Revista Electrónica de Ciencia Penal y Criminología
ISSN 1695-0194

Problemática jurídica de la prueba digital y sus implicaciones en los principios penales

Gemma Martínez Galindo
Universidad Internacional de La Rioja

MARTÍNEZ GALINDO, GEMMA. Problemática jurídica de la prueba digital y sus implicaciones en los principios penales. *Revista Electrónica de Ciencia Penal y Criminología*. 2022, núm. 24-23, pp. 1-38.
http://criminet.ugr.es/recpc/24/recpc24-23.pdf

RESUMEN: La nueva era electrónica en la que vivimos hace que cada vez tengamos que acudir más a la prueba digital para acreditar el hecho delictivo, ya sea en delitos clásicos o en delitos cibernéticos. Ello implica una urgente necesidad de modificar los planteamientos que hasta ahora teníamos sobre la prueba en derecho penal, pues los métodos de incorporación al proceso de la evidencia digital y su validez o ilicitud por vulneración de derechos fundamentales tienen implicaciones en principios penales básicos, como legalidad, culpabilidad y presunción de inocencia. El esfuerzo en el que han de verse involucrados todos los operadores jurídicos es clave para avanzar en una materia en la que existen muchas peculiaridades que exigen una gran especialización y conocimiento, pues la realidad tecnológica avanza a pasos agigantados y nuestra sociedad, y la Administración de Justicia, no está preparada para lo que en un futuro cercano va a suponer acreditar, desde un punto de vista digital, las conductas delictivas.

PALABRAS CLAVE: Prueba digital, evidencia digital, pericial informática, prueba ilícita, cadena de custodia, valoración de la prueba.

TITLE: **Legal problems of digital evidence and their implications in criminal principles**

ABSTRACT: The new electronic era in which we live means that we increasingly have to resort to digital evidence to prove the criminal act, whether in classic crimes or cybercrimes. This implies an urgent need to modify the approaches that until now we had on evidence in criminal law, since the methods of incorporating digital evidence into the process and its validity or illegality due to the violation of fundamental rights have implications for basic criminal principles, such as legality, guilt and presumption of innocence. The effort in which all legal operators must be involved is key to advancing in a matter in which there are many peculiarities that require great specialization and knowledge, since the technological reality is advancing by leaps and bounds and our society, and the Administration of Justice, is not prepared for what in the near future is going to mean proving, from a digital point of view, criminal conduct.

KEYWORDS: Digital evidence, digital evidence, computer expert, illicit evidence, chain of custody, evaluation of the evidence.

Fecha de recepción: 15 mayo 2022

Fecha de publicación en RECPC: 28 agosto 2022

Contacto: gemma.martinez@unir.net

SUMARIO: I. Concepto y características de la prueba digital en el proceso penal. II. Obtención de la evidencia digital y su conversión en prueba digital. 1. Normativa internacional para la obtención y análisis de evidencias digitales. 2. Medios de incorporación al proceso penal de la evidencia digital como prueba: la importancia de la pericial informática. III. Problemática asociada a la incorporación al proceso de la prueba digital y su incidencia sobre los principios penales. 1. Ilicitud de la prueba electrónica por vulneración de derechos fundamentales. 2. Infracción de la cadena de custodia en las evidencias digitales. IV. Errores en la valoración de las pruebas digitales por parte de los tribunales de justicia. V. Conclusiones. Bibliografía.

I. **Concepto y características de la prueba digital en el proceso penal**

Según la última Memoria de la Fiscalía General del Estado, en el año 2020 se incoaron en el conjunto del Estado un total de 16.914 procedimientos judiciales para la investigación y enjuiciamiento de hechos susceptibles de tipificarse en las categorías de delitos tecnológicos o ciberdelincuencia. Este resultado no solo da cuenta del incremento en un 28,69 % en el volumen anual de procedimientos sino que, además, confirma la tendencia ascendente que venimos constatando en relación con los ciberdelitos.

Es una evidencia que, en la actualidad, las nuevas tecnologías, el ciberespacio y la informática condicionan la vida cotidiana de todos los ciudadanos de los países desarrollados y resulta imposible entenderla sin una actividad continua empleando dispositivos informáticos o electrónicos. Este fenómeno de la digitalización se desarrolla en todos los ámbitos de la vida, ya sea en un contexto social, cultural, político, administrativo, educacional, a través del cual se promueven mayores y más intensas formas de comunicación en las interrelaciones personales y profesionales con cualquier parte del planeta. Cualquiera puede ser un generador de contenidos digitales, pues basta con tener un simple teléfono para difundir música, videos, fotos, escritos, comunicarse con otras personas, acceder a webs en las que se vierten opiniones, redes sociales, blogs, páginas personales, canales de streaming, radios IP, y muchas otras formas de generación digital. Y, como no podía ser de otro modo, también en el ámbito criminal se ha desarrollado el empleo de las nuevas tecnologías con la emisión de contenido digital que puede convertirse en el modo de cometer el delito o en la prueba del mismo, estando implicados en este proceso los principios penales tradicionales como el de legalidad (por la incorporación de nuevos tipos penales ante la obsolescencia de la legislación versus adelantos tecnológicos, cuya prueba de comisión es esencial para incorporar nuevas formas delictivas a nuestro elenco penal –pensemos, por ejemplo, en el desarrollo que están teniendo las criptomonedas y la compra de dinero no efectivo, que es un sector que actualmente carece de regulación[1]-), culpabilidad (porque la búsqueda de la evidencia digital y su conversión en

[1] Actualmente está en fase de Anteproyecto de Ley, aprobado por el Consejo de Ministros en noviembre

prueba incorporada de forma útil al proceso puede incidir en la posibilidad o no de acreditar la autoría de un sujeto o su actuar penalmente relevante) y presunción de inocencia vinculada con el principio de proporcionalidad (pues una prueba ilícita, inválida o ineficaz permite absoluciones a veces injustas).

En la actualidad, es imposible comprender la Administración de Justicia sin elementos tecnológicos y, en concreto, los procedimientos penales sin prueba en la que está inserto algún elemento electrónico, informático o digital. De hecho, la legislación procesal tuvo que introducir en 2015 para adaptarse a los nuevos tiempos, diferentes medidas de investigación tecnológica, que están previstas en los artículos 588 bis y siguientes de la Ley de Enjuiciamiento Criminal superando una obsolescencia normativa que arrojaba importantes lagunas de impunidad[2]. Con la reforma, se afrontaban importantes líneas de actuación que permiten que el Estado de Derecho no se quede atrás ante una delincuencia cada vez más sofisticada tecnológicamente, y a ello se añade la importancia que tiene en la actualidad la prueba digital, ya sea porque se necesita obtener como medio para identificar y detener al autor, acreditar la conducta delictiva y obtener las pruebas para su condena en las conductas criminales que se desarrollan a través de las nuevas tecnologías –resultando fundamental para resolver estos litigios-, es decir, en el ámbito de lo que se denomina la delincuencia cibernética o ciberdelincuencia; ya sea porque, en los delitos clásicos o comunes cometidos en el mundo off line, la evidencia cada vez más es de carácter tecnológico y digital porque la sociedad está totalmente digitalizada, siendo esta prueba esencial para acreditar el delito.

Pensemos, en el primer supuesto, cuando hablamos de ciberdelincuencia, en estafas cometidas por la instalación de un malware en el equipo de la víctima a través de un phising, en unas ciberamenazas, un childgrooming o un ciberbullying mediante de cualquier aplicación de mensajería instantánea (Whatsapp, Telegram, Signal, Messenger, etc.), en una suplantación de identidad en redes, en un hackeo o acceso ilícito a un servidor para cometer un fraude, en un ataque de denegación de servicio a una empresa para cometer unos daños informáticos o cuando se borran los datos de clientes del servidor de una empresa (supuestos que se producen con frecuencia y en los que la valoración de la prueba digital se ha considerado esencial para desvirtuar

de 2021, la reforma de los artículos 248.2, 250, 253 y la incorporación de un artículo 254 bis del Código Penal, para incorporar la Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.

