ofrecen aspectos singulares que invitan a su tratamiento de forma individualizada*".

---

247 Generalmente los dispositivos que se suelen usar se agrupan en tres diferentes categorías: dispositivos magnéticos (unidades de disco duro o HDD, del inglés Hard Disk Drive, entre otros), dispositivos ópticos (CD, DVD o BD) y los dispositivos de memoria sólida o SSD (acrónimo inglés de solid–state drive) (tarjetas de memoria, memorias USB, etc.).

248 STS 246/14, de 2 de abril. En https://vlex.es/vid/505656870.

Quedan excluidos de la regulación legal dos tipos de registros: a) por un lado, el acceso a los dispositivos de almacenamiento masivo de información cuando han sido llevados a cabo por particulares en contextos desconectados de la investigación de los hechos delictivos; b) por otro lado, el registro de dispositivos que por el objeto y fines para que los que utilizan no implican vulneración del derecho a la intimidad de los particulares[249].

Otra de las cuestiones relevantes del acceso remoto a la información es cuando esta información está en la nube. En el marco de la prestación de servicios en nube pueden producirse transferencias internacionales de datos, por lo que una de las mayores preocupaciones es la posibilidad del acceso por parte de las autoridades de un tercer país a los datos alojados o tratados en el mismo[250]. Ello es relevante por la dimensión extraterritorial de Internet que trataba en otro punto de este trabajo dados los problemas jurídicos que conlleva, en concreto, por problemas de conflicto de soberanía entre Estados[251]. En estos casos, para

249 Véase la Circular 5/2019, ya citada.

250 Señala NAVARRO CASTRO, Miguel, "El cloud computing como forma de prestación de servicios de tratamiento de datos", en *Protección de datos personales,* (coord. GONZÁLEZ PACANOWSKA, Isabel), Tirant lo Blanch, 2020, págs. 621 y ss, que: *"La utilización de los servicios en la nube exige que las empresas y consumidores cedan sus datos a terceros, con el consiguiente riesgo que ello comporta de que estos no realicen un tratamiento adecuado de los mismos. Además, la propia configuración de los servicios en la nube hace que ese tratamiento, en la mayoría de las ocasiones, no vaya a ser realizado directamente por el proveedor de servicios, sino que este a su vez subcontrate con terceros (que se pueden encontrar en países diferentes) los recursos necesarios para el tratamiento de los datos, de manera que la empresa proveedora de los servicios pueda ajustar en cada momento los recursos de que dispone a las necesidades de sus clientes. A su vez, los subcontratistas pueden igualmente subcontratar y así sucesivamente, por lo que puede darse el caso de que ni siquiera el proveedor de servicios conozca cuál es en cada momento la localización exacta de los recursos empleados o de los datos tratados. Todo ello hace que sea muy difícil el establecer una regulación eficaz de las garantías que deben respetarse en el tratamiento de los datos efectuados en los servicios en la nube. En realidad, los problemas son los del tratamiento de datos automatizados en general, pero la complejidad de los servicios en la nube hace que los problemas de localización y control se manifiesten con toda su intensidad. Además, el hecho de que la contratación del tratamiento de datos suela ir acompañada de la de un software específico del proveedor de servicios, a través del cual se va a realizar ese tratamiento, y que puede no ser totalmente compatible con el software de terceros para finalidades similares, hace que se pueda dificultar el ejercicio del derecho del cliente a la portabilidad de los datos".*

251 Señala ALONSO, Adolfo, que el principal problema es que Internet carece de legislación específica y unitaria tanto a nivel nacional como internacional, nos encontramos

poder tener acceso a los datos alojados en otro país es necesario acudir a los mecanismos de cooperación internacional si es en el ámbito de la Unión Europea o acudir a los sistemas tradicionales de convenios internacionales o de tratados de asistencia jurídica mutua si es fuera del ámbito de la Unión Europea[252].

No obstante, desde hace ya algún tiempo estamos asistiendo a una importante transformación en el ámbito de la cooperación judicial en material penal en el marco de la UE. En este sentido, ha habido un cambio considerable en cuanto a cómo era entendida. La idea del Estado como compartimento estanco soberano debe desaparecer, este concepto de "soberanía nacional" que se proyectaba de modo directo en la colaboración entre los diversos Estados miembros se ha ido flexibilizando debido a la modificación de las circunstancias del entorno europeo. En este sentido, si tenemos en consideración la necesidad de potenciar la integración europea y el deseo de consolidación de un espacio único sin fronteras, se debe avanzar en el necesario crecimiento de la cooperación internacional en el ámbito de la Unión tanto en la vertiente policial como judicial.

El objetivo de instaurar una nueva libertad en la Unión Europea debe pasar necesariamente por la libertad de que las personas puedan moverse libremente, sin controles ni fronteras, es preciso completar esta situación con unas actuaciones que impidan la disminución de la seguridad de los Estados y de los individuos que podría generarse con la citada desaparición. En definitiva, debe existir un equilibrio entre el principio de seguridad con la libre circulación de los ciudadanos.

Es patente que la desaparición de las fronteras interiores implica como beneficio que tanto las personas, como capitales, bienes y servicios circulen libremente, pero por otro lado conlleva un incremento de la delincuencia, que resulta cada vez más peligrosa, sofisticada y tecnológica. Ello provoca que se generen auténticas redes organizadas que manejan grandes sumas de capital y que operan en diversos Estados[253].

---

en un entorno donde es prácticamente imposible saber donde reside toda la información sobre nosotros por lo que es difícil asegurar su uso. En "La investigación policial de los delitos…", op. cit., pág. 51.

252 Señala VILLARINO MARZO, Jorge, *La privacidad en el entorno del cloud computing*, Madrid, 2018, pág. 222, que "la naturaleza ubicua y difuminadora de fronteras, la balcanización que define la nube, provoca que ámbitos tan tradicionalmente vinculados al principio de la territorialidad como son tanto las actuaciones de las fuerzas de seguridad como los elementos jurisdiccionales afronten nuevas dificultades".

253 *La prueba en el Proceso. Perspectivas nacionales*, (Coordinadores, BUJOSA VA-

4.1 Registro estático de dispositivos de almacenamiento masivo de información

La reforma efectuada por la LO 13/2015 a la Ley de Enjuiciamiento Criminal vino a regular expresamente las diligencias de investigación tecnológica. Así una de las diligencias introducidas por dicha Ley es la contemplada en el artículo 588 sexies que se refiere al registro de dispositivos y equipos informáticos. Esta medida de investigación es objeto de tratamiento más exhaustivo por la *Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos*.

En este artículo 588 sexies de la LECRim se regulan diferentes diligencias de investigación. Por tanto, no son solo estos dispositivos sobre los que recae la medida de investigación, sino que el legislador establece hasta cuatro posibilidades de registro diferente[254]. Todos ellos instrumentos de archivo masivo de información, aunque algunos de ellos no sea la función principal. Por un lado, contempla la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos[255] y, por otro lado, contempla el acceso a su contenido. Este acceso a la información puede ser de dispositivos electrónicos incautados dentro o fuera del domicilio del investigado. Por tanto, este artículo contempla dos diligencias diferentes, el acceso a los dispositivos electrónicos y el clonado o volcado de los mismos[256].

DELL, Lorenzo-Mateo y BUENO DE MATA, Federico), 2018, en Tirant on line, DOCUMENTO TOL6.977.376.

254 Son todos supuestos de *cloud computing*, véase a DELGADO MARTÍN, J., "Investigación del entorno virtual...," op. cit., pág. 4.

255 DELGADO MARTÍN, Joaquín, "Investigación del entorno virtual…", op. cit., pág. 4, identifica dichos dispositivos con el siguiente contenido:

– Ordenadores: dispositivos que permiten el tratamiento automatizado de datos en ejecución de un programa o software.

– Instrumentos de comunicación telefónica o telemática: dispositivos que posibilitan la transmisión de datos (comunicación telemática). y/o de la voz (comunicación telefónica).

– Dispositivos de almacenamiento masivo de información digital: instrumentos que permiten el archivo de datos en formato electrónico (cometer data).

– Repositorio telemático de datos: sitio en el que se archiva o deposita información en formato digital (datos) y al que se accede a través de una red de comunicación; se trata especialmente de los supuestos de cloud computing (nube).

256 Véase a MARTÍN RÍOS, Pilar, "El "primer acceso policial" a dispositivos de

Ambas diligencias de investigación tecnológica requieren autorización judicial, como se indica en el apartado 2 del artículo 588 *sexies* de la LECRim, la simple incautación de cualquiera de los dispositivos mencionados requiere autorización judicial suficientemente motivada que no legitima de por sí el acceso a su contenido, ello requiere también autorización judicial. Por tanto, la incautación de los equipos no conlleva de por sí el acceso a su contenido, para ello, es necesario una nueva autorización del juez[257].

Esta autorización está contemplada en el artículo 588 *sexies c* de la LECRim, en el cual se indica que en la autorización se fijarán los términos y el alcance del registro y se podrá autorizar la realización de copia de los datos informáticos[258]. En dicha autorización el juez debe precisar las condiciones necesarias para asegurar que no exista manipulación, por tanto, debe establecer las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para posibilitar en su caso un futuro dictamen pericial.

Cuando sea posible obtener una copia de los datos informáticos sin necesidad de incautar los soportes físicos de estos datos, se hará así, siempre que esta copia se haga en condiciones que garanticen la autenticidad e integridad de los datos. La excepción a esta regla es que se procederá a la incautación de los soportes físicos que contienen los datos electrónicos cuando los mismos constituyan el objeto o instrumento del delito, o como establece la ley, existan otras razones que lo justifiquen. Una de las críticas que se hacen a esta excepción es que no se hayan identificado esas razones, aunque sean en una

---

almacenamiento digital, o de cuando las garantías se supeditan a la búsqueda de la eficiencia", op. cit., págs. 840 y 841.

257 Se indica en la STS de 14 de octubre de 2019. DOCUMENTO TOL.7.531.381, que "*en consideración a esta nueva necesidad, nuestra renovada legislación procesal ha contemplado el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies) como una diligencia específica que reclama garantías singulares y diferentes al registro de otros muebles e inmuebles. Destacábamos que en este caso hay un plus que viene determinado no solo porque puede suponer desnudar virtualmente a una persona sino porque incide también en otro derecho de nueva generación como es la autodeterminación informativa*".

258 De acuerdo a la definición que ofrece el Convenio del Consejo de Europa sobre Ciberdelincuencia en su artículo 1.B se entiende por datos informáticos: "*toda representación de hechos, información, o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función*".

lista abierta[259]. La Fiscalía General del Estado en la Circular 5/2019 ha interpretado esta circunstancia "la existencia de otras razones que lo justifiquen" como "una cláusula genérica de cierre que permitiría valorar como excepción a la regla general cualquier otra circunstancia específica que pudiera darse en un caso concreto, como, por ejemplo, que los soportes físicos contengan datos o archivos informáticos que pertenecieran a un tercero o que el titular o propietario del soporte no tuviera derecho a conservar".

Además, indica que "en la determinación de estas razones deberá ponderarse siempre la importancia de las mismas en relación con el perjuicio que genera la incautación del dispositivo"[260].

Por tanto, la autorización judicial de entrada y registro en un domicilio permite la incautación de los dispositivos de almacenamiento, pero esa autorización no es válida por sí sola para registrar o acceder a la información contenida en aquellos dispositivos, siendo necesaria otra autorización judicial que legitime el acceso a la información o que en la misma se habilite específicamente a tal acceso.

Además, en los dispositivos de almacenamiento masivo de información digital como son los discos duros externos, DVDs, CDs, USBs, etc., habrá una primera fase de acceso al dispositivo y una segunda de acceso al contenido. La primera fase de acceso al dispositivo puede ser con o sin incautación. Si, por el contrario, estamos ante ordenadores o instrumentos de comunicación telefónica o telemática el acceso a la información dependerá de si están o no conectados a una red. Si lo están, la información que se busca puede estar tanto en el dispositivo como en la propia red. Pero si los instrumentos no están conectados a la red deberá procederse en todo caso al acceso al dispositivo, pues la información solo se hallará en él. En los repositorios telemáticos de datos no existe incautación física, sino que se procede directamente al acceso a la información[261]. Los repositorios telemáticos de datos son "supuestos de deslocalización de la información o *cloud computing* en los que la información se almacena de forma temporal o de manera permanente en servidores alojados en cualquier parte del mundo, y se envía a través de Internet a cachés temporales del equipo informático o dispositivo del usuario"[262].

---

259 MARTÍN, RÍOS, Pilar, "El "primer acceso policial…", op. cit., pág. 401.

260 Circular 5/2019.

261 SANCHIS CRESPO, Carolina (con VELASCO, Eloy), *Delincuencia informática*…, op. cit., págs. 379 y 380.

262 DELGADO MARTÍN, Joaquín, "Investigación del entorno virtual…", op. cit., pág. 11.

Si bien, teniendo en cuenta la necesidad de la autorización judicial en la generalidad de los casos, se permite a la Policía Judicial o al fiscal, cuando existan razones de urgencia[263] en el que se aprecie un interés constitucional legítimo[264] que lleven a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente y siempre con la antelación del plazo de veinticuatro horas, de la actuación llevada a cabo, la forma de realizarla y el resultado obtenido. En estos casos, el órgano judicial en el plazo de setenta y dos horas, confirmará o revocará de forma motivada la orden de interceptación. La actuación de la Policía debe respetar estrictamente los principios de proporcionalidad y razonabilidad para poder acceder a los datos de un dispositivo, siendo necesario siempre una resolución judicial posterior al registro policial que legitime la injerencia policial en el derecho fundamental afectado, que puede ser, como veremos posteriormente, el derecho a la intimidad o el derecho al secreto de las comunicaciones. Por tanto, es necesario siempre que exista una convalidación judicial posterior.

La finalidad de estas diligencias de investigación es precisamente la de "investigación", la de obtener datos que justifiquen la adopción de alguna medida cautelar[265]. Su finalidad, por tanto, no es probatoria sino de investigación. Para poder aportar los datos obtenidos en la investigación es necesario preconstituir la prueba para que tenga valor probatorio. Precisamente, la volatilidad de la información digital o tecnológica puede justificar la urgencia de la actuación, lo que unido al interés constitucionalmente legítimo, que no es otro, que la lucha contra la delincuencia, puede justificar que la Policía Judicial o el fiscal accedan a los datos sin necesidad de autorización, aunque posteriormente debe ser convalidada o denegada.

---

263 En la Circular de la Fiscalía 5/2019, apoyándose en la STC número 70/2002, de 3 de abril, se hace referencia a la "urgencia" que justifica la intromisión de la policía en el derecho a la intimidad sin previa autorización judicial como la necesaria para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias.

264 En la Circular 1/2013 se indica que el interés constitucionalmente legítimo "*enlaza con el art. 8.2 del CEDH que, para la admisibilidad de la injerencia de la autoridad pública en el derecho a la vida privada, considera necesario que la medida persiga a alguna de las siguientes finalidades: la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás*".

265 MARTÍN RÍOS, Pilar, "El "primer acceso policial" a dispositivos…", op. cit., pág. 843.

Esa misma característica de volatilidad unida a la facilidad de manipular los datos informáticos es lo que aconseja que la obtención de información se haga sobre copias y no sobre los dispositivos originales que a su vez permite la realización de diferentes informes periciales. Cuando se acuerde practicar copias sobre los dispositivos de almacenamiento, durante el registro de un domicilio, se hará en presencia del Letrado de la Administración de Justicia, garantizándose de esta forma la autenticidad e integridad de la copia llevada a cabo. La función en estos casos del Letrado de la Administración de Justicia será la de dar fe de la identidad del soporte de almacenamiento masivo de información, es decir, que el soporte copiado es el mismo que fue encontrado en el registro domiciliario y, de tal forma fue consignado en el acta, por el contrario, la garantía de la integridad de la copia vendrá dada por la firma digital al poderse comprobar que el resultado de la función hash[266] del original coincide exactamente con el de la copia[267]. No obstante, en los casos de realización de copias lógicas, la mejor forma de garantizar qué se copia, cómo se copia y la integridad de la copia, será su realización a presencia y bajo la fe del Letrado de la Administración de Justicia[268].

---

266 Los hashs, también denominados funciones de resumen, tal y como se describen: "*son algoritmos que consiguen crear a partir de una entrada –ya sea un texto, una contraseña o un archivo–, una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado. Es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos*". Véase a GENVETA:DEV, "¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales" accesible en https://goo.gl/fvqAmM.

267 Sobre esta copia exacta el perito debe hacer un cálculo sobre el disco duro (en el momento de la extracción), y el resultado total de bits copiados nos da un resultado alfanumérico único, que es el MD-5, y a partir de aquí, sobre este disco clonado, se pueden hacer otras copias que puedan ser objeto de pericia.