[2] En extenso, sobre estas medidas, vid. CABEZUDO RODRÍGUEZ, 2016, pp. 7 a 60; ARRABAL PLATERO, 2019, pp. 189 a 246; y PINTO /PUYOL, 2017, pp. 189 a 230.

el derecho a la presunción de inocencia[3]), o en casos más graves de ciberterrorismo[4] o distribución de pornografía infantil[5] a través de una Red Tor en la *dark web*.

Y, en el caso de delitos cometidos en el mundo off line, podemos encontrarnos, por ejemplo, con supuestos en los que los indicios de autoría para la comisión presunta de un delito de homicidio se encuentran en el teléfono móvil del sospechoso y en los datos de la unidad electrónica del vehículo[6]; casos en que un empleado graba en dispositivos externos instalados en su ordenador información sensible y confidencial de la empresa para la que trabaja semanas antes de dejar la empresa e irse a otra de la competencia; con supuestos en los que una falsedad documental se acredita con el acceso a los correos electrónicos del servidor de un trabajador en los que se constata la modificación de un archivo contable de la empresa; cuando la prueba de un

[3] La importancia de la prueba digital en estos casos está más que evidenciada en la jurisprudencia anterior, incluso, a la reforma de la Ley de Enjuiciamiento Criminal, como son prueba de ella, por ejemplo, las Sentencias de la Audiencia Provincial de Las Palmas 14/2013, de 11 de febrero *(*ECLI: ES:APGC:2013:179), de la Audiencia Provincial de Albacete 16/2012, de 26 de enero, (ECLI: ES:APAB:2012:96*),* de la Audiencia Provincial de Valladolid 263/2010, de 21 de junio (ECLI: ES:APVA:2010:854), o de la Audiencia Provincial de Madrid , de 29 de julio (ECLI:ES:APM:2010:12394), o las Sentencias del Tribunal Supremo de 533/2007, de 12 de junio y 917/2008, de 19 de diciembre. Y, en la jurisprudencia posterior, por ejemplo, en las Sentencias del Tribunal Supremo 285/2016, de 6 de abril (ECLI:ES:TS:2016:1484), 287/2017, de 19 de abril (ECLI:ES:TS:2017:1487) 478/2019, de 14 de octubre (ECLI:ES:TS:2019:3397), 373/2020, de 3 de julio (ECLI:ES:TS:2020:2169), 395/2021, de 6 de mayo (ECLI:ES:TS:2021:1737) o 91/2022, de 7 de febrero (ECLI:ES:TS:2022:528), entre muchas otras.

[4] En la Sentencia del Tribunal Supremo 400/2016, de 11 de mayo (ECLI:ES:TS:2016:2031), la prueba digital extraída del ordenador portátil del acusado fue esencial en su supuesto de propaganda y proselitismo terrorista realizado mediante videos publicados en YouTube en clave, con exaltación y propaganda de ideas de carácter terrorista.

[5] En la Sentencia del Tribunal Supremo 842/2010, de 7 de octubre (ECLI:ES:TS:2010:5597) se presentan como pruebas esenciales para verificar la posesión de material pedófilo, el disco duro y la pericial sobre el mismo, donde se guardaban archivos con ese contenido, así como la identificación de carpetas en la carpeta Incomig y My shared folder, a través de los programas Emule y Ares, respectivamente, por los que se había descargado y compartido dicho material, que fue identificado a través de su número hash. Asimismo, en la Sentencia del mismo Tribunal 240/2020, de 26 de mayo (ECLI:ES:TS:2020:1319), la pericial acreditó que el acusado almacenaba una gran cantidad de vídeos e imágenes en su ordenador, con acceso a otros usuarios a través de redes "peer to peer" de intercambio de archivos en un supuesto de difusión de pornografía infantil; en la Sentencia de la Audiencia Provincial de Madrid 818/2018, de 3 de diciembre (ECLI:ES:APM:2018:18772), la pericia informática detectó la existencia de rastros de acceso a archivos de contenido pedófilo, que habían sido borrados, e incluso un acceso directo desde el escritorio del ordenador, suficiente para condenarle por el delito de posesión de pornografía infantil; en la Sentencia del mismo órgano 481/2020, de 9 de diciembre (ECLI:ES:APM:2020:14598*),* se analizó tanto el ordenador, como el móvil y los archivos remitidos por whatsapp como prueba esencial para condenar por un delito de elaboración de pornografía infantil al acusado que consiguió, mediante amenazas e intimidación, que la víctima menor de edad le enviase videos de contenido sexual, siendo esencial el contenido de los teléfonos y las fotos en ellos descubiertas, coincidentes con el terminal de la víctima, que se entregó como evidencia cuando efectuó la denuncia; y en la Sentencia 312/2018, de 27 de abril (ECLI:ES:APM:2018:6054), también del mismo órgano judicial, fue esencial esta prueba en un supuesto de contacto por redes sociales con menores de edad convenciéndoles para que posaran desnudos o en actitudes pornográficas ante sus webcam, siendo grabadas en su ordenador, acreditándose la actuación delictiva con el análisis pericial informático de los dispositivos, tras la oportuna entrada y registro, para extraer las conversaciones mantenidas por el acusado con las menores y los archivos intervenidos.

[6] Durante la elaboración de este artículo tenemos un claro ejemplo en la investigación que está llevando a cabo la Guardia Civil de la muerte de Esther López, la joven de Traspinedo (Valladolid), como puede verse en el artículo publicado por ABAD, 2022, online.

delito de administración desleal y apropiación indebida cometida por un directivo se encuentra en su teléfono móvil y su ipad (por los mensajes remitidos a otras personas); aquéllos en que la acreditación del bullying, stalking o trato degradante se encuentra en videos subidos a diferentes plataformas de internet o contenidos en dispositivos informáticos; o cualquier otro delito, como tráfico de drogas, armas o macroperaciones contra organizaciones criminales que habrían cometido delitos contra la Administración Pública y blanqueo de capitales, en los que las evidencias digitales contienen las pruebas de los ilícitos cometidos, que hay que analizar exhaustivamente, tales como documentos o agendas informáticas, correos electrónicos, mensajes enviados o recibidos en el móvil o su geolocalización para determinar en qué lugares ha estado el investigado.

Tanto en unos supuestos como en otros es esencial, en la actualidad, para combatir estos delitos, las medidas de investigación de carácter tecnológico, la obtención de evidencias digitales y su conversión en prueba digital. Para acreditar el hecho delictivo, la extracción de pruebas y evidencias del delito y la determinación de los autores y partícipes -en aplicación de los principios penales que existen, como límites, en Derecho Penal- surgen determinados problemas y desafíos jurídicos para todos los operadores del Derecho (investigadores, abogados, fiscales y jueces) que tratan de solventarse con este tipo de evidencias digitales y forenses. Sin embargo, su obtención no está exenta de polémica porque pueden afectar claramente a los derechos y libertades de los ciudadanos (y, en consecuencia, afectar al principio de proporcionalidad entre la sanción penal y las medidas de investigación para determinar la autoría) y, por tanto, ser ilícitas o bien ser pruebas ineficaces para desvirtuar el derecho a la presunción de inocencia. Como indica ALCÁCER GUIRAO debido a la relación de este derecho fundamental con la "estructural que presenta con otros derechos fundamentales, puede decirse que el derecho a la presunción de inocencia configura el estatuto jurídico del acusado en el proceso penal"[7]. La trascendencia material de este derecho a la presunción de inocencia no puede ser ignorada, ya que la interpretación de las normas penales que implican la necesidad de acudir a la prueba digital, debe hacerse conforme a la Constitución y, por ello, resulta extremadamente relevante, por las consecuencias que implica, determinar en qué medida la obtención y valoración de esa prueba puede concluir con una absolución por aplicación de este derecho y, al contrario, la elaboración de determinadas pruebas digitales y el proceso seguido puede derivar en una presunción de culpabilidad materialmente inválida, procedente, asimismo, de una actuación que vulnera el principio de proporcionalidad entre la determinación de la sanción penal y la penas impuestas a consecuencia de una investigación.

En definitiva, el desarrollo tecnológico impone una serie de retos al operador jurídico no sólo en el ámbito probatorio, sino en relación con los principios penales

[7] ALCÁCER GUIRAO, 2021, p. 2 de la versión imprimible.

que constituyen los límites de aplicación del ius puniendi, porque pueden afectar a cuestiones esenciales como la determinación de la autoría, el dolo, la legalidad de una conducta sancionable penalmente y la proporcionalidad de los medios utilizados para castigar. Y en ellos inciden cuestiones desde cómo recoger las evidencias y custodiarlas debidamente, hasta cómo llevar a cabo su incorporación al proceso penal y sostener su validez probatoria, o en su caso, cómo impugnarlas cuando puedan perjudicar los intereses del cliente.

No existe una definición legal sobre la prueba digital, también conocida como prueba electrónica, prueba tecnológica, prueba informática o ePrueba. BUENO DE LA MATA la define como "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"[8].

Yo la definiría como aquella cuya fuente de obtención radica en los datos producidos en los procesos de comunicación, en la información contenida, almacenada, tratada o transmitida por medios electrónicos o que obra en los soportes técnicos o informáticos, y que dado el carácter efímero y manipulable que tiene -mayor que el de las otras pruebas- debe ser incorporada al proceso mediante un análisis pericial que garantice su integridad y originalidad, que contribuirá a producir un conocimiento probable respecto de las circunstancias de lugar, hecho y autoría.

De lo que sí debe diferenciarse es de la evidencia digital, pues aunque puede parecer a priori que se refieren a lo mismo, en realidad no es así, pues la prueba es un "todo" por el que se incorpora al proceso cualquier información o dato con valor suficiente para poder acreditar un hecho demostrable, y su incorporación se produce a través de medidas de investigación o medios tecnológicos; y la evidencia digital, sin embargo, es, en sí misma, la información, el documento, archivo, fichero, registro o dato almacenado en un soporte electrónico y susceptible de poder ser tratado e identificado digitalmente para su posterior aportación en un proceso judicial. La evidencia es lo primero que se recoge de las diferentes medidas de investigación y necesita ayudarse de la ciencia forense para llegar a descubrir algo; la prueba es el resultado de esta evidencia tratada e incorporada al procedimiento judicial y cuyo valor probatorio dependerá del procedimiento elegido para su aportación en juicio, así como de las garantías ofrecidas para la verificación judicial de su autenticidad e integridad.

[8] BUENO DE LA MATA, 2014, p. 130. También, DELGADO MARTÍN, 2017, p. 1 versión imprimible, la define como "toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio", que "se refiere a cualquier clase de información", que "ha de ser producida, almacenada o transmitida por medios electrónicos", y "que pueda tener efectos para acreditar hechos en el proceso abierto en cualquier orden jurisdiccional".

Se produce, por tanto, en el tránsito del mundo analógico al mundo digital, un nuevo entorno probatorio con unas características definidas, unas peculiaridades o especialidades que no se encuentran ni en la prueba documental (que es como normalmente se incorpora al proceso), ni en la testifical, ni en la pericial y que operan dentro de los límites de la represión penal enlazadas con los medios de tutela penal, que podríamos identificar del siguiente modo:

1º) La prueba digital es intangible, es decir, que no puede apreciarse directamente a través de los sentidos porque ni se puede tocar ni se puede obtener con una fotocopia o una impresión, sino que debe recabarse a través de procesos informáticos y dispositivos electrónicos para poder apreciarla, de forma más o menos compleja. Precisamente en relación con esta característica, uno de los errores que a veces cometen los Tribunales, como más adelante expondré, y que inciden, directamente en este aspecto material del que estamos hablando, del derecho a la presunción de inocencia en relación con el principio de culpabilidad, es que tratan las evidencias digitales y lo obtenido de ellas como meras pruebas de carácter documental o pericial, cuando no lo son. De esta forma se está confundiendo la representación impresa o el proceso conclusivo de análisis con la prueba en sí misma porque la prueba tecnológica son los datos, la información, el contenido digital, no el soporte que los contiene.

Debido a esta intangibilidad, en el proceso penal debe traducirse la prueba digital a un soporte que permita una sencilla comprensión (a través de la vista y el oído) del contenido incriminatorio seleccionado intervenido, para su correcta valoración contradictoria en el acto del juicio oral. Se trata de hacer visible lo invisible[9].

Así, por ejemplo, si se produce un ataque de denegación de servicio con el objetivo de dejar un servidor inoperativo sobrecargándolo, debe investigarse en la pericial la identificación del lugar o puerta trasera por dónde ha accedido al sistema el pirata cibernético y cómo ha instalado el malware que permite la toma de control del equipo de forma remota, cuándo lo hizo, a través de qué estrategias informáticas ha obtenido el acceso del modo privilegiado y de qué forma concreta, es decir, los pasos informáticos que han finalizado con el bloqueo del sistema.

Si se comete una falsificación de un correo electrónico para presentarlo en un procedimiento por despido, la prueba digital consiste en el análisis de los buzones de correo del servidor o servidores donde éstos se encuentren alojados tanto del emisor como del receptor, guardando el contenido en un archivo con formato ".pst", calculando el hash criptográfico del fichero resultante para ser analizado y obteniendo el certificado del proceso de descarga de los archivos. En realidad, no podemos ver directamente los datos, la información, sino el proceso informático que lleva a acreditar que ese correo fue falseado en sus datos esenciales (como la cabecera de la

[9] Como afirma MAGRO SERVET, 2020, online, epígrafe II, "la prueba digital o electrónica puede ser invisible y de lo que se trata es de hacer visible la prueba digital".

fecha o a quién iba destinado) porque así se ha determinado a partir de un complejo proceso técnico que llega a esa conclusión.

Y si se produce un ciberacoso en redes sociales, la prueba tecnológica consistirá en el análisis de los datos de la IP de conexión en el momento de publicar el contenido para geolocalizar la conexión; la IP de conexión en el momento de registrarse el usuario; todas las IPs de conexión que tenga almacenadas el ISP; el email, número de teléfono, identidad real y todos los datos facilitados por el usuario en el momento de registrarse en la red social; las APPs conectadas con su perfil en la red social; y todas aquellas que los investigadores consideren necesarias para llegar al convencimiento sobre la autoría de una persona en la comisión del hecho delictivo.

El informe pericial elaborado, por tanto, es el resultado inteligible del análisis de los procesos informáticos y evidencias que se pueden descubrir, pero en realidad lo que conforma la prueba se encuentra en los anexos unidos al informe, como el DVD, CD o el pen drive que recoge el contenido de la prueba con los archivos informáticos y los hash y certificados que acreditan el proceso seguido y su integridad.

2º) Consecuencia de su intangibilidad es que la prueba digital es de visualización mediata, no inmediata, como ocurre con la prueba documental o la pericial, es decir, que para ser conocido por el Tribunal o las demás partes se requiere del concurso entre el hardware y un software que permita su visualización, pues debe abrirse el soporte que contiene la información, como por ejemplo, si se trata de archivos ".pst" de correo electrónico, como indicaba, debe abrirse en un ordenador que tenga instalado el correspondiente Outlook, y si se aportan archivos de audio debe tenerse un sistema en el que pueda admitirse el formato mp4. Y ya mucho más complejo es que las partes de un proceso penal obtengan una copia del clonado de ordenadores que efectúan los investigadores, para elaborar su propio análisis de los dispositivos, pues lo que entregan es una imagen forense que, para poder acceder a ella, se requieren herramientas informáticas que no son de fácil acceso.

3º) La prueba digital, al encontrarse en un soporte informático, es replicable o duplicable, es decir, se puede copiar o replicar tantas veces como se desee, trabajando los investigadores sobre el clonado a fin de preservar la evidencia original. Con ello se plantea el problema de distinción de la originalidad, y por esto debe acreditarse indubitadamente que el original y la copia son exactos, bit a bit. Para ello se debe generar una huella digital o un número hash criptográfico que es idéntico en todos los casos y debe consignarse para acreditar la integridad de la información contenida en el dispositivo o recopilada. Es decir, ese hash criptográfico es un algoritmo que tiene la función acreditar que, dados unos datos de entrada, se genera un identificador que garantiza que siempre que tenemos los mismos datos de entrada se va a producir el mismo hash y, por tanto, cualquier cambio que se produzca en la entrada, por pequeño que éste sea, producirá un identificador completamente diferente.