Si el clonado del disco duro no se realiza siguiendo estos sistemas que verifican la identidad del disco original con el copiado, el resultado probatorio será dubitado y, por lo tanto, dicha prueba podrá ser objeto de impugnación. Véase a SANZ-GADEA GÓMEZ, Juan Bautista, *Los informes periciales informáticos en el ámbito*..., op. cit., Tirant on line, DOCUMENTO TOL5.638.931.

268 Véase la Circular 5/2019, ya citada. Anteriormente, la jurisprudencia ponía de manifiesto la necesidad de que el Letrado de la Administración de Justicia recogiese en acta todo el proceso realizado sin necesidad, por el contrario, de estar presente en el proceso de clonado. Así literalmente, el Tribunal supremo indicaba que "Y será a partir de ese momento donde se pueda prescindir de la presencia del Letrado, ya que como dice la jurisprudencia, es un proceso técnico. Y será, una vez terminado el proceso del clonado,

Las posibilidades de hacer copias de la información de los dispositivos de almacenamiento masivo de información, como hemos visto, puede ser de dos formas; o bien, la copia espejo que es una copia de la información Bit a Bit, donde se realiza un volcado o clonado de la información[269], y la otra forma es la copia lógica, que es una copia selectiva de información. En la primera se podrá incluso recuperar parte de la información que hubiese sido borrada y no sobre escrita[270]. Siempre se debería firmar el proceso con el cálculo de la función HASH, pero además, en el caso de la copia lógica, sería recomendable la presencia del Letrado dela Administración de Justicia con el fin de otorgar mayor garantía a la hora de la selección de archivos, según podemos leer en la Circular 5/2019 de la Fiscalía General del Estado.

Ahora bien, para llevar a cabo el registro de los dispositivos de almacenamiento masivo de información, en algunos casos el acceso a los datos se realizará directamente, pero en otros, el registro se desdoblará necesariamente en dos fases: una primera de acceso al dispositivo y una segunda de acceso al contenido. Como señala la doctrina que exista una o ambas dependerá de la ubicación de los datos[271].

4.2. Registro remoto de equipos

La otra posibilidad de llevar a cabo un registro de los dispositivos de almacenamiento masivo es a través del registro remoto.

El registro remoto de equipos informáticos está contemplado en el artículo 588 septies de la LECRim, sin embargo, traen causa de lo establecido en los artículos 20 y 21 del Convenio de Budapest sobre la Ciberdelincuencia de

---

cuando el Letrado de la Administración de Justicia tendrá que reflejar en el acta la hora de finalización, el código HASH resultante del proceso, los bytes de información copiada y la numeración de las bolsas donde se vuelven a precintar las evidencias. STS 1190/2009, de 03 de diciembre (Tol 1762123).

269 En la práctica, hay que tener en cuenta que el perito nunca va a trabajar sobre el disco duro original, sino sobre la copia, y de ahí la importancia de que su contenido coincida con el original, pues de lo contrario estaríamos ante una inexactitud que podría provocar la nulidad del resultado obtenido. SANZ-GADEA GÓMEZ, Juan Bautista, *Los informes periciales informáticos…, op. cit.,* en Tirant on line, DOCUMENTO TOL5.638.931.

270 Véase a FERNÁNDEZ MARTÍNEZ, Juan Carlos, "Especialidades de la prueba cuando, esta, es tecnológica", en *Nuevas tecnologías 2020,* op. cit., pág. 336.

271 SANCHIS CRESPO, Carolina (con VELASCO, Eloy), *Delincuencia informática…*, op. cit., pág. 379.

2001, donde ya se establecía la posibilidad de obtener en tiempo real datos informáticos tanto los relativos al tráfico como al contenido de comunicaciones[272]. El objeto de esta diligencia de investigación es la de "utilización de

272 *Artículo 20. Obtención en tiempo real de datos sobre el tráfico.*

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a: a) Obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y b) obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica: i) a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos

sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21. Interceptación de datos sobre el contenido.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno: a) A obtener o a grabar mediante la aplicación de medios técnicos existentes en su territorio, y b) a obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica: i) A obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos".

Aunque esta diligencia guarda numerosas similitudes con el registro estático de equipos informáticos, sin embargo, tiene algunas singularidades que han motivado su tratamiento diferenciado.

En este sentido, partiendo de que ambos registros tienen la misma finalidad y pueden recaer sobre el mismo objeto, sin embargo, existen dos características que los diferencian, como son: la clandestinidad y el carácter dinámico del registro. Así, el registro remoto se lleva a cabo sin conocimiento de su titular o usuario por lo que puede tener implicaciones en la práctica de las diligencias y, por tanto, en las necesarias garantías con las que se tienen que practicar.

En relación con el presupuesto para poder adoptar esta medida se requiere siempre autorización judicial. Es necesario para poder adoptarla que haya una autorización judicial con antelación, no es posible, a diferencia del registro estático de equipos informáticos que la practique la Policía y posteriormente sea convalidada por la autoridad judicial.

Además, en esta clase de diligencias, el ámbito de aplicación está limitado puesto que la Ley establece una serie de delitos en los que se puede solicitar su práctica, no cabe en cualquier tipo de delito, sino sólo para la investigación de los previstos legalmente[273]. La Ley limita la práctica de esta diligencia a determinados delitos, que son los más graves, precisamente por la gravedad que supone en la intromisión de los derechos fundamentales del investigado. En este sentido, la afectación en los derechos fundamentales del investigado

---

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

273 En concreto, de acuerdo al artículo 588 *septies* a, serían: a) los delitos cometidos en el seno de organizaciones criminales; b) delitos de terrorismo; c) delitos contra la Constitución, de traición y relativos a la defensa nacional; e) delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación".

es mayor que en la diligencia de registro estático de equipos informáticos por ello el legislador ha establecido unos límites en el ámbito de aplicación[274]. Además, no es suficiente para acordar esta diligencia que se circunscriba a uno de los delitos especificados en el artículo 588 septies a. sino que además la autorización judicial deberá ponderar si resulta proporcionada la concreta intromisión en los derechos fundamentales del investigado en relación con la gravedad del hecho que se está investigado.

Esta diligencia de registro remoto de dispositivos posibilita a se vez la posibilidad de interceptar las comunicaciones electrónicas. Es una de las posibles formas de realizar interceptaciones de comunicaciones, tal vez la más compleja, pero puede ofrecer algunas ventajas como puede ser la obtención de información ya desencriptada o antes de que haya sido cifrada[275].

El principal problema en relación a la opción que se elija es la que se refiere a la regulación legal aplicable, si es la correspondiente al registro remoto o es la aplicable a la interceptación de las comunicaciones telemáticas. En la Circular de la Fiscalía 5/2019 la solución que se ofrece pone el acento en el contenido de la medida y no en el medio que se emplee. Así, se indica que "cuando el Juez autorice únicamente la interceptación de las comunicaciones telemáticas, sin acceso a otros contenidos del sistema o repositorios de datos, deberán observarse las disposiciones previstas para la interceptación de comunicaciones; por el contrario, cuando se autorice el acceso al contenido del sistema y el registro de los datos que allí se encuentren, la regulación aplicable será la del registro remoto, independientemente de que la misma también permita la interceptación de las comunicaciones"[276].

Otra de las diferencias con la diligencia del registro estático de equipos informáticos es en relación al ámbito subjetivo del deber de colaboración, puesto que en la diligencia de registro remoto se amplía considerablemente el círculo de personas que tienen el deber de colaborar en la investigación de los hechos delictivos. Así, de acuerdo al artículo 588 septies b. están obligados a facilitar a los agentes investigadores la colaboración requerida para la prácti-

274 Véase a DELGADO MARTÍN, Joaquín, "Investigación del entorno virtual…", op. cit., pág. 12, quien indica que "los registros remotos prolongan en el tiempo la injerencia en los diferentes contenidos del dispositivo, por lo que suponen una afectación de elevada intensidad en los derechos a la intimidad y al secreto de las comunicaciones de la persona investigada, aunque también en el denominado derecho a la autodeterminación informativa del art. 18.4 de la Constitución".

275 Circular 5/2019, de la Fiscalía General del Estado.

276 Ibídem.

ca de la medida y el acceso al sistema, además de los prestadores de servicios y personas señaladas en el artículo 588 ter e[277] y los titulares o responsables del sistema informático o base de datos objeto del registro, también a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para llevar a cabo con éxito la práctica de la diligencia. Sin embargo, en la diligencia de registro estático de equipos informáticos, de acuerdo al artículo 588 sexies c. 5, las autoridades de investigación delictiva podrán pedir la colaboración a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo sin incluir a los prestadores de servicios y personas señaladas en el artículo 588 ter e. ni a los titulares o responsables del sistema informático o base de datos.

Probablemente, la justificación de limitar el ámbito subjetivo en la diligencia de registro estático de los equipos informáticos se deba a que el acceso a los datos se realiza generalmente a través de las claves o contraseñas y, en cambio, en el registro remoto se puede requerir comportamientos activos que exijan el desarrollo de trabajos o herramientas que posibiliten su práctica.

No obstante, para ambas diligencias de investigación está excluido el deber de colaboración tanto del investigado o encausado como de las personas que no están obligadas a declarar por razón del parentesco y aquellas que de conformidad con el artículo 416.2 de la LECrim no puedan declarar en virtud del secreto profesional.

El legislador, a la hora de regular el registro remoto de equipos informáticos no permite que se deje de colaborar con los agentes de investigación cuando suponga una carga desproporcionada para el afectado, a diferencia del registro estático. En este sentido, entre los bienes jurídicos o intereses puestos en juego el legislador ha primado la práctica de esta diligencia a través del registro remoto, por encima de la protección del sujeto sometido a la colaboración requerida, la gravedad de los delitos que pueden ser investigados a través de esta diligencia de investigación justificaría ya de por sí la realización de la misma.

---

277 En este artículo se especifica en concreto a "los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual".

Finalmente, otra de las singularidades de la diligencia de registro remoto es que la LECRim establece que los sujetos requeridos para prestar la colaboración tienen la obligación de guardar secreto de las actividades requeridas por las autoridades de investigación. Es evidente que para que sea factible la práctica de la diligencia es necesario que las personas que están colaborando se abstengan de dar a conocer esa información, puesto que, de otra forma, la clandestinidad que caracteriza a esta técnica de registro desaparecería y no se conseguiría ningún resultado.

h. 2 Ámbito europeo

Como apuntaba anteriormente, para la persecución de estas nuevas figuras delictivas es necesario la creación de nuevas herramientas para la investigación y seguimiento de los autores con la finalidad de poder castigarlos y dado que en la era en la que vivimos, conocida como era digital, la comunicación no tiene fronteras es necesario articular mecanismos más allá de los previstos por cada Estado.

Esta necesidad era ya patente en la Directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales, donde en su Considerando 27 se indicaba que: "*Los responsables de la investigación y del enjuiciamiento de las infracciones contempladas en la presente Directiva deben disponer de unos instrumentos de investigación eficaces. Entre estos instrumentos podrán figurar la interceptación de comunicaciones, la vigilancia discreta, incluida la electrónica, el control de cuentas bancarias y otros medios de investigación financiera, teniendo en cuenta, entre otras cosas, el principio de proporcionalidad y la índole y gravedad de las infracciones que se estén investigando. Cuando proceda y de conformidad con el Derecho nacional, entre dichos instrumentos podrá encontrarse también la posibilidad de que los servicios de seguridad utilicen una identidad oculta en Internet*"[278].

En el Informe emitido por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior sobre la Directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales, la ponente[279] manifestó que: "*La investigación y el enjuiciamiento de las infracciones relacionadas con los abusos sexuales a menores en línea siguen suponiendo un reto para los cuerpos y fuerzas de seguridad y para las autoridades judiciales. Los expertos que presentaron*

278 Publicado en el Diario Oficial de la Unión Europea el 7.12.2011, L 335/4.

279 Anna María Corazza Bildt.

elementos de prueba ante la Comisión LIBE detectaron diversos factores que reducen la eficacia de las técnicas de investigación en línea: el cifrado de las comunicaciones en línea, las diferencias en las normas aplicables a la conservación de datos en los Estados miembros, el creciente uso de las herramientas de anonimización y el uso del almacenamiento en la nube. En dichas situaciones no siempre es fácil determinar qué país es competente y qué legislación es aplicable a la recogida de los elementos de prueba. A este respecto, es esencial una cooperación reforzada a escala internacional y de la Unión"[280].

En la Propuesta de Resolución del Parlamento Europeo sobre la aplicación de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, en su numeral 20 se destaca que "algunas de las principales dificultades a las que se enfrentan los cuerpos y fuerzas de seguridad y las autoridades judiciales en la investigación y el enjuiciamiento de las infracciones relacionadas con los abusos sexuales de menores en línea se derivan especialmente de la dimensión transfronteriza de las investigaciones y de la dependencia de las pruebas electrónicas; señala, en particular, la necesidad de mejorar las técnicas de investigación digitales para poder seguir el rápido ritmo de los avances tecnológicos" y "manifiesta su preocupación por el uso de tecnologías de traducción de direcciones de red de clase portadora (NAT CGN) por los proveedores de servicios de internet que permiten compartir una sola dirección IP entre varios usuarios en un mismo momento, lo que pone en peligro la seguridad en línea y la capacidad para determinar responsabilidades; pide a los Estados miembros que alienten a los proveedores de servicios de internet y a los operadores de red a que adopten las medidas necesarias para limitar el número de usuarios por dirección IP, eliminar de forma progresiva la utilización de las tecnologías CGN y efectuar las inversiones necesarias para adoptar con urgencia la siguiente generación de direcciones de protocolo de internet versión 6 (IPv6)"[281].

En definitiva, es mas que patente la preocupación a nivel europeo e inter-

280 En el Informe sobre la aplicación de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, de 27.11.2017, (2015/2129(INI)), publicado en http://www.europarl.europa.eu/doceo/document/A-8-2017-0368_ES.html.

281 http://www.europarl.europa.eu/doceo/document/A-8-2017-0368_ES.html.

nacional por buscar herramientas que permitan la investigación de los hechos delictivos acordes con la naturaleza de esos hechos, la mayoría de los cuales cometidos a través del uso de las nuevas tecnologías. En esta labor de investigación es importante resaltar el papel fundamental que desempeñan los Proveedores de servicios en la comunicación y tratamiento de los datos.

Precisamente con ese propósito, se creo a nivel europeo el *European Cybercrime Centre* (EC3), cuyo principal objetivo es luchar no solo contra la ciberdelincuencia, sino también de aportar análisis de investigación y movilizar los recursos pertinentes en la lucha contra la criminalidad informática[282]. Es el mismo Centro el que hace hincapié en la necesidad de unir las fuerzas, la cooperación y colaboración entre las autoridades de los diferentes países miembros en la captura de los ciberdelincuentes, reforzando la idea de que se trata de un delito de carácter transfronterizo, sin límites[283].

El Centro Europeo de Ciberdelincuencia (EC3) fue creado por Europol en 2013 para reforzar la respuesta policial a la ciberdelincuencia en la UE y, por tanto, ayudar a proteger a los ciudadanos, las empresas y los gobiernos europeos de la delincuencia en línea.

En este sentido, dentro de las Consideraciones generales emitidas en *el Informe presentado por el Parlamento Europeo sobre la lucha contra la ciberdelincuencia*[284], dentro de los Considerandos se hacía referencia a varias cuestiones importantes a tener en cuenta; en primer lugar, el número tan elevado de delitos que quedan sin investigar y por lo tanto impunes; añadido a ello el bajo porcentaje de asuntos que se denuncian, así como el retraso en materia de detección, permitiendo que los ciberdelincuentes desarrollen múltiples vías de entrada y salida o puertas traseras, también la dificultad de acceder a las pruebas electrónicas, tanto en lo relativo a la obtención como a la admisibilidad de estas ante los tribunales, y por último, la complejidad tanto en los procedimientos como los problemas judiciales relacionados con el carácter transfronterizo de los ciberdelitos.