Así, tanto los investigadores privados (que lo hacen ante Notario) como los policiales (bajo la fe del Letrado de la Administración de Justicia), realizan clonado de las evidencias digitales o, en su caso, garantizan la originalidad de la información que entregan los servidores a través del correspondiente certificado de la copia.

4º) Es volátil, es decir, dura poco tiempo. La prueba digital es mudable, inconstante por su propia naturaleza intangible, siendo ésta una de las características más palpables de los delitos cometidos a través de las nuevas tecnologías y que más preocupa para la determinación de la autoría del delito y el dolo.

5º) En relación con la volatilidad, las pruebas de este tipo también son delebles, es decir, la prueba digital puede ser fácilmente destruida, ya sea de forma casual o intencionada, no siendo necesaria la destrucción del soporte digital que la contiene, pues basta con borrar la información, los datos o la huella digital mediante un formateo del disco duro de un ordenador.

Por ejemplo, en unas injurias y calumnias contra un personaje público vertidas en una red social, o en una difusión de un contenido íntimo, o en un delito de provocación al odio contra un colectivo concreto, desde que se vierten hasta que se solicita por la Policía a la red social la información para identificar al autor, los concretos mensajes ya pueden haber desaparecido.

O la propia víctima menor de edad, por ejemplo, que es víctima de un acoso y sextorsión por alguien con el que ha contactado por una red social y, después, le solicita por whatsapp fotografías íntimas, que, en un primer momento, para evitar que sus padres vean las conversaciones, por vergüenza, las borra, hasta que les confiesa lo ocurrido, no pudiendo acreditarlas cuando acude a la policía.

Por eso es esencial llevar a cabo medidas de aseguramiento de la prueba que, por ejemplo, puede ser la denuncia inmediata por la propia víctima a la red social de la publicación solicitándole el aseguramiento y almacenamiento de los datos para poder aportarlos en la solicitud judicial que se haga posteriormente o entregar el dispositivo informático a los peritos para su correspondiente análisis forense y extracción de contenido borrado. Además, los investigadores también pueden solicitar este aseguramiento, como les permite el artículo 588 octies de la Ley de Enjuiciamiento Criminal.

O, por ejemplo, cuando se incauta un router, antes de ser desenchufado, deben realizarse capturas de pantalla de la información contenida en las diferentes partes de las memorias, para obtener datos de qué equipos han estado conectados (MAC, IP usada, estado y tiempo de conexión), IPs de sitios web a los que se ha conectado, con las horas de conexión, siendo la parte más importante a salvaguardar la memoria RAM, ya que es la que se borra al apagar y en ella se guardan los datos de la configuración, las tablas ARP (IPs de conexión y MACs) o las redes a las que está conectado el router, datos todos ellos esenciales para poder acreditar el hecho delictivo. Después, se procede a su desconexión para introducirlo en una bolsa (numerada y

esencialmente, tipo Farady) de evidencias digitales que quedará precintada, junto con el adaptador de corriente para su posterior reconexión en el laboratorio forense, con todas las garantías. Y lo mismo ocurre con los dispositivos móviles, que deben apagarse inmediatamente y las baterías retirarse, si es posible, para conservar la información de ubicación de la torre móvil y los registros de llamadas ya que, si el dispositivo permanece encendido, los comandos de destrucción remota podrían usarse sin el conocimiento del investigador, además de que pueden instalarse actualizaciones que podrían comprometer los datos.

6º) Y ya no sólo es volátil o deleble, sino que la prueba digital es de fácil manipulación, alteración o, incluso, suplantación, lo que añade especial complejidad para que una evidencia digital adquiera capacidad probatoria de la culpabilidad. Pero hay veces que, por mucho que se produzca una alteración, la huella digital deja rastro, aunque solo puede observarse con operaciones técnicas muy complejas.

Así, por ejemplo, la mera conversión de una imagen a otro formato que ocupe menos espacio o simplemente a uno de los admitidos por el sistema Lexnet de presentación de escritos, o la alteración de los metadatos para eliminar el usuario y anonimizar el archivo, o la manipulación de una comunicación para que aparezcan en Whatsapp mensajes como si fueran remitidos por una persona cuando no han sido realmente enviados por ella, supone una alteración de la evidencia, que entraña múltiples dificultades si no aportamos, además, el archivo original en el que conste el archivo o la supuesta comunicación.

Sin embargo, no considero como ARRABAL PLATERO, que la facilidad de manipulación de las evidencias sea la misma que con otros tipos de pruebas no tecnológicas como la modificación de un documento impreso o la declaración de un testigo[10], pues aunque existan tutoriales a disposición del público para alterar y manipular las evidencias electrónicas, como afirma esta autora, no está al alcance de cualquiera llevar a cabo este tipo de manipulaciones, que implica tener unos mínimos conocimientos informáticos y saber utilizar técnicamente los dispositivos.

7º) En ocasiones es parcial, pues está formada por múltiples ficheros informáticos, repartidos en distintos soportes digitales y localizaciones, como por ejemplo un sistema de información en la nube, lo que añade todavía más complejidad en su aprehensión, preservación y análisis.

8º) La prueba digital es heterogénea, precisamente por la diversidad de fuentes, lo que conlleva diferentes formas de incorporación al proceso de las evidencias, a lo que me referiré más adelante.

[10] Vid. ARRABAL PLATERO, 2019, p. 45.

9º) Y es intrusiva, porque en ocasiones puede afectar a derechos y libertades fundamentales de las personas, en concreto puede ser lesiva para la intimidad –incluso de terceros-, o su derecho al secreto de las comunicaciones.

II. **Obtención de la evidencia digital y su conversión en prueba digital**

Para que el Juez forme su convicción, las evidencias digitales que se obtienen por diferentes medios y diligencias deben incorporarse al proceso para convertirse en pruebas digitales y ello puede resultar más o menos complejo en función del comportamiento delictivo y los datos que deben analizarse en los procesos de comunicación, planteándose a veces importantes retos no sólo en esa obtención, sino en la interpretación o análisis de los elementos informáticos forenses.

La incorporación al proceso de la prueba digital no es sencilla. Comenzando porque en la actualidad no tenemos una regulación expresa y sistemática en nuestra legislación procesal de los procesos de obtención y puesta a disposición del Juzgado de las evidencias como un proceso de integración completa que resulte de su tratamiento y valoración. Siguiendo porque no tenemos cobertura legal que pueda garantizar la cadena de custodia y la integridad de la prueba, ello además de la dificultad técnica que entraña (pues exige conocimientos muy específicos y la necesidad de que la prueba digital se presente de forma comprensible para neófitos en la materia). Y terminando con la problemática que existe por la ausencia de infraestructura técnica en las dependencias judiciales para reproducir en Juicio Oral los distintos soportes en los que se encuentran almacenadas las evidencias digitales que dan origen a esa prueba que se trata de hacer valer. Es decir, en ocasiones existe una cierta complejidad para dotar de un valor jurídico a esa prueba, su validez y eficacia procesal, debiendo los abogados definir la estrategia probatoria para enfrentar todos los riesgos de manipulación, alteración o impugnación existentes.

En efecto, actualmente en nuestra legislación procesal no existen directrices en las que pueda basarse un investigador para la obtención de la evidencia digital que, después, puede conformar la prueba. Tenemos un limbo jurídico que en teoría rodea todo su funcionamiento[11].

Contamos con diversas medidas de investigación tecnológica previstas en los artículos 588 bis a octies de la Ley de Enjuiciamiento Criminal. En ellas, se encuentran las medidas de investigación inicial que no requieren autorización judicial puesto que se considera que no afectan a derechos fundamentales, que son las siguientes: acceso a la dirección o identificación del número IP; identificación y conocimiento del número IMSI o IMEI; la identificación de los titulares de un número de teléfono;

[11] A estos problemas procesales por la falta de una norma habilitante para la concreción del procedimiento a través del cual se lleva a cabo el hacking legal ya se refería en 2011, VELASCO NÚÑEZ, 2011, p. 10. Y, en la actualidad, MAGRO SERVET, 2021, online, epígrafe I, insiste en dotar de una verdadera autonomía a esta prueba digital, como también BUENO DE LA MATA, 2014, p. 181.

los seguimientos y utilización de dispositivos técnicos de captación de la imagen -fotografía o videograbación digital- en lugares públicos; y, obviamente, el acceso al contenido público en la red y a las fuentes OSINT). Y a su vez, hay otras que sí requieren autorización judicial porque afectan a derechos y libertades de los ciudadanos, como son: la interceptación de las comunicaciones telefónicas y telemáticas (artículo 588 ter); la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (artículo 588 quáter); la utilización de dispositivos técnicos de seguimiento y localización (art. 588 quinquies); el registro de dispositivos de almacenamiento masivo de información (artículo 588 sexies); el registros remotos sobre equipos informáticos o denominado hacking legal o judicial (artículo 588 septies); y el agente encubierto informático (artículo 282 bis) del que hay que diferenciar otras figuras para las que no se necesita autorización judicial como el ciberpatrullador, el agente que accede a un sistema para compartir simplemente archivos o el empleo inicial de un nickname de un detenido en un canal cerrado para obtener indicios de comisión de delitos.

Sin embargo, la regulación de estas medidas se refiere, básicamente, a los presupuestos comunes (los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad) que tienen que ser reflejados en las resoluciones que se adoptan, previstos en el artículo 588 bis de la Norma Procesal, pero no hace referencia a las directrices que deben seguirse en la obtención, recogida, conservación y almacenamiento de las evidencias digitales, ni al proceso de incorporación de la prueba en el correspondiente procedimiento, ni a la investigación por otros medios como son el volcado de información de servidores, o a la obtención de correos electrónicos o de SMS, al análisis de páginas web o a la investigación por medio de la inteligencia artificial de los delitos cometidos[12].

A su vez, las Circulares de la Fiscalía General del Estado 1/2019 (sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica previstas en la Ley de Enjuiciamiento Criminal), 2/2019 (sobre interceptación de comunicaciones telefónicas y telemáticas), 3/2019 (sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos), 4/2019 (sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y localización) y la 5/2019 (sobre registro de dispositivos y equipos informáticos), todas de 6 de marzo, desarrollan los preceptos legales recogidos en la Ley de Enjuiciamiento Criminal desde un punto de vista exclusivamente jurídico, en

[12] En este sentido, el artículo 14 de la Ley Orgánica 7/2021, de 26 de mayo prohíbe "las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea". Y es obvio que, en la actualidad, no existe cobertura legal para la aplicación de estas tecnologías de inteligencia artificial como, por ejemplo, los sistemas de reconocimiento facial automatizados, por parte de las fuerzas de seguridad y los jueces.

relación al alcance de las medidas, presupuestos y requisitos para su adopción, control de la medida y acceso de las partes, entre otras cuestiones, sin entrar, tampoco, en cuestiones técnicas que son esenciales para garantizar la originalidad e integridad de la prueba digital que, como he dicho, tiene unas peculiaridades propias.

1. *Normativa internacional para la obtención y análisis de evidencias digitales*

Existe normativa extraprocesal que conforma la prueba digital de forma que, aunque no tiene el valor de tratado internacional ni de norma jurídica, regula los estándares internacionales de calidad comúnmente aceptados. Sin embargo, al carecer de cobertura legal ni tiene que ser conocida y aplicada por el Juez de oficio, ni le vincula, lo cual no quiere decir que no deba de ser tenida en cuenta, y que, de no respetarse, sea más sencillo impugnar la prueba digital aportada al procedimiento.

En el ámbito internacional hay dos normas ISO en relación con el análisis forense de la evidencia digital: la ISO/IEC 27037:2012, "Guidelines for identification, collection, acquisition and preservation of digital evidence", y la ISO/IEC 27042:2015, "Guidelines for the analysis and interpretation of digital evidence", que proporcionan un estándar para la identificación, adquisición, recolección, análisis, interpretación y preservación de la evidencia digital.

La ISO/IEC 27037:2012 proporciona orientaciones sobre mejores prácticas en la identificación, adquisición y preservación de evidencias digitales potenciales que permitan aprovechar su valor probatorio y fue ratificada por AENOR en diciembre de 2016. Las bases son que la evidencia digital debe ser adquirida del modo menos intrusivo posible, tras un proceso que sea trazable y auditable, tratando de preservar la utilidad y originalidad de la prueba y que ese proceso debe ser reproducible, comprensible y verificable, y para ello las herramientas utilizadas deben ser contrastadas. Esta norma establece, además, que la evidencia digital es gobernada por tres principios fundamentales:

a) Relevancia, en cuanto a la vinculación del sospechoso con el delito y la víctima, pudiendo ser usada para formular hipótesis o apoyar éstas o ratificar algún hecho o indicio y para el esclarecimiento del delito.

b) Confiabilidad, porque las técnicas utilizadas para la extracción de la evidencia han debido ser probadas previamente, teniendo en cuenta siempre el margen de error de las herramientas forenses, que debe hacerse patente, siendo necesarios los test de eficacia y eficiencia de las herramientas y procesos de los análisis forenses informáticos; y

c) Suficiencia, pues la recolección de evidencias debe estar enfocada a apoyar y confirmar el resto de inferencias, pruebas y otras evidencias del delito, de forma que se deben analizar todos los dispositivos electrónicos hallados y relacionados con el

delito y hay que confirmar que los datos no se han eliminado o alterado en los dispositivos, evitando caer en trampas o errores. A este respecto, debe tenerse en cuenta que existen en línea diversos recursos que permiten a casi cualquier persona dominar técnicas de ocultación, utilización de redes privadas virtuales y re-enrutamiento de direcciones IP, de forma que no es necesario ser un hacker experto para ocultar los datos o falsear información, por lo que debe tenerse presente esta circunstancia en la recogida de evidencias y el análisis forense.

Esta norma también divide en grupos a las personas o especialistas encargados de los diferentes procesos de identificación, recolección, adquisición y preservación de las evidencias digitales: por un lado, especialistas en evidencia digital de primera intervención o Digital Evidence First Responder (DEFRs)[13], especialistas en evidencia digital o Digital Evidence Specialist (DESs)[14] y especialistas en respuestas a incidentes y directores de laboratorios forenses.

Por otro lado, la ISO/IEC 27042/2015, ratificada también por AENOR en diciembre de 2016 establece una serie de presupuestos para el análisis e interpretación de las evidencias digitales y proporciona directrices sobre cómo un perito informático puede abordar la evidencia digital en un incidente o en una intervención pericial, desde su identificación (evidencia digital potencial), pasando por su análisis (evidencia digital), hasta que es aceptada como prueba en un juicio (prueba digital).

Aparte de ellas hay otras normas UNE ISO (como la 71505 y 71506) y Directrices (como la RFC 3227) sobre la recolección de evidencias y su almacenamiento, la gestión de evidencias electrónicas o la metodología para el análisis forense de las evidencias electrónicas.

Es obvio que estas medidas deben utilizarse en todos los procedimientos de obtención de evidencias, porque van a incidir en la valoración que efectúen los Tribunales de la prueba que resulte de ellas[15].

[13] Como indica esta norma, es una persona que está autorizada, formada y habilitada para actuar en la escena de un incidente, y así recoger y adquirir las evidencias digitales con las debidas garantías. Sus responsabilidades serían: asegurar la zona dónde ha sucedido el hecho y los elementos materiales probatorios que se hallen; evitar que personal no autorizado tenga acceso a la zona y a los dispositivos; y realizar fotografías del estado de la zona y documentar el estado de los dispositivos.

[14] Se trata de un técnico, como indica esta norma que, además de poder actuar en determinadas situaciones como DEFR, posee conocimientos, habilidades y preparación, estando especializado en más aspectos tecnológicos. Sus habilidades son: ser un tercero neutral, ajeno al proceso y a los intereses particulares que se encuentren en discusión; ser un experto, con formación, experiencia, conocimientos especializados, científicos o prácticos según el caso; y ser una persona que voluntariamente, acepte incorporar sus conocimientos al proceso.

[15] A este respecto, en el artículo 487 del Anteproyecto de la Ley de Enjuiciamiento Criminal de 2020 bajo la rúbrica «Valor de la diligencia», se indica que "los informes periciales solo tendrán valor probatorio cuando estén basados en técnicas y procedimientos fiables y suficientemente contrastados", indicando en su apartado segundo que "la observancia de la regulación contenida en esta ley sobre la realización del informe pericial será valorada por el tribunal a los efectos de determinar su fiabilidad".