Otra de las Consideraciones que resaltó el Parlamento en el Informe citado era la constatación de que los jóvenes utilizan internet a una edad cada vez

282 AGUILAR CÁRCELES, Marta María, "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención…", op. cit.

283 Ibídem.

284 Véase el Informe del Parlamento Europeo del 25 de julio de 2017, sobre la lucha contra la ciberdelincuencia (2017/2068(INI), en https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_ES.html.

más temprana y son especialmente vulnerables a distintos peligros, como es el embaucamiento y otras formas de explotación sexual en línea (ciberacoso, abuso sexual, coacción y extorsión sexual), así como también la usurpación de datos personales. En el Informe se resalta también la importancia de proteger especialmente a los jóvenes dada la influencia que pueden tener sobre ellos las peligrosas campañas destinadas a promover distintos tipos de autolesiones; Finalmente, se hace hincapié a los servicios que ofrecen las distintas herramientas on line para los delincuentes, quienes pueden localizar y embaucar víctimas más rápido gracias precisamente a las salas de chat, el correo electrónico, los juegos en línea y las redes sociales, y que las redes ocultas entre iguales (P2P) siguen siendo las plataformas fundamentales que utilizan los agresores sexuales de menores para conseguir y difundir material vinculado con la explotación sexual de menores, así como para rastrear nuevas víctimas pasando desapercibidos.

Teniendo en cuenta todas estas Consideraciones, se hacía hincapié en la necesidad de llevar a cabo un plan de acción para proteger los derechos de todos los menores ya sea en el ciberespacio como fuera de él, y a este respecto abogaba porque las fuerzas y cuerpos de seguridad del Estado dirijan sus esfuerzos a este propósito para lo que necesariamente se debe reforzar la cooperación judicial y policial entre los Estados miembros y con Europol y su Centro Europeo de Ciberdelincuencia (EC3) para prevenir y combatir la ciberdelincuencia, en particular, la explotación sexual de menores en línea. Además, en dicho Informe se instaba a la Comisión y a los Estados miembros a poner en marcha todas las herramientas jurídicas necesarias para luchar contra el fenómeno de la violencia en línea contra las mujeres y el ciberacoso, y en este sentido, solicitaba a la Unión Europea y a los Estados miembros, en particular, que unieran fuerzas para conseguir un marco de delitos penales que obligue a las empresas de internet a eliminar el contenido ofensivo, degradante y humillante, o a poner fin a su divulgación; finalmente, pedía asimismo que se estableciese apoyo psicológico para mujeres víctimas de violencia en internet y para niñas objeto de ciberacoso.

El EC3 adopta un enfoque triple para la lucha contra el ciberdelito: análisis forense, estrategia y operaciones.

Dentro de las medidas de actuación destaca la relativa a la prevención de esos delitos, para el logro de este objetivo han desarrollado un programa de prevención donde se resalta la importancia de asesorar a los propios ciudadanos y a las empresas de la Unión Europea para luchar contra ese peligro.

Desde la propia institución son conscientes de que la evolución de los delitos cibernéticos es constante, propiciando, por un lado, que se creen nuevos contextos y formas de perpetración del delito y, por otro, que se incremente el número de víctimas potenciales, motivo por el cual los mecanismos de prevención se centran en el seguimiento de dichas tecnologías emergentes[285].

Estas actividades cuentan con el apoyo del Equipo de Inteligencia Cibernética (CIT), cuyos analistas recopilan y procesan información relacionada con el delito cibernético de fuentes públicas, privadas y abiertas e identifican amenazas y patrones emergentes[286]. Además, el EC3 cuenta con el apoyo de diferentes organismos, como son el Grupo de Trabajo de la Unión Europea en la Lucha contra la Ciberdelincuencia (European Union Cybercrime Taskforce, EUCTF), la Agencia Europea de Seguridad en Redes e Información (European Network and Information Security Agency, ENISA), la Unidad de Cooperación Judicial de la Unión Europea (European Union's Judicial Cooperation Unit, EUROJUST) o la Organización Internacional de Policía Criminal (International Criminal Police Organization, INTERPOL)[287].

Por otro lado, habría que destacar la función que lleva a cabo la Agencia Europea para la Seguridad de la Información y de las redes -European Information Network Security Agency, EINSA[288]- donde, entre otras funciones encomendadas, se encuentra la que se dirige a los menores de edad, por ser la más preocupante, la cual orienta sus fines a la concienciación sobre protección de datos personales o de aquel material que pudiera afectar a la propia imagen. La protección en este ámbito conlleva ineludiblemente por estar vinculado a ello, la prevención del cyberbullying o del child grooming, entre otros ilícitos perpetrados por la red y que afectan a menores[289].

---

285 Ibídem.

286 Véase en https://www.cybersecurityintelligence.com/europol-european-cybercrime-centre-ec3-1146.html

287 Véase a AGUILAR CÁRCELES, M. M, "Cibercrimen y cibervictimización…", op. cit.

288 La Agencia de la Unión Europea para la Ciberseguridad, ENISA, es la agencia de la Unión dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Establecida en 2004 y reforzada por la Ley de Ciberseguridad de la UE, la Agencia de Ciberseguridad de la Unión Europea contribuye a la política cibernética de la UE, mejora la confiabilidad de los productos, servicios y procesos de TIC con esquemas de certificación de ciberseguridad, coopera con los Estados miembros y los organismos de la UE, y ayuda a Europa a prepararse para los retos cibernéticos del mañana, véase en https://www.enisa.europa.eu/about-enisa.

289 AGUILAR CÁRCELES, M. M. (2015). "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido", op. cit.

i. El almacenamiento y conservación de datos electrónicos

La averiguación de los hechos delictivos requiere generalmente la colaboración de muchas personas no sólo de los órganos encargados de la investigación y persecución de los delitos sino también de otros sujetos que no implicados en la comisión de lo hechos guardan o conservan información relevante para la averiguación de aquellos, me estoy refiriendo a las empresas proveedoras de servicios de Internet. La colaboración de estos proveedores de servicios es fundamental porque guardan y, por tanto, pueden ceder información relevante sobre los abonados y suscriptores que puede constituir posteriormente prueba en el proceso penal. Su colaboración, por tanto, con la Justicia es primordial.

El almacenamiento de datos personales por los servicios de comunicaciones electrónicas puede obedecer a diferentes razones, hay veces que se conservan durante un plazo limitado de tiempo por razones de interés comercial con la finalidad de facturar los servicios prestados por las compañías de servicios, y otras veces se conservan por razones de interés público. La conservación de estos datos personales en sí puede no implicar ningún problema si se hace por un tiempo breve, el problema surge cuando se almacenan datos personales de un sinfín de personas por tiempo ilimitado y teniendo en cuenta que pueden llegar a ser cedidos a terceros[290].

Precisamente, con el propósito de imponer obligaciones a los Estados en materia de conservación de datos personales, desde la Unión Europea, se ha desarrollado una regulación en materia de telecomunicaciones que se inicia con la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[291]. Esta regulación sectorial posteriormente sería ampliada y reforzada por la Directiva 2006/24/CE de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[292], cuyo

290 LÓPEZ JIMÉNEZ, Raquel, "El nuevo enfoque jurídico sobre el sistema de cesión de datos tras la Sentencia del Tribunal de Justicia de 2 de octubre de 2018", en *Uso y Cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios* (Dir. COLOMER HERNÁNDEZ), Aranzadi, 2019.

291 Publicada el 31.7.2002, en el Diario Oficial de las Comunidades Europeas, L 201/37.

292 Publicada el 13.4.2006, en el Diario Oficial de la Unión Europea, L 105/54.

contenido se integra en el ordenamiento español a través de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que sin embargo fue invalidada por el Tribunal de Justicia de la Unión Europea por ser contraria a la Carta de Derechos Fundamentales de la Unión Europea[293], mediante sentencia de 8 de abril de 2014, Digital Rights Ireland y Seitlinger y otros (asuntos acumulados C-293/12 y C-594/12)[294] y posteriormente la sentencia de 21 de diciembre de 2016, asuntos acumulados C-203/15 Tele2 Sverige AB / Postochtelestyrelsen y C-698/15 Secretaty of State for the Home Department/Tom Watson y otros[295].

Sin embargo, la decisión del TJUE, en su sentencia de 2 de octubre de 2018[296], al contrario de lo que parecía previsible, parece legitimar la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de telecomunicaciones, que por tanto sigue en vigor en nuestro Ordenamiento a pesar de la declaración de invalidez de la Directiva 2006/24/CE de la cual es desarrollo[297].

En España, la primera ley que concretó y desarrolló el derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales fue la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. Este ley fue derogada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos que, a su vez, ha sido derogada por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

---

293 Publicada en el Diario Oficial de la Unión Europea el 30.3.2010, C 83/389.

294 http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5609cf5b3c2bf440785fb94310e73e6ab.e34KaxiLc3qMb40Rch0SaxyKahj0?text=&docid=150642&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=983449.

295 https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=ES.

296 Nº C-207/16.

297 Sobre la vigencia de dicha Ley véase el trabajo de POLO ROCA, Andoni, "La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión", en *Revista de Internet, Derecho y Política*, núm. 33 (octubre), 2021.

En el ámbito europeo el último escalón en esta evolución ha tenido lugar con la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Al tener el Reglamento europeo eficacia directa, su finalidad principal es la de intentar paliar los obstáculos existentes en la armonización de los ordenamientos de los Estados miembros en relación con el tratamiento de los datos personales y la libre circulación de los mismos, a diferencia de la Directiva la cual dejaba a los Estados miembros la implementación de la misma en sus ordenamientos, lo que en la práctica ha supuesto una diversidad de regulaciones en el ámbito interno. En este sentido, la Ley Orgánica 3/2018, de 5 de diciembre, tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

Esta última ley se ha aplicado para lo dispuesto en el Reglamento 2016/679, que se ha mantenido en vigor hasta que se ha traspuesto la Directiva 2016/680, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

No ha sido hasta mayo de 2021, es decir, con más de dos años de retraso[298], cuando la Directiva 2016/680 ha sido traspuesta definitivamente por nuestro Ordenamiento mediante la Ley Orgánica 7/2021, de 26 de mayo, regulando finalmente la protección de las personas físicas en el tratamiento de los datos personales en todas las labores de prevención, detección, investigación o enjuiciamiento de infracciones penales, así como de protección y prevención frente a las amenazas contra la seguridad pública. Así, se incorpora a la legislación española la Directiva de la Unión Europea en esta materia, que forma parte del denominado "paquete de protección de datos" impulsado por

298 La fecha límite de trasposición de la Directiva era la de 6 de mayo de 2018.

la Comisión Europea y cuyo objetivo es la protección de las personas físicas en lo que respecta al tratamiento de datos personales y su libre circulación y se crea un marco regulador nacional en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, principalmente policiales, fiscales y judiciales, en la prevención, persecución y enjuiciamiento de delitos tal y como venían exigiendo las autoridades europeas. Ámbito que hasta ahora estaba falto de regulación[299].

Hecho ese apunte, y continuando con el almacenamiento y conservación de datos electrónicos por las empresas proveedoras de servicios de Internet, la regulación actual en materia de tratamiento de datos electrónicos y protección de los mismos viene contemplada por la Ley 25/2007.

De acuerdo con el artículo 3 de la Ley 25/2007, y la Disposición Adicional Única que se refiere a los servicios de telefonía móvil mediante tarjeta de prepago, podemos diferenciar tres tipos de datos[300]:

a) datos de localización o de tráfico;

b) datos del abonado o usuario y;

c) datos de contenido[301].

Todos ellos son datos personales, entendidos como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"[302].

---

299 Véase mi trabajo "Algunas cuestiones relativas a la protección de las personas físicas en el tratamiento de datos personales en materia penal. La transposición de la Directiva 2016/680 por la Ley 7/2021, de 26 de mayo", en *Revista de derecho y proceso penal, Aranzadi*, número 63, 2021, 46 págs.

300 Véase a este respecto a VÁZQUEZ SECO, Luis, "Incorporación de datos al proceso. Vigencia de la Ley 25/2007 de 18 de octubre de conservación de datos relativos a las comunicaciones electrónicas y a redes públicas e interpretación de la Ley a la luz de la reforma operada por LO 13/2015", en https://www.fiscal.es/

301 Véase el trabajo de PÉREZ GIL, Julio y GONZÁLEZ LÓPEZ, Juan José, "Cesión de datos personales para la investigación penal. Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal", *Diario La Ley*, Nº 7401, Sección Doctrina, 13 de Mayo, 2010, Año XXXI, Editorial LA LEY 3661/2010, págs. 6 y 7.

302 Definición dada en el artículo 4 del Reglamento (UE) 2016/679 del Parlamento

Los primeros se refieren a metadatos que vienen asociados a los datos del mensaje transmitido, y hacen referencia a fecha y hora, duración de la comunicación y datos de localización y movimiento, entre otros[303]. Todos estos datos de forma conjunta permiten dibujar un perfil del individuo que a su vez posibilitan apreciar patrones de comportamiento delictivos. Tal y como se ha indicado "dada la magnitud de la capacidad de agregar, relacionar, y extraer nueva información de datos aparentemente inocuos, resulta difícil precisar qué actividades y prácticas podrán poner en peligro la privacidad de los usuarios de la red"[304].

Los segundos se refieren a los datos que identifican al usuario o abonado y que se han generado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones, como, por ejemplo, el número de los terminales implicados, el IP, titular de los números, incluida la tarjeta pre-pago, etc[305].

Hay autores que hablan también de "datos de conexión" para referirse a "la categoría de datos donde convergen los "datos de tráfico" con los datos del "abonado o suscriptor""[306].

Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), publicado el 4.5.2016, L 119/1, Diario Oficial de la Unión Europea, en https://www.boe.es/doue/2016/119/L00001-00088.pdf.

303 En la STJUE de 2 de octubre de 2018, se indica que "*a efectos de la presente Directiva (se refiere a la de 2002) se entenderá por: b) "datos de tráfico": cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma; c) "datos de localización": cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público; d) "comunicación": cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información*".

304 MARTÍNEZ LÓPEZ-SÁEZ, Mónica, *Una revisión del derecho fundamental a la protección de datos…,* op, cit.

305 Ibídem.

306 QUEVEDO GÓNZALEZ, Josefina, *Investigación y prueba del ciberdelito*, op. cit., pág. 187.

Los últimos son los datos que se refieren al mensaje transmitido, es decir, al contenido concreto de la comunicación. En relación con estos datos, de acuerdo al artículo 1, apartado 3 y al artículo 3 de la Ley 25/2007, no pueden ser conservados por las operadoras de servicios de comunicaciones. Por tanto, la única manera de conseguir estos datos sería a través de autorización judicial en el momento en el que se está llevando a cabo la comunicación puesto que las compañías no pueden conservar en ningún caso estos datos.

Además de los datos transcritos, la reforma de la Ley de Enjuiciamiento Criminal por la LO 13/2015 vino a ampliar el ámbito objetivo de la Ley 25/2007 al establecer en el artículo 588 ter j de la LECrim, la posibilidad de ceder otros datos como son aquellos que por propia iniciativa por motivos comerciales o de otra índole conserven las operadoras.

Como ha señalado la doctrina[307], los momentos en los que estas empresas proveedoras de servicios de Internet y operadoras que prestan servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, pueden o deben colaborar con la Justicia de acuerdo a la Ley de Enjuiciamiento Criminal se circunscribirían a cuatro. El primero de ellos, en la conservación y cesión de datos, artículo 588 ter j de la LECrim; el segundo en la interceptación de las comunicaciones, artículo 588 ter e; el tercero en la orden de conservación de datos de acuerdo al artículo 588 octies de la LECrim; y finalmente, en el registro remoto previsto en el artículo 588 septies b de la LECrim. Son todos ellos momentos diferentes en los que a través de estas diligencias de investigación se requiere la colaboración en algunos casos activa de estas empresas.

Estas diligencias son fundamentales para obtener información relevante para incorporarla posteriormente al proceso penal como prueba. En muchos de los delitos cometidos *on line*, se necesita la colaboración de estas empresas para que los datos almacenados y conservados sean cedidas.

j. La injerencia de las nuevas herramientas o instrumentos para la investigación, seguimiento y sanción de los delitos telemáticos en los derechos fundamentales de las personas

Una de las cuestiones problemáticas que surgen en relación con los nuevos medios de investigación tecnológicos es la posible injerencia de los mismos

307 Véase a QUEVEDO GONZÁLEZ, Josefina, *Investigación y prueba del ciberdelito*, op. cit., págs. 126 a 128.

en los derechos fundamentales de las personas investigadas. A mi parecer, esta es una de las cuestiones más problemáticas puesto que lo fundamental es encontrar un equilibrio entre la posibilidad y necesidad de almacenar y recopilar ingentes cantidades de datos y el asegurar la no agresión de la imparable tecnología en los derechos de las personas. En este sentido, no hay que perder de vista que el Derecho persigue la innovación tecnológica, pero al hacerlo debe salvaguardar, equilibrando, los derechos y libertades personales, fundamentalmente el derecho a la intimidad y a la vida privada, pero también el derecho a la protección de datos personales.

Nuestro Tribunal Constitucional ha delimitado el objeto de protección del derecho fundamental a la protección de datos personales y ha destacado que alcanza: "*a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo*"[308].