2. *Medios de incorporación al proceso penal de la evidencia digital como prueba: la importancia de la pericial informática*

Como he indicado, la prueba tecnológica puede provenir de diferentes fuentes y, en su incorporación al proceso, sigue pensándose en una prueba documental, cuando, en puridad, no lo es. Esta es la consecuencia de no tener en la era digital en que vivimos una regulación procesal específica. De este modo, suele confundirse el resultado de la diligencia de investigación que se transcribe en un oficio o que, simplemente se reproduce mediante un documento o representación impresa o informática (que constituye, realmente, una prueba de carácter documental y posibilita, incluso, la introducción de pruebas falsas), con el soporte y la prueba digital en sí misma considerada, que no puede ser nunca directamente apreciable a través de los sentidos, sino mediante un proceso informático intermedio que transforma los bits en un formato inteligible por el ser humano.

Lo que se introduce en el proceso no es el soporte material, sino lo inmaterial. Para que la información almacenada de forma digital en un soporte electrónico tenga carácter de documento electrónico se exige que la información contenida pueda ser identificada de forma autónoma, constando tanto la fecha de su creación como la identidad de su autor, los sellos electrónicos, los sellos de tiempo y el servicio cualificado de entrega, como refiere DELGADO MARTÍN[16].

En ese proceso de conversión, sin embargo, se puede producir cualquier manipulación, porque los datos almacenados en sistemas informáticos pueden ser modificados sin que quede ninguna huella al respecto, lo que no resulta complicado cuando los documentos electrónicos son generados utilizando la información existente en equipos o dispositivos bajo el completo control de la parte que va a aportarlos a la causa, ya sea como acusación (cuando, por ejemplo, se aportan conversaciones privadas de una red social para acreditar una extorsión) o como defensa (cuando se aporta, por ejemplo, un documento impreso de una ubicación de Google en la que supuestamente estaba el investigado).

El proceso a través del cual se incorpora a un expediente esa prueba digital, por tanto, es cada vez más complejo y no podemos dejarlo al albur, pues ante una impugnación de la prueba porque no se haya acreditado su integridad y la ausencia de manipulación, la conclusión es que siempre se debe beneficiar al acusado y absolver. Es esencial, por tanto, evidenciar que la prueba digital aportada al proceso se corresponde en su identidad con el original, pues la prevalencia probatoria debe determinarse en función de la robustez de su contenido inmaterial y la autenticidad e inalterabilidad de éste. No es que diga que resulta inválida la prueba incorporada a través de documentos impresos, digitales o electrónicos[17] -fácilmente manipulables-, sino

[16] Vid. DELGADO MARTÍN, 2022, online, apartado 5.1a).

[17] El art. 3.5 de la derogada Ley 59/2003, de 19 de diciembre, definía el documento electrónico como aquel que incluye información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico

que no garantiza su indemnidad y, por tanto, puede que no sea eficaz para desvirtuar el derecho a la presunción de inocencia. Por ello, si queremos acreditar el hecho punible y la autoría debemos tender a una mayor exhaustividad para garantizar la originalidad e integridad del contenido digital para que goce de todas las garantías procesales y sea correctamente valorada.

Hay diferentes formas de incorporar al proceso esa prueba digital como resultado de la evidencia electrónica analizada y tratada pero, ante una impugnación del contenido de la prueba documental impresa, de los oficios policiales, de la aportación de videos, pantallazos u otro tipo de evidencias, el informe pericial informático es la única prueba de autenticidad que puede concluir la comisión del delito y la autoría del culpable.

Es decir, debe realizarse el examen de las evidencias por expertos informáticos, que cada vez están teniendo más presencia en nuestros Tribunales. La pericial informática, empero, tampoco puede considerarse la prueba digital en sí misma (al igual que no lo es la documental), sino que constituye la forma a través de la cual se podrá incorporar la prueba digital a un procedimiento judicial. El informe pericial lo que hace es reflejar el análisis de las evidencias, es decir, la fuente de prueba, y llegar a unas conclusiones objetivas.

En este sentido, cuando se trata de incorporar al proceso contenido de páginas web, comentarios en redes sociales, mensajes en chats públicos o privados de distintas aplicaciones de mensajería instantánea, o correos electrónicos, la mera incorporación del formato impreso digital como documento, la mera captura de pantalla, sin

según un formato determinado y susceptible de identificación y tratamiento diferenciado. Esta definición no ha sido incluida en la actual Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, pero, acudiendo al artículo 26 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, al apartado II de la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico, y al artículo 3.35 del Reglamento (UE) nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado, podemos concluir que documento electrónico es todo aquel que está almacenado en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado, que contiene información o un conjunto de datos de cualquier naturaleza (ya sea texto escrito o registro sonoro, visual o audiovisual) y cuyos componentes son, además de su contenido, la firma electrónica y los metadatos. De hecho, la jurisprudencia, desde 2007, ha venido admitiendo este concepto amplio de documento para integrar el delito de falsedad documental de los arts. 390 y siguientes, como todo objeto corporal que refleja una realidad fáctica con trascendencia jurídica, aunque ya no se le identifique ni con el papel, como soporte, ni con la escritura, como unidad de significación, entendiendo que cabe el electrónico en cuanto se encuentra representado en datos electromagnéticos o informáticos y almacenado o contenido en un soporte o elemento físico de tal naturaleza. Desde la Sentencia del Tribunal Supremo 1066/2009, de 4 de noviembre (ECLI:ES:TS:2009:7129) hasta la Sentencia del mismo Tribunal (caso Gürtel) 507/2020, de 14 de octubre (ECLI:ES:TS:2020:3191), reiterada por muchas otras, se ha indicado que "el soporte papel ha sido superado por las nuevas tecnologías de la documentación e información", afirmando que se considera documento "cualquier sistema que permita incorporar ideas, declaraciones, informes o datos susceptibles de ser reproducidos en su momento", porque "imprime en las neuronas tecnológicas, de forma indeleble, aquello que se ha querido transmitir por el que maneja los hilos que transmiten las ideas, pensamientos o realidades de los que se quiere que quede constancia".

identificar el proceso por el que se ha obtenido ni garantizar la obtención, no es suficiente para extraer las conclusiones de prueba que se pretenden. Ese mero documento privado (o, incluso, público, si se protocoliza ante Notario o si se transcribe bajo la fe del Letrado de la Administración de Justicia) se limitar a reflejar un dato, pero no acredita la originalidad ni la realidad del envío de un mensaje o de un comentario en una red social ni la autoría de quien se encuentra detrás de un usuario o cuenta de correo, ni es suficiente para identificar la titularidad de una dirección IP[18], cuestiones que son esenciales para completar toda la prueba y llegar a acreditar un hecho ilícito.

No podemos limitarnos, por tanto, a obtener y aportar una captura de pantalla porque, con ello, únicamente presentamos aquello que aparece exteriorizado, que en realidad no es la totalidad de lo que se encuentra almacenado en el soporte electrónico de que se trate, pues no queda constancia de la integridad de los medios en que se almacenaba originalmente la información, y en particular su preservación a los efectos de posteriores comprobaciones e informes. No podemos hacer depender la validez y eficacia de la prueba de que el acusado impugne o no el documento o reconozca su contenido.

Esta ausencia de garantía ya fue reflejada por la Sala Segunda del Tribunal Supremo en la Sentencia 300/2015, de 19 de mayo[19] cuando, ante una comunicación mantenida entre dos personas a través de una red social, se consideró que no era suficiente aportar los meros pantallazos de la conversación, porque podían ser susceptibles de ser manipulados, indicando esta resolución, en su Fundamento Jurídico Cuarto, 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"[20]. O en un correo electrónico, pues la mera aportación del documento impreso no garantiza el origen, el contenido y la ausencia de alteración entre que salió del servidor del remitente y llegó al del destinatario[21].

[18] Sentencia del Tribunal Supremo 987/2012, de 3 de diciembre (ECLI:ES:TS:2012:8316).