Por tanto, la jurisprudencia ha delimitado el derecho a la protección de datos personales de una manera amplia, comprendiendo dentro del mismo cualesquiera datos referidos a la persona.

En el ámbito de la investigación de los ciberdelitos y las nuevas tecnologías, los derechos que pueden verse más afectados serían el derecho a la intimidad y el derecho al secreto de las comunicaciones además del derecho a

308 STC 292/2000. Véase sobre ello el trabajo de FERNÁNDEZ LÓPEZ, Juan Manuel, (Magistrado. Ex-Director de la Agencia de Protección de Datos), *El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario*, en *file:///Users/raqlj/Downloads/Dialnet-ElDerechoFundamentalALaProteccionDeLosDatosPersona-500300.pdf*.

la protección de datos personales y el derecho al propio entorno virtual que, como analizaré a continuación, es un derecho de origen reciente que englobaría a los derechos fundamentales anteriores[309].

Precisamente, porque en la práctica de estas diligencias de investigación pueden verse afectados diferentes derechos fundamentales es necesario que previamente el órgano judicial dicte una autorización judicial. El Tribunal Supremo ha justificado la exigencia de esta autorización judicial precisamente en la incidencia que pueden tener en los derechos fundamentales de las personas y así ha sostenido que: "*Las razones que fundan esa previsión de permiso judicial radican tanto en las posibles injerencias en derechos fundamentales amparadas en un engaño o simulación (derecho a no declararse culpable o a no declarar contra sí mismo; intimidad; inviolabilidad del domicilio en el caso de agentes encubiertos tradicionales); la afectación de derechos de nueva generación como la autodeterminación informativa (recht auf informationelle selbstbestimmung) o el derecho a la identidad virtual - STC 173/2011 de 1 de noviembre - o al propio entorno virtual - STS 204/2016 , de 10 de marzo -; la interdicción de arbitrariedad de los poderes públicos; así como también en la necesidad de dotar al agente de inmunidad* en sentido figurado y no técnico jurídico- respecto de actuaciones que objetivamente podrían ser típicas y, por tanto, susceptibles de persecución penal. A ello se refiere específicamente el párrafo 2º del art. 282 bis. 6 -envío de archivos ilícitos-"[310].

Por tanto, la necesidad de control judicial obedece a la posible injerencia en los derechos fundamentales de las personas, los cuales pueden ser muy variados, desde el derecho al secreto de las comunicaciones, el derecho a la intimidad, el derecho a la protección de datos personales hasta el derecho al propio entorno virtual. Este último derecho nace como consecuencia de la implantación de las nuevas tecnologías ya que el acceso a la información tecnológica puede afectar a una heterogeneidad de derechos, como veremos seguidamente, se habla de "plurifuncionalidad" de los datos almacenados y era necesario una regulación unitaria para garantizar precisamente la no vulneración de ningún derecho fundamental teniendo en cuenta que la protección de cada uno tiene una diferente intensidad. De hecho, en el ámbito de la ciencia, y en lo que respecta a la prueba científica, en la actualidad la en-

309 Véase el trabajo de QUEVEDO GONZÁLEZ, Josefina, *Investigación y prueba en los ciberdelitos*, op. cit., págs. 137 y ss.

310 STS de 11 de abril de 2018, TOL6.586.812.

trada en el proceso de esta nueva categoría, tanto en su obtención, admisión, como práctica y valoración, supone la afectación de derechos fundamentales de diferente naturaleza sobre los cuales no se puede realizar una casuística, solo poner ejemplos, dado el avance de la ciencia, y teniendo en cuenta que en el futuro surgirán probablemente nuevos métodos científicos creadores de alguna nueva prueba de estas características. Al respecto, señala la doctrina que se está empezando a hablar de derechos de cuarta generación, que son aquellos surgidos como consecuencia de los nuevos avances tecnológicos. Por tanto, los ejemplos que se indican son sólo ejemplos a efectos de reflejar las numerosas cuestiones que pueden surgir en relación al procedimiento de obtención de fuentes de prueba pertenecientes a esta nueva categoría probatoria[311].

j.1 El secreto de las comunicaciones

Parece que cuando hablamos de las diligencias de investigación tecnológicas estas siempre inciden en el derecho al secreto de las comunicaciones porque suponen precisamente investigar sobre las comunicaciones, aunque sean electrónicas, pero ello no siempre es así. No siempre que se practican diligencias de investigación tecnológicas se incide en el derecho al secreto de las comunicaciones, la característica fundamental para determinar si se puede violentar el derecho al secreto de las comunicaciones reside precisamente en si la comunicación está todavía en marcha o si, por el contrario, esa comunicación ya ha finalizado. En este sentido, sólo las comunicaciones que están en marcha pueden verse afectadas por el derecho al secreto de las comunicaciones, de otra forma, puede verse vulnerado el derecho a la intimidad si son datos que pueden revelar información de la vida privada del comunicante, o el derecho a la autodeterminación informativa, pero en ningún caso afectarían al derecho al secreto de las comunicaciones.

A este respecto el Tribunal Supremo, recogiendo la doctrina del Tribunal Constitucional, ha establecido en una sentencia relativamente reciente que*: "Las especiales características del instrumento técnico sobre el que se asentó la investigación judicial (smartphone)* que, por un lado, permite la comunicación telemática en sus distintas modalidades de conversación oral o escrita y, aun en esta, por distintos instrumentos como son los mensajes electróni-

311 SANCHEZ RUBIO, Ana, *La prueba científica en la justicia penal*, Tirant on line, op. cit., DOCUMENTO TOL7.571.683.

cos por *emails,* o la mensajería instantánea *sms (short message service,* por sus siglas en inglés*), o a través de plataformas de comunicación específicas como WhatsApp* o *telegram,* y que por otro lado realiza un registro de todos los datos referidos a estas conversaciones, además de otras circunstancias que dependen de la configuración personal del usuario, tales como fotografías, vídeos, historial de geolocalización, navegación por internet, o el rastro de las distintas iniciativas que haya impulsado el usuario durante la utilización de las distintas utilidades o aplicaciones informáticas que tenga instaladas, justifica principiar por la aclaración, ya reiterada en numerosas sentencias *de esta Sala, que distingue entre las comunicaciones en marcha, de aquellos otros procesos de correspondencia o de relación que ya están cerrados. Solo las primeras se encuentran afectadas por el derecho al secreto de las comunicaciones, mientras que aquellas que terminaron y cuya existencia presente deriva de un proceso técnico o electrónico de conservación o documentación, a lo que conciernen es al derecho a la intimidad y/o, en su caso, a la autodeterminación informativa mediante el control de datos personales. Así lo recoge reiterada jurisprudencia de esta Sala (SSTS 1235/2002, de 27 de junio; 1647/2002, de 1 de octubre; 528/2014; 864/2015, de 10 de diciembre o 849/2018, de 23 de octubre), y lo plasma una estable doctrina constitucional que, entre otras en su sentencia 70/2002, de 3 de abril, expresaba que: "(...) La protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos"*[312].

La distinción entre vulnerar un derecho u otro es importante porque la protección jurisdiccional es diferente en relación a su intensidad, de forma que se le otorga una mayor protección al derecho a la intimidad domiciliaria (artículo 18.2 de la CE) y al secreto de las comunicaciones (artículo 18.3 de la CE), por ejemplo, que al derecho a la intimidad personal o al derecho a la protección de datos personales puesto que estos últimos pueden verse limitados cuando existe un interés que prevalece sobre ellos.

Precisando aún más, señala el Tribunal Supremo en la misma sentencia citada anteriormente que: *"La distinción resulta de particular transcendencia si se considera que nuestra norma constitucional atribuye a la función jurisdiccional la garantía de la afectación del derecho únicamente respecto de la intimidad domiciliaria (art. 18.2 CE) y el secreto de las comunicaciones*

312 STS de 14 de octubre de 2019, DOCUMENTO TOL7.531.381.

(art. 18.3), sin que tal monopolio se aprecia respecto del resto de derechos que en el mismo artículo se contienen, para los que nuestro ordenamiento jurídico reconoce la posibilidad de ser limitados en situación de prevalencia de otros intereses públicos en conflicto, pero sin estar sometida la intromisión a un pronunciamiento judicial, siendo los ejemplos más frecuentes y habituales los cacheos personales realizados por agentes policiales en determinados supuestos y circunstancias, además de registros en maleteros de vehículos o los que pueden desarrollarse en establecimiento públicos.

En nuestra reciente sentencia 489/2018, de 23 de octubre, dejábamos perfecta constancia de la consideración de esta Sala respecto de la cuestión que el recurso suscita, por lo que debemos necesariamente remitirnos a lo allí expuesto. Decíamos en aquella sentencia que, partiendo de la plurifuncionalidad de los datos que se almacenan en cualquier ordenador y otros dispositivos asimilables por su capacidad de acumular información vinculada a una persona (smartphone), se conviene en la necesidad de un tratamiento unitario a partir de la proclamación de un derecho del individuo al entorno digital. Sería un derecho de nueva generación que serviría para alumbrar y justificar distintos escalones de protección jurisdiccional (SSTS 342/2013, de 17 de abril; 587/2014, de 24 de febrero, y 587/2014, de 18 de julio).

La sentencia destaca que, en consideración a esta nueva necesidad, nuestra renovada legislación procesal ha contemplado el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies) como una diligencia específica que reclama garantías singulares y diferentes al registro de otros muebles o inmuebles. Destacábamos que en este caso hay un plus que viene determinado no solo porque puede suponer desnudar virtualmente a una persona, sino porque incide también en otro derecho de nueva generación como es la autodeterminación informativa"[313].

Está aceptado tanto por la doctrina como por la jurisprudencia que los mensajes de correo electrónico[314], una vez que se han descargado desde el

313 STS de 14 de octubre de 2019, DOCUMENTO TOL7.531.381.

314 Desde un punto de vista técnico, en el correo electrónico se podrían diferenciar dos partes; por un lado, el cuerpo del correo y, por otro, las cabeceras. El cuerpo del correo estaría formado por el contenido del mensaje en sí, incluyendo dentro de él los posibles adjuntos, y su contenido depende exclusivamente de lo que haya querido incluir el usuario del mismo. En relación con las cabeceras, contienen información tanto facilitada por el usuario del correo como por la añadida por el servidor o servidores (asunto, destinatario, emisor, por los que pasa el correo hasta llegar a su destino. Véase a QUEVEDO GÓNZALEZ, Josefina, *Investigación y prueba del ciberdelito*, op. cit., págs. 214 y ss, concretamen-

servidor y han sido leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de formar parte del ámbito que sería propio de la inviolabilidad del secreto de las comunicaciones[315]. Cuando la comunicación ha finalizado, la información contenida en el mensaje es, desde ese momento, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya protección constitucional no se discute, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones[316].

Además, hay que reseñar que en las comunicaciones a través de medios electrónicos el derecho al secreto de las comunicaciones, la comunicación ampara también a los datos que acompañan al proceso de comunicación, es decir, cualquier dato informático. En relación con lo que se entiende por datos informáticos hay que acudir a la definición ofrecida por el Convenio de Ciberdelincuencia de Budapest, donde en su artículo 1.d), lo define como "cualquier dato informático relativo a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que impiden el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación y el tipo de servicio subyacente".

En definitiva, en relación con las actuaciones que afecten al derecho a la intimidad, la Constitución no establece una reserva absoluta a la autoridad judicial, a diferencia de lo que ocurre con el derecho a al inviolabilidad del domicilio o con el derecho al secreto de las comunicaciones por ejemplo, por

---

te nota 380, donde se indica la relevancia de estas cabeceras puesto que son importantes para determinar los datos de tráfico y algunos aspectos relevantes en la investigación sobre todo de la autoría de los correos electrónicos, en concreto para conocer el origen, el itinerario y el destino que un mensaje ha seguido entre el emisor y el receptor puesto que cada vez que el mensaje pasa por un servidor de correo éste añade un campo de datos a las cabeceras con la etiqueta Received, especificándose el nombre del servidor, su dirección IP, el servidor del correo utilizado así como la fecha y hora en la que se emitió y se recibió el mensaje.

315 El proceso de comunicación a través de la red puede dividirse en tres fases. La primera es la transmisión; la segunda el almacenamiento del correo en el servidor del receptor y; la tercera el acceso del recepto al mensaje. En este sentido, la transmisión concluiría cuando el destinatario accede al contenido del mensaje y no cuando recibe la comunicación. Cuando el proceso de comunicación está en curso es cuando se vería afectado el derecho al secreto de las comunicaciones, véase para una mayor profundización a QUEVEDO GÓNZALEZ, Josefina, *Investigación y prueba en el ciberdelito*, op. cit., págs. 158 y ss.

316 STS 342/2013, de 17 de abril, Número de recurso: 146/2012, ECLI: ESTS:2013:2222.

tanto, la jurisprudencia ha venido permitiendo que las Fuerzas y Cuerpos de Seguridad del Estado siempre de manera excepcional y en determinados casos de urgencia y necesidad y con la suficiente y precisa habilitación legal lleven a cabo prácticas de investigación que constituyan una injerencia leve en el derecho a la intimidad del afectado.

En consecuencia, en relación con el delito de "sexting", objeto de nuestro estudio entre otros delitos, la posibilidad de los agentes de policía de observar o registrar la agenda de un teléfono móvil donde consta el listado de números identificados con un nombre y los números de teléfono correspondientes no supone, de acuerdo a la doctrina del Tribunal Supremo una injerencia en el derecho al secreto de las comunicaciones debiendo por tanto tener autorización judicial, sino una injerencia en el derecho a la intimidad para lo cual, como decía anteriormente, no se necesita esa autorización[317]. La reforma de la LECrim por la Ley Orgánica 13/2015, regulando las diligencias de investigación tecnológicas ha sido acorde con esta doctrina jurisprudencial, al no exigir legalmente el control judicial

Para lo que sí se necesita autorización judicial es para intervenir la comunicación, es decir, para acceder a ese correo electrónico antes de que haya sido leído por su destinatario. Aquí es verdaderamente importante para tratar de averiguar la autoría de los delitos de "sexting", "grooming", etc., y los posibles participantes, el estudio de las cabeceras de un correo electrónico porque determina los distintos servidores de correo por los que ha transitado dicho mensaje, además se puede localizar los usuarios que se han descargado el mensaje o que lo han reenviado, y también se puede averiguar si un correo proveniente de un cierto dominio de internet se ha procesado efectivamente en servidores relacionados con dicho dominio o por el contrario proviene de sistemas que en principio no son propios del mismo, lo que supondría que el mensaje ha podido ser manipulado y, por tanto, falseado[318].

– En relación con los prestadores de servicios de mensajería electrónica, los cuales pueden ser requeridos por el juzgado para que acrediten la autenticidad e integridad del contenido de mensajes electrónicos, aportando copias del contenido de las comunicaciones, se plantea la cuestión de si pueden ha-

317 SSTS 663/2011, de 7 de julio, Número de Recurso 10603/2010, ECLI: ES:TS:2011:5170; STS 104/2011, de 1 de marzo, Número de Recurso: 1174/2010, ECLI:ES:TS;2011/1316, entre otras.

318 QUEVEDO GONZÁLEZ, Josefina, *Investigación y prueba del ciberdelito*, op. cit., pág. 215, concretamente nota 380.

cerlo o, por el contrario, ello supone vulnerar algún derecho fundamental de los interlocutores.

Si acudimos a la Ley General de Telecomunicaciones[319], en su artículo 39, se prevé que: "*1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias*".

En concreto, en el artículo 18 de nuestra Constitución, apartados 3 y 4, se establece que: "*3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial". 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*[320].

Si bien, en aquellos medios de Internet, como por ejemplo chats o foros donde se comunican varias personas a la vez de forma simultánea y en tiempo real, y no comunicaciones bidireccionales cerradas entre dos usuarios, sino que son accesibles a cualquier usuario de Internet no pueden tener la consideración de comunicaciones privadas, por tanto, no estarían amparadas por el derecho al secreto de las comunicaciones puesto que es el propio usuario el que accede a la red pública y asume que muchos de los datos se convierten en públicos para todos los usuarios. Por tanto, para la grabación u observación de estas comunicaciones no es necesaria la autorización judicial. Son comunicaciones públicas y, por tanto, no reservadas a los titulares de la misma. No se necesita autorización para hacer público lo que ya es público.

j.2 El derecho a la intimidad

Como he comentado anteriormente, la práctica de las diligencias de investigación tecnológica puede vulnerar, además del secreto a las comunicaciones cuando éstas están en marcha, el derecho a la intimidad personal recogido en el artículo 18.1 de la CE[321], además de otros derechos fundamentales.

---

319 Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, publicada en el BOE, número 114, de 10/05/2014.

320 La LO 13/2015, es la plasmación concreta de esa ley limitadora del uso de la informática que configura la Constitución.

321 Ha señalado el Tribunal Constitucional (STC 173/2011) que: *"el derecho a la inti-*

El art. 18 de la CE garantiza el derecho a la intimidad personal y familiar, pero como indica la doctrina "no define ni perfila el significado de la noción de intimidad, ni su relación con el resto de manifestaciones de este derecho tan personalísimo"[322]. Por ello, nuestro Tribunal Constitucional ha llevado a cabo una minuciosa labor de definición y concreción de este derecho fundamental como lo ha hecho con otros muchos.

Partiendo de esta premisa, en lo que se refiere precisamente al derecho a la intimidad, nuestro Tribunal Constitucional ha venido a manifestar a este respecto, en relación en concreto con los datos que se pueden alojar en un ordenador personal, que: "*el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad*

---

midad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 CE), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (SSTC 207/1996 , de 16 de diciembre, FJ 3; 186/2000, de 10 de julio, FJ 5; 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 4; y 159/2009, de 29 de junio, FJ 3). De forma que "lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio" (SSTC 127/2003, de 30 de junio, FJ 7 y 89/2006, de 27 de marzo, FJ 5). Del precepto constitucional citado se deduce que el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2"). En *Tirant on line*, DOCUMENTO TOL2.288.705.

322 Véase a este respecto el trabajo de MARTÍNEZ DE PISÓN, José, "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional", en AFD, 2016 (XXXII), pp. 409-430, ISSN: 0518-0872.

por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información"[323].

Hemos visto que la protección jurisdiccional que se le confiere a este derecho es de menor intensidad que la que se le confiere al derecho al secreto de las comunicaciones. En este sentido, la jurisprudencia ha mantenido que: "*El derecho a la intimidad es constitucionalmente susceptible de limitación o sacrificio, aun cuando se proyecte en los instrumentos tecnológicos que contemplamos, siempre que la resolución judicial habilitante de la injerencia en el derecho sea conforme con unas exigencias de legalidad constitucional que se entienden claramente satisfechas en el presente caso. En el caso de autos, la solicitud de volcado y clonado del contenido de la información existente en los teléfonos móviles de los recurrentes se concretó en el oficio de la Guardia Civil, acordándose su práctica por Auto del Juez de Instrucción de 18 de septiembre de 2015. La resolución no solo contiene una exteriorización de los motivos que conducen al juez a autorizar la injerencia en el derecho a la intimidad, sino que refleja una acertada satisfacción de los principios de proporcionalidad y razonabilidad del acceso a tal información*"[324].

Los presupuestos que legalmente habilitan la intromisión en el derecho

323 Ibídem.

324 STS de 14 de octubre de 2019, DOCUMENTO TOL7.531.381.

fundamental a la intimidad personal de acuerdo con los parámetros constitucionales se ponen de manifiesto en la siguiente sentencia que literalmente transcribo:

"tampoco podrá considerarse ilegítima aquella injerencia o intromisión en el derecho a la intimidad que encuentra su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos (STC 159/2009, de 29 de junio, FJ 3). A esto se refiere nuestra doctrina cuando alude al carácter no ilimitado o absoluto de los derechos fundamentales, de forma que el derecho a la intimidad personal, como cualquier otro derecho, puede verse sometido a restricciones (SSTC 98/2000, de 10 de abril, FJ 5; 156/2001, de 2 de julio, FJ 4; y 70/2009, de 23 de marzo, FJ 3). Así, aunque el art. 18.1 CE no prevé expresamente la posibilidad de un sacrificio legítimo del derecho a la intimidad -a diferencia de lo que ocurre en otros supuestos, como respecto de los derechos reconocidos en los arts. 18.2 y 3 CE -, su ámbito de protección puede ceder en aquellos casos en los que se constata la existencia de un interés constitucionalmente prevalente al interés de la persona en mantener la privacidad de determinada información. Precisando esta doctrina, recordábamos en la STC 70/2002, de 3 de abril, FJ 10, (resumiendo lo dicho en la STC 207/1996, de 16 de diciembre, FJ 4) que los requisitos que proporcionan una justificación constitucional objetiva y razonable a la injerencia en el derecho a la intimidad son los siguientes: la existencia de un fin constitucionalmente legítimo; que la medida limitativa del derecho esté prevista en la ley (principio de legalidad); que como regla general se acuerde mediante una resolución judicial motivada (si bien reconociendo que debido a la falta de reserva constitucional a favor del Juez, la ley puede autorizar a la policía judicial para la práctica de inspecciones, reconocimientos e incluso de intervenciones corporales leves, siempre y cuando se respeten los principios de proporcionalidad y razonabilidad) y, finalmente, la estricta observancia del principio de proporcionalidad, concretado, a su vez, en las tres siguientes condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)» (STC 89/2006 , de 27 de marzo, FJ 3).

Por lo que se refiere a la concurrencia de un fin constitucionalmente legítimo que puede permitir la injerencia en el derecho a la intimidad, este Tribunal ha venido sosteniendo que reviste esta naturaleza "el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal» (SSTC 25/2005, de 14 de febrero, FJ 6 y 206/2007, de 24 de septiembre, FJ 6). En efecto, «la persecución y castigo del delito constituye un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana, bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE» [SSTC 127/2000, de 16 de mayo, FJ 3 a) y 292/2000, de 30 de noviembre, FJ 9]. También hemos precisado que «reviste relevancia e interés público la información sobre los resultados positivos o negativos que alcanzan en sus *investigaciones* las fuerzas y cuerpos de seguridad, especialmente si los delitos cometidos entrañan una cierta gravedad o han causado un impacto considerable en la opinión pública, extendiéndose aquella relevancia o interés a cuantos datos o hechos novedosos puedan ir descubriéndose por las más diversas vías, en el curso de las *investigaciones* dirigidas al esclarecimiento de su autoría, causas y circunstancias del hecho delictivo» (STC 14/2003 , de 28 de enero, FJ 11).

De lo anterior, se deduce que el legislador ha de habilitar las potestades o instrumentos jurídicos que sean adecuados para que, dentro del respeto debido a los principios y valores constitucionales, las fuerzas y cuerpos de seguridad del Estado cumplan con esta función de averiguación del delito. Como reseñamos en la STC 70/2002 , de 3 de abril, FJ 10, "[p]or lo que respecta a la habilitación legal en virtud de la cual la policía judicial puede practicar la injerencia en el derecho a la intimidad del detenido, en el momento de la detención, las normas aplicables son, en primer lugar el art. 282 LECrim, que establece como obligaciones de la policía judicial la de averiguar los delitos públicos que se cometieron en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro poniéndolos a disposición de la Autoridad Judicial'. En la misma línea, el art. 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, establece como funciones de éstos, entre otras, f) 'prevenir la comisión de actos delictivos'; g) 'investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente y elaborar los

informes técnicos y periciales procedentes'. Por último, el art. 14 de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana, establece que las autoridades competentes podrán disponer las actuaciones policiales estrictamente necesarias para asegurar la consecución de las finalidades previstas en el art. 1 de esta Ley, finalidades entre las que se encuentra la prevención de la comisión de delitos". Según la citada Sentencia (mismo fundamento jurídico) existe, por tanto, "una habilitación legal específica que faculta a la policía para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente. Entre esas diligencias (que la Ley no enumera casuísticamente, pero que limita adjetivándolas y orientándolas a un fin) podrá encontrarse la de examinar o acceder al contenido de esos instrumentos o efectos, y en concreto, de documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que -como exige el propio texto legal- ello sea necesario (estrictamente necesario, conforme al art. 14 de la Ley Orgánica 1/1992), estricta necesidad que habrá de valorarse atendidas las circunstancias del caso y que ha de entenderse como la exigencia legal de una estricta observancia de los requisitos dimanantes del principio de proporcionalidad. Así interpretada la norma, puede afirmarse que la habilitación legal existente cumple en principio con las exigencias de certeza y seguridad jurídica dimanantes del principio de legalidad, sin perjuicio de una mayor concreción en eventuales reformas legislativas".

Precisando aún más en lo que se refiere concretamente a la exigencia de autorización judicial, en la misma sentencia se indica que: "*el criterio general, conforme a nuestra jurisprudencia, es que sólo pueden llevarse a cabo injerencias en el ámbito de este derecho fundamental mediante la preceptiva resolución judicial motivada que se adecue al principio de proporcionalidad (SSTC 207/1996, de 16 de diciembre, FJ 4; 25/2005, de 14 de febrero, FJ 6; y 233/2005 , de 26 de septiembre, FJ 4). Esta regla no se aplica, también según nuestra doctrina, en los supuestos en que concurran motivos justificados para la intervención policial inmediata, que ha de respetar también el principio de proporcionalidad. De manera significativa hemos resaltado en la STC 70/2002, de 3 de abril, que "la regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir*

ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad" [FJ 10 b) 3]. Bien entendido que "la valoración de la urgencia y necesidad de la intervención policial ha de realizarse ex ante y es susceptible de control judicial ex post, al igual que el respeto al principio de proporcionalidad. La constatación ex post de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales" [FJ 10 b) 5]. En esta línea en la STC 206/2007, de 24 de septiembre, FJ 8, afirmábamos que "la regla general es que sólo mediante una resolución judicial motivada se pueden adoptar tales medidas y que, de adoptarse sin consentimiento del afectado y sin autorización judicial, han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad". En esta Sentencia razonábamos que no había existido una autorización judicial previa para la injerencia acaecida en el derecho a la intimidad (en este caso un análisis de sangre interesado por la Guardia Civil), entendiéndose como relevante el hecho de que tampoco por los órganos judiciales se había efectuado posteriormente una "ponderación de los intereses en conflicto teniendo en cuenta el derecho fundamental en juego que les condujera a considerar justificada –a la vista de las circunstancias del caso– la actuación policial sin previa autorización judicial" (mismo fundamento jurídico)"[325].

En definitiva, el ámbito de protección del derecho a la intimidad puede ceder cuando existe un fin constitucionalmente legítimo como es el interés público en la persecución de los delitos. Por supuesto que el consentimiento del afectado legitima la injerencia del Estado en el derecho a la intimidad ya que, como ha señalado el Tribunal Constitucional, corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conoci-

325 Sentencia del Tribunal Constitucional 173/2011, en Tirant on line, DOCUMENTO TOL2.288.705.

miento ajeno, aunque dicho consentimiento puede ser revocado en cualquier momento[326].

La información sobre la diligencia a practicar es preceptiva para que el investigado pueda prestar el consentimiento. Ahora bien, este consentimiento, tal y como admite la jurisprudencia, no necesita ser expreso, pudiendo ser tácito pero que se derive de actos concluyentes. También puede ser verbal[327].

También hay que tener en cuenta que, aunque se haya prestado el consentimiento, la injerencia del Estado en el derecho a la intimidad no puede subvertir "*los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida*" (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2)[328].

j.3 El derecho al propio entorno virtual

Comienzo este apartado destacando unos párrafos de la Exposición de Motivos de la LO 13/2015 que resumen brevemente la importancia de los instrumentos tecnológicos en relación con la información que pueden llegar a proporcionar. Así, se establece que la reforma "*descarta cualquier duda acerca de que esos instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción. De ahí la exigente regulación respecto del acceso a su contenido*". Y es que estos instrumentos contienen información y, por tanto, datos de diferente naturaleza lo que a su vez conlleva que su acceso pueda afectar a diferentes derechos. El legislador así lo ha entendido y ha regulado de forma unitaria los datos contenidos en estos instrumentos, datos que configuran un derecho constitucional de nueva generación, en concreto, el derecho a la protección del propio entorno virtual o a la identidad virtual. Por tanto, este derecho ostentaría identidad propia o autónoma, independientemente de los otros derechos[329]. Este derecho al propio entorno virtual es una de las consecuencias

326 Véanse entre otras STC 83/2002, de 22 de abril; STC 196/2006, de 3 de julio; STC 173/2011, de 7 de noviembre y STC 159/2009, de 29 de junio.

327 STC 173/2011, citada.

328 Ibídem.

329 El Tribunal Supremo en STS de 23 de octubre de 2018, núm. 489/2018, DOCUMENTO TOL6.917.487, ha manifestado que: "*Algunos precedentes alientan la aparición de un derecho vinculado a los mencionados pero con cierta vocación de emanciparse para cobrar autonomía e identidad propias. Partiendo de la plurifuncionalidad* de los

de lo que ha dado en llamarse transformación digital. Se trata, en este caso, de la transformación digital del derecho a la intimidad[330].

En este sentido, tanto los derechos al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1 CE), como el derecho a la inviolabilidad domiciliaria (art. 18.2 CE), y el derecho al secreto de las comunicaciones (art. 18.3 CE) o el derecho a la protección de datos (art. 18.4 CE)[331], constituyen manifestaciones de la intimidad, sin embargo, no todos ostentan la misma protección constitucional, por ello, es relevante que el legislador configure como derecho autónomo a el derecho al propio entorno virtual. Todos estos datos sueltos afectan al derecho a la intimidad, pero además pueden suponer el diseño del perfil personal del sujeto titular de esos datos. Por ello, la protección a todos estos datos ha de ser integral y no de forma aislada.

Este nuevo derecho tendría su fundamento no tanto en la consideración individualizada de los datos obtenidos de una persona a través de las nuevas tecnologías, puesto que pueden no indicar nada, sino en la consideración conjunta de todos ellos, puesto que analizados en su conjunta pueden llegar

---

datos que se almacenan en cualquier ordenador y otros dispositivos asimilables por su capacidad de acumular información vinculada a una persona (*smartphone) se conviene en la necesidad de un tratamiento unitario a partir de la proclamación de un derecho al entorno digital. Sería un derecho de nueva generación que serviría para alumbrar y justificar distintos escalones de protección jurisdiccional (SSTS 342/2013, de 17 de abril; 587/2014, de 24 de febrero, y 587/2014, de 18 de julio).*

De ahí que en nuestra renovada legislación procesal haya emergido en fechas recientes, como diligencia específica que reclama garantías singulares (diferentes al registro de un vehículo o una maleta, por ejemplo) el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a) LECrim y ss, introducidos por la LO 13/2015, de 5 de octubre). Es normativa, no aplicable al presente supuesto: el mandato va dirigido a las fuerzas policiales y, además, es legislación no vigente en el momento de los hechos. Pero ayuda la referencia en cuanto que en buena medida tal legislación se limita a conferir formato normativo a ideas ya presentes y exigidas en jurisprudencia precedente".

330 SANCHIS CRESPO, (con VELASCO, Eloy), *Delincuencia informática. Tipos delictivos e investigación*..., op. cit., pág. 262.

331 Se trata de un derecho de configuración jurisprudencial a través de un conjunto de sentencias que tienen su origen con la STC 254/1993 y culminan con la STC 292/2000. Véase *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, publicación que pertenece al Instituto Nacional de Tecnologías de la Comunicación (INTECO) y a la Agencia Española de Protección de Datos, febrero 2009, pág. 81.

a descubrir características relevantes de la personalidad de su titular[332]. En definitiva, todos estos datos en su conjunto dibujarían un perfil altamente descriptivo de la personalidad de su titular que es necesario proteger frente a las intromisiones tanto de terceros como de los poderes públicos, por cuanto afectan a la misma peculiaridad o individualidad de la persona[333].

Concretamente, este derecho serviría para vislumbrar y justificar distintos escalones de protección jurisdiccional puesto que, como he indicado anteriormente, no ostenta la misma protección el derecho al secreto de las comunicaciones que el derecho a la intimidad personal, por tanto, ese nuevo derecho que requiere autorización judicial para limitarlo englobaría a su vez una heterogeneidad de derechos que se verían afectados.

En este sentido, señala la jurisprudencia que "*la razón de ser de la necesidad de esta autorización judicial con carácter generalizado es la consideración de estos instrumentos como lugar de almacenamiento de una serie compleja de datos que afectan de modo muy variado a la intimidad del investigado como ya señalaba la STS 342/2013 (comunicaciones a través de sistemas de mensajería, por ejemplo, tuteladas por el art 18 3º CE, contactos o fotografías, por ejemplo, tuteladas por el art 18 1º CE que garantiza el derecho a la intimidad, datos personales y de geolocalización, que pueden estar tutelados por el derecho a la protección de datos, art 18 4º CE). Es por ello por lo que el Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual*"[334].