[19] ECLI:ES:TS:2015:2047.

[20] Vid., también, Sentencias del Tribunal Supremo 754/2015, de 27 de noviembre (ECLI:ES:TS:2015:5421), 782/2016, de 16 de octubre (ECLI:ES:TS:2016:4517), 291/2019, de 31 de mayo (ECLI:ES:TS:2019:1786) y 332/2019, de 27 de junio (ECLI:ES:TS:2019:2205), así como Sentencia de la Audiencia Provincial de Asturias 474/2019, de 23 de diciembre (ECLI:ES:APO:2019:3692) y de la Audiencia Provincial de Badajoz 176/2019, de 9 de octubre (ECLI:ES:APBA:2019:1175). Asimismo, DELGADO MARTÍN, 2015, RODRÍGUEZ LAINZ, 2015, y GARCÍA MESCUA, 2018.

[21] Sobre la valoración probatoria del correo electrónico, páginas webs y whatsapp, vid. ARMENTA DEU, 2018 y RUBIO ALAMILLO, 2016.

La garantía de que no existe manipulación solo se obtiene, como se ha indicado, mediante la elaboración del correspondiente dictamen pericial informático, ya sea privado o de la Policía Judicial, cuyo trabajo consistirá principalmente en el desarrollo de procedimientos encaminados a preservar las evidencias digitales, a través de la realización de copias forenses o clonados de la información digital almacenada, y el análisis que resulte necesario para la investigación, trasladando el resultado a un informe pericial técnico que será el que se aporte en el procedimiento penal[22].

Esta relevancia la hemos visto en decenas de ocasiones en los últimos años, pero es mucho más impactante en supuestos en los que se encuentran implicados menores, como ocurrió en el analizado en la Sentencia de la Audiencia Provincial de Madrid 481/2020, de 9 de diciembre[23], seguido por un delito de elaboración de pornografía infantil en el que una persona consiguió, mediante amenazas e intimidación, que la víctima menor de edad le enviase videos de contenido sexual. En ese caso fue esencial el análisis del móvil de la víctima, que entregó como evidencia cuando efectuó la denuncia, y del ordenador del acusado, así como la elaboración de la correspondiente pericial informática con los datos obtenidos, para constituir la prueba digital que enervó el derecho a la presunción de inocencia. Preservar en ese momento de la denuncia, por tanto, la integridad de la evidencia para realizar la pericia informática es fundamental y los agentes deben tener especial cuidado en seguir todos los protocolos para ello.

En definitiva, la finalidad de la aportación de pruebas electrónicas mediante informe pericial informático, en caso de evidencias digitales, supone garantizar en el proceso judicial la originalidad, autenticidad e integridad de la información digital que se presente como prueba digital.

A la misma conclusión debe llegarse en relación con las medidas de investigación tecnológica a que antes me refería, pues en las intervenciones telefónicas por parte de la Policía Judicial, ésta se limita a indicar en sus Oficios que el Centro de recepción que asume la responsabilidad de recibir la señal e información originales de las operadoras en el Sistema Integral de Interceptación de las Comunicaciones Electrónicas (SITEL), que está localizado en dependencias policiales y el día, hora e intervinientes, pero cuando se trata de hacer valer en Juicio el contenido de conversaciones telefónicas que se han intervenido, no debemos introducirlas simplemente a través de la referencia a las transcripciones que figuran en las actuaciones, sino que debe exigirse la reproducción del contenido obrante en el soporte digital concreto[24].

[22] En extenso, sobre la prueba pericial informática, vid. MARTÍNEZ GALINDO, 2021, pp. 741 a 771.

[23] ECLI: ES:APM:2020:14598.

[24] Sobre los requisitos de las intervenciones telefónicas para ser consideradas pruebas de cargo susceptibles de ser valoradas en Plenario, la Sentencia del Tribunal Supremo 23/2015, de 4 de febrero (ECLI:ES:TS:2015:219), establece que debe producirse "1) La aportación de las cintas. 2) La trascripción mecanográfica de las mismas, bien integra o bien de los aspectos relevantes para la investigación, cuando la prueba se realice sobre la base de las transcripciones y no directamente mediante la audición de las cintas. 3) El cotejo bajo la fe del Secretario judicial de tales párrafos con las cintas originales, para el caso de que dicha

Sin embargo, en la actualidad es absolutamente posible la manipulación de los archivos digitales de voz, para poder construir una conversación ilícita a partir de otras grabaciones (véase el sistema deepfake utilizado en algún anuncio de televisión), lo que conlleva la necesidad de asegurar su autenticidad a través del correspondiente proceso técnico. Esto me lleva a pensar en la necesidad como abogada de que, ante cualquier duda en las transcripciones o en la identidad de los interlocutores de los teléfonos intervenidos, debe impugnarse, siempre, la prueba, para que se garantice el sistema de volcado y la integridad de los contenidos[25].

En las grabaciones de comunicaciones orales estaríamos ante la misma situación, porque en los Oficios que se remiten al Juzgado no se indica qué sistema es el empleado para la grabación, ni cómo se lleva a cabo la instalación de los micrófonos y en qué lugares o a que distancia, ni se identifican los aparatos de grabación del sonido ambiental (marca, modelo, software, modo de archivo de las grabaciones y demás datos), ni el procedimiento para la activación y desactivación, distancia, por medio de qué sistema (por teléfono, GPS, internet, etc.), a qué distancia se encontraban los agentes, en qué tipo de soporte quedó archivado, cómo se produce el volcado de las conversaciones e intervenciones telefónicas y demás vicisitudes que garantizan que la prueba es original y se ha practicado con todas las garantías. Toda esta información

trascripción mecanográfica se encargue -como es usual- a los funcionarios policiales. 4) La disponibilidad de este material para las partes. 5) Y finalmente la audición o lectura de las mismas en el juicio oral, que da cumplimiento a los principios de oralidad y contradicción, previa petición de las partes, pues si estas no lo solicitan, dando por bueno su contenido, la buena fe procesal impediría invocar tal falta de audición o lectura en esta sede casacional", indicando, con referencia a la Sentencia del Tribunal Constitucional 128/1988, que no habiéndose impugnado no se le puede negar valor probatorio a las transcripciones.

[25] Sobre esta cuestión resulta de interés la Sentencia del Tribunal Supremo 492/2016, de 8 de junio (ECLI: ES:TS:2016:2557), en la que se cuestionan las intervenciones telefónicas, la grabación ejecutada mediante el sistema SITEL y el volcado de la información, afirmando que "la puesta en tela de juicio del SITEL, cuando se limita a cuestionar in abstracto la fiabilidad del sistema, o de manera genérica la autenticidad del contenido de los discos aportados, sin apuntar razones que hagan pensar que, en el caso concreto que es objeto de examen, pudo haberse producido alguna manipulación de los contenidos de los CDs aportados al Juzgado, no puede tener acogida", e indicando esta resolución que este sistema "por definición, carece de soporte original, en la medida en que las conversaciones se registran en un ordenador central del que se extraen las sucesivas copias", añadiendo que "las características técnicas del disco sobre el que se vuelcan los datos no es el dato relevante, sino las garantías del sellado que acompaña a los soportes que son ofrecidos a la autoridad judicial (STS 636/2012, de 13 de julio). Asimismo, esta resolución indica que "aunque en los autos de intervención telefónica se establece que el disco magnético óptico original se pondrá a disposición judicial una vez finalizada la intervención o cuando se complete su capacidad, ello no significa que el disco duro deba entregarse materialmente al Juzgado, sino que como medio de investigación judicial que ejecuta la policía, tales grabaciones permanecen en el disco duro hasta que la autoridad judicial ordene su borrado, pues en cualquier momento del proceso es posible la verificación de la integridad de los contenidos volcados a los soportes CD/DVD entregados en el juzgado, mediante su contraste con los que quedan registrados en el Servidor Central del SITEL a disposición de la autoridad judicial. Contraste que puede realizar el juzgado en los correspondientes terminales para acreditar su identidad con la matriz del servidor central", y añadiendo que "los policías encargados de la investigación no acceden en ningún momento al sistema central de almacenamiento, recogiendo únicamente un volcado de esa información con la correspondiente firma electrónica digital asociada, transfiriéndola a un CD/DVD para su entrega a la Autoridad judicial, garantizando de esta manera la autenticidad e integridad de la información almacenada en el sistema central, y en cuanto a una posible manipulación de los contenidos de los CDs aportados al Juzgado, no expone las razones que fundamenten sus sospechas".

pertenece a la cadena de custodia, a la que ahora me referiré, pero es esencial su registro porque, de otro modo, la integridad de la prueba no podría garantizarse plenamente, ya que las partes y el Tribunal carecen de la información básica para dar por válida la información obtenida con esas grabaciones.