Por tanto, para garantizar una protección eficaz no hay que atender a los datos de forma separada puesto que cada dato tendría un régimen diferente sino que hay que hacerlo de forma conjunta, de otra forma, la posibilidad de que los agentes policiales acceden a cualquier dato sería nula o escasa ya que algunos datos estarían protegidos por el derecho a la intimidad y otros por el derecho a la inviolabilidad de las comunicaciones y ello teniendo en cuen-

---

332 Véase a QUEVEDO GONZÁLEZ, Josefina, *Investigación y prueba del ciberdelito*, op. cit., pág. 166.

333 Así ha sido puesto de manifiesto por nuestro Tribunal Constitucional en STC 173/2011, citada en varias ocasiones por su relevancia en la materia.

334 Auto de la Audiencia Provincial de Valladolid, de 28 de mayo de 2019, DOCUMENTO TOL7.356.285.

ta que todos los datos estarían contenidos en el mismo dispositivo. El Tribunal Supremo ha manifestado que "*la contemplación disgregada de cada una de esas realidades con regímenes de protección diferenciados resultaría ineficaz*"[335].

Esta es la razón por la que el Legislador, como señala la jurisprudencia, singulariza el tratamiento a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación como es el derecho a la identidad virtual[336]. La doctrina señala que sería algo así como un "superderecho", en el sentido de que aglutinaría en su interior una multiplicidad de ellos, todos relativos al ámbito de la privacidad, pero de distinto grado[337].

Por tanto, con el acceso a la información de estos nuevos instrumentos tecnológicos el primer derecho que se vería afectado es el derecho a la autodeterminación informativa cuya protección no es tan intensa como la del resto de derechos afectados[338]. A este respecto, el Tribunal Supremo desde hace ya tiempo viene manifestando que: "*Las exigencias del derecho a la autodeterminación informativa, concernido de manera determinante, no son tan intensas en cuanto a la necesidad de intervención judicial. Ese es el primero de los derechos que puede verse afectado. Pero no toda incidencia en ese derecho reclama inexorablemente habilitación judicial como demuestran las simulaciones policiales investigadoras de corta duración (v.gr., requerimiento de droga por un agente que oculta su identidad a quien parece estar vendiéndola en una vía pública) que, según entiende generalizadamente la doctrina y unánimemente la jurisprudencia, no precisan de ese previo plácet* judicial. (STS 835/2013, de 6 de noviembre)". *"Es relevante, de una parte, que en el mundo de la red el empleo de una identidad supuesta es la regla: todos se asoman a ese mundo usando un nick*. En este punto el *ciber* agente encubierto se aparta del agente encubierto convencional en un dato: la asignación de identidad supuesta es una de las vertientes que impulsa a la conveniencia de una autorización. En la red no se produce engaño por la

335 STS 3574/2018- ECLI:ES:TS: 2018: 3754.

336 Véase el Auto de la Audiencia Provincial de Gerona de 27 de marzo de 2018, en Tirant on line, DOCUMENTO TOL7.390.070.

337 SANCHIS CRESPO (con VELASCO, Eloy), *Delincuencia informática. Tipos delictivos e investigación*..., op. cit., pág. 262.

338 El Tribunal Constitucional en Sentencia 292/2000, ya ponía de manifiesto que el derecho a la protección de datos puede verse limitado por entre otros, la averiguación, persecución y castigo del delito.

utilización de pseudónimo. Todos lo utilizan: es una regla de ese espacio de comunicación"[339].

El derecho a la protección de los datos personales no se recoge expresamente en el artículo 18.4 de la Constitución española, aunque se puede entender implícitamente contenido en el mismo como protección contra las amenazas a la dignidad, identidad, libertad e intimidad de las personas. Es un derecho que pone de relieve la necesaria protección de los datos personales frente al tratamiento automatizado de los mismos que afecta al control de "nuestras vidas y personalidad"[340]. Este derecho puede verse limitado fundamentalmente en lo que afecta al tratamiento de los datos personales del investigado en el proceso. En este sentido, el derecho a controlar los datos y, por tanto, el derecho al previo consentimiento para la recogida de los datos y el derecho a acceder, rectificar y cancelar dichos datos puede limitarse o ceder en el transcurso del proceso penal con el fin de garantizar la investigación penal.

Otro de los derechos que puede verse afectado por el acceso a los datos de los instrumentos de comunicación telemática es el derecho a la intimidad, por ello, además de ser necesaria la autorización judicial es necesario que en la misma se justifique la necesidad de dicho acceso llevando a cabo una ponderación de la limitación del derecho afectado. Así, el Tribunal Supremo tiene establecido que: *"Nuestro legislador ha establecido que, salvo autorización de su titular, el acceso a la información y al contenido existente en estos instrumentos de comunicación telefónica o telemática,* además de a los dispositivos de almacenamiento masivo de información digital, no solo precisa de una específica decisión judicial habilitante, sino que requiere de una justificación específica que pondere el singular riesgo de afectación del derecho a la intimidad, incluso en aquellos supuestos en los que la incautación haya venido precedida de otra decisión judicial que limitara el derecho a la intimidad y autorizara el acceso al lugar en el que estos dispositivos pudieran encontrarse (art. 588 sexies a y b). Indicábamos en la sentencia anteriormente citada y que nos sirve de guía*: "La necesidad de esta autorización judicial (subsidiaria del consentimiento: si el afectado accede de forma libre, no hay cuestión) obedece a la consideración de estos instrumentos como esferas de almace-*

339 Sentencia del TS de 11 de abril de 2010, DOCUMENTO TOL6.586.812.

340 PÉREZ ESTRADA, Miren Josune, "La vulneración de datos personales en la aportación de la prueba en el proceso penal", en *Justicia: ¿Garantías versus eficiencia?,* Tirant lo Blanch, 2019, pág. 880, concretamente nota 2.

namiento de una serie compleja y densa de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones tuteladas por el art 18 3º CE; contactos, fotografías, archivos personales, tuteladas por el art 18 1º CE; datos personales y de geolocalización, que pueden cobijarse en el derecho a la protección de datos, art 18 4º CE). La contemplación disgregada de cada una de esas realidades con regímenes de protección diferenciados resultaría ineficaz. Permitido, por ejemplo, el acceso directo de los agentes policiales a estos instrumentos para investigar datos únicamente protegidos por el derecho a la intimidad (v.gr., los contactos incluidos en la agenda), no se podría acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo. El Legislador con buen criterio ha optado por otorgar un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando ese derecho constitucional de nueva generación, el derecho a la protección del propio entorno virtual"[341].

En definitiva, el derecho al propio entorno virtual como categoría única garantiza que se dé una protección adecuada a todos los derechos que se verían afectados por el acceso a la información de los instrumentos tecnológicos o telemáticos teniendo en cuenta que la naturaleza de los datos contenidos en esa información es diferente y, por tanto, la protección también lo sería. El nivel de exigencia del ordenamiento jurídico para legitimar la intromisión en los derechos afectados será diferente, al igual que será diferente la exigencia de protección según que la injerencia lo sea en el núcleo básico o profundo del derecho fundamental afectado o en aspectos básicos que no afectan a su núcleo básico. El Tribunal Supremo en la misma sentencia citada anteriormente establece esta consideración al manifestar que: "*en lo que atañe a que la heterogeneidad de los derechos afectados por el acceso a la información existente en estos dispositivos justificaba un trato unitario, decía la misma sentencia: "La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que,*

341 STS de 14 de octubre de 2019, TOL 7.531.381.

más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos"[342].

Es necesario poner de relieve el peligro que puede suponer este rastro o huella digital y el control del ciberespacio. Como se ha puesto de manifiesto existe el riesgo por parte de los Gobiernos de ejercer dicho control sobre la vida de los ciudadanos, por lo que han de establecerse las medidas legales oportunas para la protección de las personas, en concreto, la protección de los datos personales, frente a la intromisión en su privacidad[343].

En definitiva, la necesidad de contar con un acto jurisdiccional que habilite la intervención de un ordenador para acceder a su contenido es manifiesta tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para la injerencia en los derechos a la inviolabilidad de las comunicaciones y a la intimidad[344]. Como ha indicado la jurisprudencia que acabo de citar se trata de contemplar de forma unitaria mensajes, imágenes, documentos y, en general todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado con la finalidad de otorgarle una mayor protección jurisdiccional[345].

---

342 Ibídem.

343 Véase PLAZA PENADÉS, Javier, "La "piratería" en la Red. Una asignatura pendiente para el Gobierno de España", en *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 40, Enero - Abril 2016.

344 Véase a ZARAGOZA TEJADA, Javier Ignacio (coord..), *Investigación tecnológica y derechos fundamentales*, 1ª ed., noviembre de 2017, en https://idoc.pub/documents/zaragoza-tejada-javier-ignacio-investigación-tecnologicas-y-derechos-fundamentalespdf-d4p7pm7vzd4p

345 PÉREZ ESTRADA, Miren Josue, "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información", en *Revista Brasileña de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1297-1330, set.-dez. 2019.págs. 1297 y ss.

k. La regulación en el ámbito europeo

Sin entrar en profundidad en la regulación europea no puedo dejar de comentar cuál ha sido la situación legal hasta hace poco y cual la situación actual, puesto que en los últimos años se ha avanzado bastante en materia de prueba transnacional o transfronteriza en su modalidad tanto física como en formato electrónico, telemático o virtual.

En este sentido, recientemente en el ámbito de la Unión Europea se han dictado instrumentos jurídicos que posibilitan y potencian una mayor eficacia en la lucha contra la criminalidad a través de la cooperación policial y judicial internacional tanto en forma física como virtual. Estos instrumentos posibilitan que la investigación de los hechos delictivos transfronterizos sea más fácil puesto que no va a ser necesario acudir a instancias internacionales para investigar las huellas o rastros dejados en el entorno digital o virtual, sino que los propios Estados van a ver reforzados sus poderes de investigación o de obtención de pruebas en otro Estado miembro.

Desde hace tiempo se viene insistiendo en la necesidad de regular el tratamiento de los datos personales en el ámbito de las nuevas tecnologías por la implicación que puede suponer en los derechos fundamentales de las personas, así en el ámbito europeo podemos indicar algunas disposiciones que han sido tomadas ocupándose de esta materia. De manera cronológica se debe empezar citando el Convenio núm. 108 del Consejo de Europa sobre protección de los datos informatizados de carácter personal (1981), vinculante para España, y las Recomendaciones del Comité de Ministros que lo desarrollan, en particular, la Recomendación sobre datos personales utilizados en el sector policial (1987) y la Recomendación sobre privacidad en Internet (1999). El preámbulo de esta última Recomendación -R(99) 5, de 23 de febrero de 1999- pone de relieve que "*el desarrollo de las tecnologías y la generalización de la recogida y del tratamiento de datos personales en las 'autopistas de la información' suponen riesgos para la intimidad de las personas naturales" y que "las comunicaciones con ayuda de las nuevas tecnologías de la información están también sujetas al respeto de los derechos humanos y de las libertades fundamentales, en concreto al respeto a la intimidad y del secreto de las comunicaciones, tal y como se garantizan en el artículo 8 de la Convención Europea de los Derechos Humanos*". En este misma Recomendación se manifiesta que: "*el uso de Internet supone una responsabilidad en cada acción e implica riesgos para la intimidad" (introducción), por cuanto*

cada visita a un sitio de Internet deja una serie de "rastros electrónicos" que pueden utilizarse para establecer "un perfil de su persona y sus intereses" (apartado II, 2), subrayando también que la dirección de correo electrónico constituye "un dato de carácter personal que otras personas pueden querer utilizar para diferentes fines" (apartado II, 6)"[346].

Además, cabe mencionar las resoluciones del Parlamento Europeo de 17 de septiembre de 1996 y de 17 de diciembre de 1998, relativas al respeto de los derechos humanos en la Unión Europea, la primera en cuanto dispone en su apartado 53 que: "*el respeto de la vida privada y familiar, de la reputación, del domicilio y de las comunicaciones privadas, tanto de las personas físicas como jurídicas, así como la protección de datos de carácter personal son derechos fundamentales básicos respecto de los cuales los Estados miembros deben ejercer una especial protección, habida cuenta de la incidencia negativa que sobre los mismos tienen las nuevas tecnologías y que sólo la armonización de las legislaciones nacionales en la materia, confiriendo una alta protección, es susceptible de responder a este desafío*", y la segunda, al subrayar en su apartado 23 que: "*el derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia, así como a la protección de los datos de carácter personal, representan derechos fundamentales que los Estados tienen la obligación de proteger y que, por consiguiente, toda medida de vigilancia óptica, acústica o informática deberá adoptarse dentro de su más estricto respeto y acompañada en todos los casos de garantías judiciales*".

En relación con la protección de los datos personales en el ámbito concreto del proceso penal cuando se trata de la detección, investigación o enjuiciamiento de determinados hechos delictivos se ha trabajado bastante a nivel europeo. Destaca a este respecto la Directiva 2016/680, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. En nuestro Ordenamiento jurídico, aquella Decisión ha sido implementada por la Ley 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Como se indica

346 STC 173/2011, citada anteriormente.

en el Preámbulo de esta Ley, la misma asume la finalidad de lograr un elevado nivel de protección de los derechos de la ciudadanía, en general, y de sus datos personales, en particular, que resulte homologable al del resto de los Estados miembros de la Unión Europea, incorporando y concretando las reglas que establece la Directiva.

Todo ello, en relación a la protección de datos personales, tanto en el ámbito físico como virtual o electrónico. Por lo que respecta a las concretas medidas de investigación o prueba en el proceso penal, recientemente se han dictado nuevos instrumentos que posibilitan la investigación de los hechos delictivos transfronterizos basándose en el principio de reconocimiento mutuo entre los Estados miembros. Entre estos nuevos instrumentos hay que hacer mención a la Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014, relativa a la orden de investigación europea en materia penal, implementada en nuestro ordenamiento por la Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre de Reconocimiento mutuo de resoluciones penales en la Unión Europea, para incorporar aquella Directiva además de modificar otras cuestiones relevantes que se habían puesto de manifiesto durante la práctica de dicha Ley.

Dado el existente acervo legislativo en materia de cooperación judicial penal, integrado hasta ahora tanto por normas convencionales como por decisiones marco muchos más flexibles, este nuevo mecanismo jurídico viene a reemplazar, en materia de obtención de pruebas, y unificar toda la materia en un único instrumento normativo de mayor vinculación para los países miembros para así facilitar y agilizar la obtención y transmisión de pruebas entre los Estados miembros de la Unión Europea. Su objetivo es facilitar y agilizar la obtención y transmisión de las pruebas entre los Estados miembros de la Unión Europea[347].

La Orden Europea de Investigación vino a sustituir determinadas disposiciones relativas a la prueba tanto del Convenio Europeo de Asistencia judicial en materia penal del Consejo de Europa de 20 de abril de 1959, así como sus dos protocolos adicionales y los acuerdos bilaterales celebrados de acuerdo a su artículo 26, como el Convenio relativo a la aplicación del Acuerdo Schengen, y también el Convenio relativo a la Asistencia judicial en materia penal entre los Estados miembros de la Unión Europea y su Protocolo del 2001.

347 Véase mi trabajo "La trasposición de la orden europea de investigación en España por la Ley 3/2018, de 11 de junio", en *Justicia*, Revista de Derecho Procesal, ISNN: 0211-7754, nº 2, 2018, págs. 269 a 352.

Otro de los instrumentos jurídicos de reconocimiento muto es la 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, de 7 de abril de 2018[348]. Este instrumento jurídico nace como un instrumento adicional completando la orden de investigación europea en materia de prueba electrónica. No es un mecanismo que venga a sustituir a la orden europea de investigación, sino que nace con la vocación de mejorar la obtención de pruebas cuando su naturaleza es electrónica. Es un nuevo instrumento jurídico en consonancia con la realidad tecnológica que vivimos. Además, supone un añadido a las posibilidades que ya tienen los Estados miembros en materia de investigación y obtención de prueba puesto que la Propuesta de Reglamento ofrece instrumentos adicionales a las autoridades encargadas de la investigación para que obtengan pruebas electrónicas sin limitar las competencias ya previstas por la legislación nacional. En nuestro ordenamiento la regulación actual está contenida en la Ley 25/2007, en lo que se refiere a la conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Aunque es una ley muy controvertida, no obstante, es de aplicación en ese ámbito.

Todo ello refleja el avance constante en materia de nuevas tecnologías y la necesidad del Derecho de regular estos avances con la finalidad de conseguir que los delitos no queden impunes, precisamente por no tener mecanismos jurídicos con los que luchar contra esta delincuencia, cada vez más globalizada.

k.1 Antecedentes legislativos

Hasta hace no mucho la regulación de la prueba electrónica no se encuadraba en ninguna categoría específica, sino que por el contrario existían disposiciones generales aplicables a la prueba tradicional. Los Estados de la Unión Europea no tenían ninguna regulación nacional específica en materia de prueba electrónica.

En este sentido, a través del Programa Marco AGIS, se llevó a cabo un estudio que fue el primero de su género en Europa dirigido por la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea. Este proyecto concluyó con una Guía de Mejora, que fue un referente para Europa.

Los países participantes en dicho proyecto fueron 16 y se analizaron más de setenta y ocho normas. El proyecto se dividió en dos fases.

348 En https://eur-lex.europa.eu/legal-content/ES/TXT/.

1ª Fase:

El objetivo de la primera fase fue la de encontrar un concepto de prueba electrónica, sin embargo, no se encontró una definición específica de la misma, aunque sí términos aplicables de forma analógica de la prueba electrónica. Tampoco existía en toda Europa ningún procedimiento específico para admitir la prueba electrónica, se aplicaba el procedimiento general, resaltaban Reino Unido y Bélgica, países que tenían las normas más similares a la que sería un procedimiento específico para la prueba electrónica.

2º Fase:

El objetivo de la segunda fase del Proyecto fue la de entrevistar a los agentes sociales que tenían relación con la obtención, conservación, proposición y admisión de la prueba electrónica en los procedimientos judiciales.

La percepción que se obtuvo fue la de que no existía una regulación en Europa heterogénea y además existía multitud de contradicciones. El propósito, por tanto, era el de conseguir la armonización de la materia a nivel europeo, pero a través de normas generales que permitiesen a cada país su implementación de acuerdo con su tradición jurídica. También se propugnaba la creación de unas normas de mínimos a nivel internacional y no sólo a nivel europeo[349].

La preocupación por establecer un enfoque común a nivel europeo de la justicia penal en el ciberespacio era de orden prioritario, y siempre estuvo presente en los objetivos del Parlamento Europeo[350], la finalidad a conseguir con el enfoque común era la de reforzar el respeto del imperio de la ley en el ciberespacio, procurar la obtención de pruebas electrónicas en los procedimientos penales y contribuir a resolver las causas en plazos mucho más breves que en la actualidad.

El Parlamento Europeo en dicho Informe reconocía que al no existir una normativa unitaria conlleva muchas dificultades para los prestadores de servicios cuando tienen que cumplir con los requerimientos de las Fuerzas y Cuerpos de Seguridad del Estado, y por ello, solicitaba a la Comisión que llevase a cabo una propuesta a nivel europeo en relación con las pruebas elec-

---

349 INSA, F., LÁZARO, C. y GARCÍA, N., "Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo", en *Revista venezolana de Información, Tecnología y Conocimiento*, 5 (2), 2008, págs. 139-152.

350 Informe de 25 de julio de 2017, publicado en https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_ES.html.

trónicas incluyendo normas armonizadas para determinar si los prestadores de servicios pueden considerarse nacionales o extranjeros e imponiendo a los prestadores de servicios la obligación de responder a las solicitudes de otros Estados miembros formuladas con las debidas garantías procesales y de conformidad con la orden europea de investigación (OEI), todo ello atendiendo al principio de proporcionalidad para no vulnerar el ejercicio de la libertad de establecimiento y de prestación de servicios, y asegurar las garantías adecuadas, con la finalidad de velar por la seguridad jurídica, así como a mejorar la capacidad de respuesta a las peticiones de las fuerzas de seguridad de los prestadores de servicios y los intermediarios[351];

Además, el Parlamento ha puesto verdadero énfasis en que este marco unitario de regulación de las pruebas electrónicas debe garantizar los derechos y libertades de todas las personas que puedan verse afectadas, debiendo incluirse en dicho marco la necesidad de dirigir las primeras solicitudes de pruebas electrónicas a quienes son propietarios o controladores de los datos, así como también a cualquier otra persona afectada por esos datos[352].

k.2 Situación actual

Dada la complejidad técnica de la prueba electrónica, existe una verdadera desventaja por parte de las autoridades competentes para descubrir los delitos cometidos en red, por ello, en la actualidad muchos de los delitos cometidos en ese ámbito quedan impunes.

El Parlamento europeo es consciente de esta realidad y desde hace ya algún tiempo y dado el aumento considerable de ciberdelitos en estos últimos años, viene manifestando su preocupación por tal realidad y lamenta que, en la actualidad, no existan normas europeas en materia de formación y certificación. En este sentido, confiesa que la tendencia en materia de ciberdelincuencia requiere un mayor nivel de pericia técnica por parte de los profesionales y por ello ve con buenos ojos las iniciativas que están teniendo lugar actualmen-

351 Resolución del Parlamento Europeo, de 3 de octubre de 2017, sobre la lucha contra la ciberdelincuencia (2017/2068 (INI), en https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_FR.html.

352 Por ejemplo como indica el Parlamento, su derecho al respeto del secreto profesional y a solicitar reparación en caso de acceso desproporcionado o ilegal a los datos, véase la Resolución del Parlamento Europeo, de 3 de octubre de 2017, sobre la lucha contra la ciberdelincuencia (2017/2068 (INI), en https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_FR.html.

te, como el Grupo Europeo de Formación y Educación en Ciberdelincuencia (ECTEG), el proyecto de formación de los formadores y las actividades de formación en el marco del ciclo de actuación de la Unión ya estén allanando el camino para colmar la laguna de conocimientos a nivel europeo[353].

Es de destacar el trabajo de la Comisión sobre la creación de una plataforma de cooperación, equipada con un canal de comunicación seguro que permite el intercambio digital de decisiones de investigación europeas, en lo que respecta a las pruebas y respuestas electrónicas entre las autoridades judiciales de la Unión. En este sentido es meritoria la Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO, por el que se establece el programa Europa Digital para el período 2021-2027[354].

Como se indica en la Exposición de Motivos de dicha Propuesta de Reglamento: "*El programa Europa Digital es un elemento central de la respuesta integral de la Comisión al desafío de la transformación digital, que forma parte de la propuesta del marco financiero plurianual (MFP) para 2021-2027. Su objetivo es ofrecer un instrumento de gasto adaptado a los requisitos operativos de la creación de capacidades en las áreas identificadas por el Consejo Europeo, y explotar las sinergias entre ellos.*

353 En el Informe de 25 de julio de 2017, véase en https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_ES.html, se pide entre otras cuestiones que:

- CEPOL y a la Red Europea de Formación Judicial extiendan su oferta de cursos de formación dedicados a temas relativos a la ciberdelincuencia a las fuerzas de seguridad y las autoridades judiciales competentes de toda la Unión;

- Subraya que el número de ciberdelitos remitidos a Eurojust ha aumentado un 30 %; pide que se prevea financiación suficiente y, si procede, se amplíe la plantilla de Eurojust para que la agencia pueda hacer frente a su creciente carga de trabajo en relación con la ciberdelincuencia, así como desarrollar y consolidar su apoyo en asuntos transfronterizos a los fiscales nacionales especializados en ciberdelincuencia, en particular a través de la Red Judicial Europea sobre Ciberdelincuencia recientemente establecida;

- Que se revise el mandato de la ENISA y se refuercen las agencias nacionales de ciberseguridad; pide que se refuercen los cometidos, el personal y los recursos de la ENISA; destaca que el nuevo mandato debería incluir asimismo vínculos más estrechos con Europol y las partes interesadas del sector, de manera que la agencia pueda brindar un mejor apoyo a las autoridades competentes en la lucha contra la ciberdelincuencia;

- Que la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) elabore un manual práctico y detallado que proporcione directrices a los Estados miembros en relación con los controles de supervisión y escrutinio.

354 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018PC0434&from=FR. La presente Propuesta es de aplicación desde el 1 de enero de 2021.

Por lo tanto, se centrará en reforzar las capacidades de Europa en informática de alto rendimiento, inteligencia artificial, ciberseguridad y competencias digitales avanzadas y en garantizar su amplio uso en la economía y la sociedad. Fomentadas simultáneamente, ayudarán a crear una economía de datos próspera, promoverán la inclusión y garantizarán la creación de valor. Ignorar o debilitar uno de los pilares socavará toda la construcción ya que están estrechamente interrelacionados y son interdependientes: por ejemplo, la inteligencia artificial tiene necesidad de la ciberseguridad para ser fiable, la ciberseguridad necesita a la informática de alto rendimiento para procesar la enorme cantidad de datos que deben asegurarse, los servicios digitales necesitan estas tres capacidades para adaptarse a las normas futuras; por último, todos los elementos anteriores requieren competencias avanzadas adecuadas. Más importante aún, este programa se concentrará en las áreas en las que ningún Estado miembro por sí solo puede garantizar el nivel requerido para el éxito digital. También pondrá su atención en aquellas áreas donde el gasto público tenga un mayor impacto, especialmente en la mejora de la eficiencia y la calidad de los servicios en las áreas de interés público como la salud, la justicia, la protección de los consumidores y las administraciones públicas, y en la ayuda a las pymes para adaptarse al cambio digital"[355].

Además, la Estrategia de la Unión de Seguridad para el período comprendido entre 2020-2025 constituye un marco estratégico en el que se integran todas las iniciativas políticas y normativas de la Unión Europea en la lucha contra la ciberdelincuencia, centrándose en el desarrollo de habilidades y capacidades para conseguir un entorno seguro que responda a las necesidades del futuro, establece un alcance global de la sociedad en su conjunto para asegurar una respuesta efectiva y de manera coordinada ante la volatilidad del entorno virtual y sus crecientes amenazas. Esta Estrategia define las prioridades y acciones estratégicas para abordar los riesgos físicos y digitales de forma integrada en toda la Unión Europea, concentrándose en dónde la UE puede aportar más valor[356].

355 Ibídem.

356 Véase COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy, Bruselas 24.7.2020, en https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN.

l. Ámbito internacional

En lo que respecta al ámbito internacional, en el momento presente se está trabajando en la actualización del Segundo Protocolo Adicional al Convenio de Budapest sobre la Ciberdelincuencia.

Como ya vimos anteriormente, el Convenio de Budapest sobre Ciberdelincuencia surgió precisamente con la finalidad de ofrecer de forma prioritaria una política penal común para proteger a los ciudadanos frente a la ciberdelincuencia, concretamente el propósito era configurar una legislación adecuada y reforzar la cooperación internacional, dada la transformación llevada a cabo por la digitalización, la convergencia y la globalización de las redes informáticas[357].

Con este mismo propósito el Consejo de Europa inició en septiembre de 2017 la elaboración de este Segundo Protocolo Adicional precisamente para mejorar el acceso transfronterizo a las pruebas electrónicas en las investigaciones penales. En este sentido, este documento incorpora disposiciones dirigidas a fijar un régimen de asistencia judicial más competente, a potenciar la cooperación directa con los proveedores de servicios de terceros países que son partes en el Convenio y a posibilitar el acceso remoto por las autoridades a servidores u ordenadores; además, prevé un marco general y garantías multilaterales para ampliar las búsquedas a través de las fronteras, y garantías y requisitos preceptivos en materia de protección de datos[358]. En junio de 2019, los Estados encargaron a la Comisión europea de entablar negociaciones a nivel internacional para firmar el Segundo Protocolo Adicional, fijando el año 2020 como fecha límite[359].

Actualmente se está trabajando en la preparación del Segundo Protocolo Adicional que tiene por objeto afianzar los lazos en materia de cooperación internacional y facilitar la obtención de evidencia electrónica para poder brindar una respuesta eficaz en la investigación criminal para trabajar contra el

357 Véase el Preámbulo del Convenio sobre la Ciberdelincuencia ya citado repetidamente.

358 ALONSO LECUIT, Javier, "El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea", en *Estudios Internacionales y Estratégicos*", ARI 4/2021 – 14/1/2021, en http://www.realinstitutoelcano.org/

359 Véase la Declaración 2/2021 sobre el nuevo proyecto de disposiciones del Segundo Protocolo adicional al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest) Adoptada el 2 de febrero de 2021, en https://edpb.europa.eu/system/files/2021-06/statement022021onbudapestconventionnewprovisions_es.pdf.

ciberdelito[360]. El ámbito de aplicación del presente proyecto de Segundo Protocolo de acuerdo al artículo 2 es el de las investigaciones o procedimientos penales específicos relativos a los delitos relacionados con sistemas y datos informáticos, y a la obtención de pruebas en forma electrónica de un delito penal.

El borrador del "Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y divulgación de pruebas electrónicas" prevé entre otras finalidades:

- – Cooperación directa con proveedores de servicios (artículo 6) y entidades que presten servicios de dominio en el territorio de otra Parte para obtener información que esté en posesión o bajo el control de la entidad, con el fin de identificar o ponerse en contacto con el titular de un nombre de dominio, así como obtener la divulgación de información especificada y almacenada del abonado que esté en posesión o bajo el control de dicho proveedor de servicios, cuando la información sobre el abonado sea necesaria para las investigaciones o procedimientos penales específicos de la Parte emisora.

– Formas aceleradas de cooperación entre las Partes para la divulgación de información de suscriptores y datos de tráfico (artículo 8);

– Cooperación y divulgación aceleradas en situaciones de emergencia (artículos 9 y 10);

– Herramientas adicionales para la asistencia mutua (artículos 11 y 12);

– Protección de datos y otras salvaguardias del estado de derecho (artículos 13 y 14).

360 Véase en https://rm.coe.int/0900001680a27dbe.

BIBLIOGRAFÍA

1. AGUILAR CÁRCELES, Marta María, "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido", en *Revista Criminalidad*, 2015, 57 (1): 121-135. En http://www.scielo.org.co/scielo.php?pid=S1794-31082015000100009&script=sci_arttext.
2. AIGE MUT, María Belén, "Las nuevas diligencias de investigación tecnológica", en *ibdigital.uib.cat*.
3. ALCOCEBA GIL, Juan Manuel y LÓPEZ ORTEGA, Juan José, "De la intimidad territorial a la informativa: la defensa de la intimidad a través de sus manifestaciones constitucionales", en *Foro. Revista de Ciencias Jurídicas y Sociales*, Nueva Época, Universidad Complutense de Madrid, vol. 22, núm. 1 (2019), págs. 87-99, en https://dx.doi.org/10.5209/foro.66635.
4. ALONSO, Adolfo, «La investigación policial de los delitos relacionados con nuevas tecnologías», *Estudios Jurídicos. Ministerio Fiscal,* número 2, 2003.
5. ALONSO LECUIT, Javier, "El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea", en *Estudios Internacionales y Estratégicos*", ARI 4/2021 – 14/1/2021, en http://www.realinstitutoelcano.org/
6. ALONSO RUIDO, Patricia, *Evaluación del fenómeno del sexting y de los riesgos emergentes de la red en adolescentes de la provincia de Ourense*, dirigido por Rodríguez Castro, Yolanda y Lameiras Fernández, María, 2017, Universidad de Vigo.
7. ANGUIANO JIMÉNEZ, José María, "La prueba electrónica en la banca digital. El soporte duradero", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016.
8. AÑÓN CALVETE, JUAN, *Diligencias de Investigación Tecnológica y Derechos Fundamentales*, 2015, Tirant on line, DOCUMENTO TOL5.429.306
9. ARRABAL PLATERO, Paloma, *Prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, 2019, en Tirant on line, DOCUMENTO TOL7.712.007.
10. BENTHAM, J., *Antología,* (Traducciones de HERNÁNDES ORTEGA, G. y VANCELLS, M.), Barcelona, 1991, pág. 35.
11. *La prueba en el Proceso. Perspectivas nacionales*, (Coordinadores, BUJOSA VADELL, Lorenzo-Mateo y BUENO DE MATA, Federico), 2018, en Tirant on line, DOCUMENTO TOL6.977.376.
12. BUENO DE MATA, Federico, *Prueba electrónica y proceso 2.0, Especial referencia al proceso civil*, Tirant lo Blanch, 2014, en Tirant on line, Documento TOL4.147.241.
13. CARNELUTTI, *La prueba civil*, Ediciones Depalma, Buenos Aires, 1982.

14. CAROU GARCÍA, Sara, "El agente encubierto como instrumento de lucha contra la pornografía infantil en Internet. El guardián al otro lado del espejo", en *Cuadernos de la Guardia Civil*, nº 56, 2018.
15. CASTILLEJO MANZANARES, Raquel, "Alguna de las cuestiones que plantean las diligencias de investigación tecnológica", en *Revista Aranzadi de Derecho y Proceso Penal*, 45, enero-marzo 2017.
16. DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba electrónica*, Valencia, Tirant Lo Blanch, 2009, en Tirant on line, Documento TOL1.436.940.
17. DELGADO MARTÍN, Joaquín, "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma operada por LO 13/2015", en *Diario LA LEY*, nº 8693, de 2 de febrero de 2016.
18. DELGADO MARTÍN, Joaquín, *Investigación tecnológica y prueba digital en todas las jurisdicciones,* Wolter Kluwer, La Ley, 2018, 555 págs.
19. DELGADO MARTÍN, Joaquín, "La protección de datos personales en el proceso penal (II), en ELDERECHO.COM, Tribunal 30-04-2019.
20. DELGADO MORÁN, Juan José, *Sociedad de Control y Panóptico Electrónico. La Victima de la Videovigilancia*, Murcia, septiembre, 2018, en http://repositorio.ucam.edu/bitstream/handle/10952/3839/Tesis.pdf?isAllowed=y&sequence=1.
21. DEL ROSAL BLASCO*, Criminalidad organizada y nuevas tecnologías: algunas consideraciones fenomenológicas y político-criminales*, 2001, en Tirant on line, Documento TOL163.240.
22. ENCINAR DEL POZO, M. A., "La invalidez de la Directiva sobre Conservación y Cesión de los datos relativos a las Comunicaciones", en Revista SEPIN/SP/DOCT/18682, 7 de noviembre de 2014.
23. FERNÁNDEZ LÓPEZ, Juan Manuel, *El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario*, en *file:///Users/raqlj/Downloads/Dialnet-ElDerechoFundamentalALaProteccionDeLosDatosPersona-500300.pdf*
24. FERNÁNDEZ NIETO, Josefa, "Reforma del Código Penal hacia una nueva dimensión de la protección en los delitos de sexting y grooming", en *Diario la Ley*, N. 8714, Sección Doctrina, 3 de marzo de 2016, Ref. D-93, Editorial La Ley, 18 págs.
25. FERNÁNDEZ DOYAGUE, Amalia, "La denominada violencia cibernética. Internet y las redes sociales", en Consejo General de la Abogacía Española, noviembre 2014, en https://www.abogacia.es/2014/11/26/la-denominada-violencia-cibernetica-internet-y-las-redes-sociales/
26. FERNÁNDEZ MARTÍNEZ, Juan Carlos, "Especialidades de la prueba cuando, esta, es tecnológica", en *Nuevas tecnologías 2020*, Tirant lo Blanch, 2020, 504 págs.

27. FLORENCIO MOLINA, Miguel, *La prueba digital,* Manuales de Derecho Aplicado, junio de 2017, pág. 20, en https://www.miguelflorencio.com/books/Derecho/pruebadigital.pdf.
28. FLORES PRADA, Ignacio, *Criminalidad informática. Aspectos sustantivos y procesales*, Tirant lo Blanch, 2012.
29. FLORES PRADA, Ignacio, "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia", en *Revista Electrónica de Ciencia Penal y Criminología*, núm. 17, 2015. Disponible en internet: http://criminet.ugr.es/recpc/17/recpc17-21.pdf.
30. GALLARDO, Miguel, en *Extorsionabilidad, extorsionistas y extorsionología pericial forense Hacia la victimología de los chantajeados por "extorsionoscopia"*, en https://www.miguelgallardo.es/extorsionologo.pdf.
31. GALLEGO SOLER, José Ignacio, *Comentarios al Código Penal. Reforma LO 5/2010*, Tirant lo Blanch, Valencia, 2010.
32. GARCÍA GONZÁLEZ, J., *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*, Tirant lo Blanch, Valencia, 2010.
33. GARCÍA TORRES, María Luisa, "La tramitación electrónica de los procedimientos judiciales, según la ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y comunicación en la administración de justicia. Especial referencia al proceso civil", en *Revista Internacional de Estudios de Derecho Procesal y Arbitraje*, www.riedpa.com, núm. 3, 2011, en http://www.riedpa.com/COMU/documentos/RIEDPA31102.pdf, 31 págs.
34. GASCÓN INCHAUSTI, Fernando, *Orden Europea de Investigación y Prueba Transfronteriza en la Unión Europea*, (coord. GONZÁLEZ CANO, María Isabel), Tirant lo Blanch, 2019, en Tirant on line, DOCUMENTO TOL7.558.495.
35. GENVETA: DEV, "¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales" accesible en https://goo.gl/fvqAmM.
36. GONZÁLEZ-CUELLAR SERRANO, Nicolás, *Proporcionalidad y derechos fundamentales en el proceso penal*, Ed. Colex, Madrid, 1990.
37. GONZÁLEZ COLLANTES, Tália, "Los delitos contra la intimidad tras la reforma de 2015: luces y sombras", en *Revista de Derecho Penal y Criminología*, 3.ª Época, n.º 13 (enero de 2015), págs. 51-84.
38. GONZÁLEZ NAVARRO, Alicia, *El proceso penal. Cuestiones fundamentales,* 2017, (coord. FUENTES SORIANO, Olga), en Tirant on line, DOCUMENTO TOL6.080.359.
39. GUZMÁN FLUJA, Vicente, Anticipación y preconstitución de la prueba en el proceso penal, Tirant on line, 2006, DOCUMENTO TOL865.119.
40. HERNÁNDEZ DOMÍNGUEZ, Juan José, y MARTÍNEZ MARTÍN, José Israel, *Secreto de las comunicaciones. Alcance de protección constitucional de si interceptación y casuística*, DILEX, 2015.

41. Informe 327/2003 de la AEPD, en https://www.aepd.es/informes/historicos/2003-0327.pdf.
42. Informe sobre la aplicación de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, de 27.11.2017, (2015/2129(INI)), publicado en http://www.europarl.europa.eu/doceo/document/A-8-2017-0368_ES.html.
43. INSA, F., LÁZARO, C. y GARCÍA, N., "Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo", en *Revista venezolana de Información, Tecnología y Conocimiento*, 5 (2), 2008, págs. 139-152.
44. LAUDAN, L., «La elemental aritmética epistémica del derecho II: los inapropiados recursos de la teoría moral para abordar el derecho penal», en VÁZQUEZ, C., *Estándares de prueba y prueba científica*, Marcial Pons, Madrid, 2013, p. 121.
45. LEDESMA NARVÁEZ, Marianella, "La prueba documental electrónica", en *Revista Foro Jurídico*, número 15, 2016, págs. 17 a 25.
46. LÓPEZ, Antonio, "La investigación policial en Internet: estructuras de cooperación internacional", en *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, Número 5 (2007) I ISSN 1699-8154, pág. 66. Véase en http://idp.uoc.edu
47. LÓPEZ JIMÉNEZ, Raquel, "Algunas cuestiones relativas a la protección de las personas físicas en el tratamiento de datos personales en materia penal", Revista de Derecho y Proceso Penal, Thomson Reuters, 2021, julio-septiembre, número 63.
48. LÓPEZ JIMÉNEZ, Raquel, "El nuevo enfoque jurídico sobre el sistema de cesión de datos tras la Sentencia del Tribunal de Justicia de 2 de octubre de 2018", en *Uso y Cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios* (Dir. COLOMER HERNÁNDEZ), Aranzadi, 2019.
49. LÓPEZ JIMÉNEZ, Raquel, "El nuevo marco jurídico transfronterizo de las pruebas electrónicas. Las órdenes de entrega y conservación de las pruebas electrónicas", en *Revista General de Derecho* Europeo, noviembre, número 49, 2019, en https://www-iustel-com.biblioteca5.uc3m.es//v2/revistas/detalle_revista.asp?id_noticia=421898&texto=.
50. LÓPEZ JIMÉNEZ, Raquel, "La trasposición de la orden europea de investigación en España por la Ley 3/2018, de 11 de junio", en *Justicia*, Revista de Derecho Procesal, ISNN: 0211-7754, nº 2, 2018, págs. 269 a 352.
51. LÓPEZ ORTEGA, Juan José y ALCOCEBA GIL, Juan Manuel, "Prevenir y evitar: consideraciones en torno a un modelo de intervención penal anticipativa",

en *Derechos del condenado y necesidad de pena*, (Obra Colectiva: Carmen Juanatey Dorado (dir.), y Natalia Sánchez-Moraleda Vilches (dir.)), Aranzadi Thomson Reuters, 2018, pág. 90.

52. MAGRO SERVET, Vicente, "El delito de sexting (o difusión de imágenes tomadas con consentimiento de la víctima) en la violencia de género", *En la Ley Penal*, N 137, marzo-abril 2019.
53. MARTÍN RÍOS, Pilar, "El "primer acceso policial" a dispositivos de almacenamiento digital o de cuando las garantías se supeditan a la búsqueda de la eficiencia", en *Justicia: ¿Garantías versus eficiencia?,* Tirant lo Blanch, 2019.
54. MARTÍNEZ DE PISÓN, José, "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional", en AFD, 2016 (XXXII), pp. 409-430, ISSN: 0518-0872.
55. MARTÍNEZ LOPEZ-SAEZ, Mónica, *Una revisión del derecho fundamental a la protección de datos de carácter personal*, 2018, Tirant on line, DOCUMENTO TOL6.820.902.
56. MIRA ROS, Corazón de María, "La prueba electrónica: algunas concesiones a la seguridad jurídico preventiva", véase en https://www.uv.es.
57. MONTESDEOCA RODRÍGUEZ, Daniel, "El delito de descubrimiento y revelación de secretos en el uso de las tecnologías de la información y comunicación: especial referencia a la mensajería instantánea", en *Diario LA LEY*, nº 9770, de 14 de enero de 2021, Nº 9770, 14 de ene. de 2021, Editorial Wolters Kluwer.
58. MONTOYA ROJAS, Alejandra, "La informática forense como herramienta para la aplicación de la prueba electrónica", en *Revista CES Derecho*, vol. 1, nº 1, 2010.
59. MORENO CATENA, Víctor, *Derecho procesal penal* (con CORTÉS DOMÍNGUEZ), Tirant lo Blanch, 2021, 1ª ed.,
60. NAVARRO CASTRO, Miguel, "El cloud computing como forma de prestación de servicios de tratamiento de datos", en *Protección de datos personales,* (coord. GONZÁLEZ PACANOWSKA, Isabel), Tirant lo Blanch, 2020
61. OLIVA LEÓN, Ricardo, "La prueba electrónica envenenada", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016, pág. 58.
62. ORTIZ PRADILLO, Juan Carlos, *La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, en Fundación alternativas, 2013, 60 págs., véase en https://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf
63. ORTUÑO NAVALÓN, María del Carmen, *La prueba electrónica ante los Tribunales*, Tirant lo Blanch, 2014, en Tirant on line, Documento TOL4.125.955 y Documento TOL4.125957.

64. PALAZZI, PABLO A., *Los Delitos Informáticos en el Código Penal Análisis de la ley 26.388*, Buenos Aires, 2016, en https://www.academia.edu/37287925/Los_Delitos_Informaticos_en_El_Pablo_a_Palazzi_2_pdf?auto=download.
65. PERALES CAÑETE, Rafael, "Exiftool: Los metadatos sirven de algo", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016.
66. PÉREZ CONCILLO, Eloísa, "La difusión de sexting ajeno como violencia de género", en *Revista Aranzadi de Derecho y Proceso Penal*, 2018, núm. 51.
67. PÉREZ CONCILLO, Eloísa, *Intimidad y difusión de sexting no consentido,* Tirant lo Blanch, 2018.
68. PÉREZ ESTRADA, Miren Josune, "La investigación del delito a través de las nuevas tecnologías. Nuevos medios de investigación en el proceso penal", (dir. DE LA CUESTA ARZAMENDI), en *Derecho Penal informático*, Thomson Reuters, 2010, pág. 314.
69. PÉREZ ESTRADA, Miren Josue, "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información", en *Revista Brasileña de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1297-1330, set.-dez. 2019, págs. 1297 y ss.
70. PÉREZ ESTRADA, Miren Josune, "La vulneración de datos personales en la aportación de la prueba en el proceso penal", en *Justicia: ¿Garantías versus eficiencia?,* Tirant lo Blanch, 2019.
71. PÉREZ GIL, Julio, "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal", en *Justicia: ¿Garantías versus eficiencia?*, (Dir. JIMÉNEZ CONDE y BELLIDO PENADÉS), Tirant lo Blanch, 2019.
72. PÉREZ PALACI, José Enrique, "La prueba electrónica: Consideraciones", 2014, pág. 3, en www.prolex.org
73. PLAZA PENADÉS, Javier, "La "piratería" en la Red. Una asignatura pendiente para el Gobierno de España", en *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 40, Enero - Abril 2016.
74. POLO ROCA, Andoni, "La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión", en *Revista de Internet, Derecho y Política*, núm. 33 (octubre), 2021.
75. QUEVEDO GONZÁLEZ, Josefina, *Investigación y prueba del ciberdelito*, Tesis Doctoral dirigida por ORTEGO PÉREZ, Fr., y tutorizada por VALLESPÏN PËREZ, D., defendida en la Universidad de Barcelona, Facultad de Derecho, 2017, disponible en disposit.ub.edu.
76. RODRÍGUEZ RUBIO, Carmen, "Nuevas diligencias de investigación y de prueba: el registro de dispositivos de almacenamiento masivo de información", en https://dx.doi.org/10.5209/foro.74004,Foro, Nueva época, vol. 23, núm. 1 (2020): 267-304, ISSN:1698-5583.

77. ROJAS ROSCO, Raúl, "La prueba digital en el ámbito laboral ¿son válidos los pantallazos?", en *La prueba electrónica. Validez y eficacia procesal*, Desafíos legales, 2016.
78. ROUANET MOSCARDÓ, JAIME, "Valor probatorio procesal del documento electrónico", en *Informática y Derecho*, dialnet.unirioja.es, págs. 163 a 175.
79. RUIZ SIERRA, Joana, "El delito de "stalking"", en *Revista Foro FICP (Tribuna y Boletín de la FICP)*, 2017-2 (septiembre 2017), en https://ficp.es/wp-content/uploads/2013/06/Foro-FICP-2017-2.pdf.
80. SALVADORI, Iván, "La controvertida relevancia penal del sexting en el derecho italiano y comparado", en *Revista Electrónica de Ciencia Penal y Criminología,* págs. 19-29 (2017), también en http://criminet.ugr.es/recpc – ISSN 1695-0194.
81. SÁNCHEZ SISCART, José Manuel, "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EEUU", en *Revista del Poder Judicial*, número 91, 2011, págs. 31- 42.
82. SANCHEZ RUBIO, Ana, *La prueba científica en la justicia penal,* Tirant lo Blanch, 2019, en Tirant on line, DOCUMENTO TOL7.571.683.
83. SANZ-GADEA GÓMEZ, Juan Bautista, *Los informes periciales informáticos en el ámbito de las nuevas tecnologías y prueba ilícita (RJC 39/2015*), 2015, Tirant on line, DOCUMENTO TOL5.638.931.
84. SUBIJANA ZUNZUNEGUI, Ignacio José, "Policial judicial y derecho a la intimidad en el seno de la investigación criminal", en *EGUZKILORE*, Número extraordinario 10, San Sebastián, Octubre 1997, págs. 121- 160.
85. TARUFFO, M, en "Conocimiento científico y estándares de prueba judicial", en Revista *Jueces para la Democracia*, nº 52, marzo 2005.
86. VALLS PRIETO, Javier, "Nuevas formas de combatir el crimen en internet y sus riesgos", en *Revista Electrónica de Ciencia Penal y Criminología,* RECPC 18-22 (2016), 36 págs.
87. VELASCO, Eloy y SANCHIS CRESPO, Carolina, *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, Valencia, 2019.
88. VILLACAMPA ESTIARTE, Carolina, *El delito de online child grooming o propuesta sexual telemática a menores*, 2015, Tirant on line, TOL5.204.097.
89. VILLARREAL, Vladimir, Sistemas Operativos, 2017, pág. 76. En Fuente del documento Repositorios Institucional UTP-Ridda2: http://ridda2.utp.ac.pa/handle/123456789/5074.
90. VILLARINO MARZO, Jorge, *La privacidad en el entorno del cloud computing*, Madrid, 2018.
91. VILLEGAS GARCÍA, M. A., "Imágenes íntimas e internet. Cerco legislativo a la venganza privada en la red", en *Aranzadi*, número 876, 2014.

92. ZAFRA ESPINOSA DE LOS MONTEROS, Rocío, "El ciberagente en la lucha de la pornografía infantil", en *Libro Homenaje al profesor MARTÍN OSTOS*, pág. 1974.
93. ZARAGOZA TEJADA José Ignacio, "El agente encubierto "online: la última frontera de la investigación penal", en *Revista Aranzadi Doctrinal*, nº 1, 2017.
94. ZARAGOZA TEJADA, Javier Ignacio (coord..), *Investigación tecnológica y derechos fundamentales*, 1ª ed., noviembre de 2017, en https://idoc.pub/documents/zaragoza-tejada-javier-ignacio-investigación-tecnologicas-y-derechos-fundamentalespdf-d4p7pm7vzd4p