O cuando se utilizan dispositivos de seguimiento y localización GPS o colocación de balizas, simplemente se incorpora al proceso el resultado de esos seguimientos, pero nunca suele plantearse que esa información ha podido ser manipulada. Se parte de la veracidad de los datos porque un agente de Policía Judicial así lo indica. Sin embargo, el Oficio que vuelca los datos obtenidos con el seguimiento no garantiza la integridad de esa información porque mediante aplicaciones que no exigen grandes conocimientos informáticos, un tercero puede inducirse en el terminal móvil para que facilite una información de geolocalización falsa con una mera modificación de los ajustes del terminal, habilitando las opciones de desarrollador, entre las cuales el sistema permite ubicaciones simuladas. Por ello, la geolocalización no puede considerarse una prueba plena, tampoco, en el proceso penal a menos que se acredite la integridad de la información mediante el oportuno informe técnico, salvo que la geolocalización se requiera de las propias compañías operadoras de telefonía a través de sus antenas de repetición, conforme a la obligación de conservación de los datos de tráfico generados o tratados en el marco de prestación de servicios de comunicación, en vez de a través de la localización del propio terminal con aplicaciones móviles.

Y tampoco sería prueba plena cuando se incorpora una fotografía o un video proveniente de seguimientos policiales a un investigado, en que no se anexa el archivo digital, sino únicamente el soporte plasmado en el correspondiente atestado o informe de inteligencia policial, pero es obvia la capacidad que existe actualmente de editar estos archivos.

Por otro lado, en el registro de dispositivos de almacenamiento masivo de información (artículo 588 sexies), hay que tomar en cuenta que cualquier dispositivo electrónico (un ordenador, una tablet, un smartphone, un GPS, un iPod, una cámara digital, etc.) tiene ficheros almacenados en su disco duro o en su memoria que, de una forma o de otra, puede copiarse, moverse, borrarse y editarse y que, aunque existan medidas de seguridad que cada vez son más exhaustivas, pueden ser objeto de manipulación o pirateo con la instalación de un virus. En consecuencia, el mero análisis de la información que suele hacerse por la Policía Judicial no sería suficiente para garantizar la integridad e indemnidad de los datos, porque la manipulación se ha podido producir con anterioridad al clonado sobre el que trabajan los investigadores. Hay multitud de ejemplos de manipulaciones de teléfonos, donde el emisor no es realmente el emisor; de aparatos GPS que mandan coordenadas de una ubicación por donde jamás pasaron; de correos electrónicos enviados por emisores que jamás tuvieron email; de fotografías que muestran una escena que nunca sucedió; de videos que muestran una secuencia de imágenes que nunca tuvieron lugar, y muchos otros ejemplos.

Distinto es el registro remoto sobre equipos informáticos o denominado hacking legal o judicial (artículo 588 septies) y el agente encubierto informático (artículo 282 bis) porque en ambos casos, la garantía de indemnidad de los datos obtenidos está soportada, precisamente, en la prueba pericial tecnológica que se elabora con los pasos concretos de la diligencia de investigación, obrantes en pieza secreta[26].

En definitiva, considero que estamos en un ámbito absolutamente novedoso e incierto por el avance de la tecnología, que no está siendo correctamente valorado en sede judicial, pues se parte de determinadas presunciones que no pueden considerarse plenamente ciertas. Deben modificarse los planteamientos de incorporación al proceso de todas estas diligencias que contienen evidencias digitales porque, para conformar la prueba digital, igual que no es suficiente la aportación de meros pantallazos o documentos impresos, tampoco puede serlo la mera aportación de los archivos con las conversaciones intervenidas o grabadas o las localizaciones GPS. Y para garantizar la inexistencia de manipulación en estos archivos, debe exigirse la correspondiente pericial técnica que acredite la integridad de todos los datos que, hasta ahora, no se incluyen en los oficios policiales. Es la importancia de lo invisible, pero esencial si queremos mantener la originalidad de la prueba y que ésta despliegue todos sus efectos en el proceso.

En este sentido, no puede equipararse la incorporación a la causa de la evidencia digital cuando se trata de datos electrónicos de una comunicación o informáticos con las impugnaciones de cadena de custodia que ya están resueltas por nuestros Tribunales en el sentido de que, como señala la Sentencia del Tribunal Supremo 990/2016, de 12 de enero[27] (Fundamento Jurídico Decimotercero) para considerar su ruptura "no es suficiente con el planteamiento de dudas de carácter genérico", sino que tiene que existir una duda razonable y 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"[28]. En el caso de la prueba digital debe dudarse, siempre, de su originalidad, pues a la parte que la impugna le resultaría imposible plantear dudas razonables más allá de la mera característica manipulable de la evidencia electrónica, como afirmaba la antes referida Sentencia del Tribunal Supremo 300/2015, de 19 de mayo.

Esto es similar a lo que ocurría hace veinticinco años cuando comencé en el ejercicio de la abogacía cuando, en una alcoholemia, no se acompañaba al atestado el certificado que acreditaba que el alcoholímetro había pasado todas las revisiones y,

[26] A este respecto, como indica SÁNCHEZ GONZÁLEZ, 2022, online, epígrafe II, el agente encubierto informático debe documentar sus actuaciones en actas que serán puestas a disposición del Juez de instrucción a la mayor brevedad posible, avalando la Sentencia del Tribunal Supremo 104/2019, de 27 de febrero (ECLI:ES:TS:2019:658), que las citadas actas puedan incorporarse en el acto de la vista sin que ello afecte al derecho a la defensa cuando los investigados han conocido el resultado de la investigación a través de las resoluciones procesales.

[27] ECLI:ES:TS:2017:80.

[28] Vid, también, Sentencia del Tribunal Supremo 115/2014, de 25 de febrero (ECLI:ES:TS:2014:764).

ante la duda, se absolvía. Los Tribunales confiaban en la palabra de los agentes y en la garantía del aparato, hasta que empezaron a impugnarse esos resultados. Ahora, por tanto, debería ocurrir algo similar: si no está garantizada la integridad de la información mediante el oportuno proceso pericial informático de descarga de los datos que garantice la originalidad y la no manipulación de las pruebas procedentes del análisis de evidencias digitales, la duda debería motivar que el Tribunal, ante una impugnación, deba inclinarse por la absolución, sin necesidad de acreditar que existan indicios de manipulación, pues la prueba del delito debe aportarla la acusación y ser eficaz para una condena. En materia de prueba digital no debe otorgarse presunción de veracidad a lo que los agentes de Policía Judicial incorporan a un Oficio, porque es manipulable aun sin que ellos puedan ser conscientes.

Si nos estamos desenvolviendo y actuando en el mundo digital hay que adaptarse a él en el modo probatorio y, por tanto, acudir a los medios y herramientas que aporten garantías y protejan los contenidos y la información en soportes automatizados, lo que nos obliga a que si queremos aportar una evidencia digital para que se pueda considerar verdadera prueba, deben adoptarse una serie de cautelas que de ordinario no se adoptan y no confiar ciegamente en los procesos electrónicos, fácilmente manipulables con los conocimientos adecuados.

III. **Problemática asociada a la incorporación al proceso de la prueba digital y su incidencia sobre los principios penales**

Tanto las medidas de investigación tecnológica a que me he referido de los artículos 588 bis y siguientes de la Ley de Enjuiciamiento Criminal como la incorporación de pruebas digitales por particulares, pueden generar cierta problemática cuando se incorporan al proceso, porque puede derivar en una prueba ilícita cuando se produce una vulneración de los derechos fundamentales, afectando, con ello, a la proporcionalidad, o bien en una prueba ineficaz para desvirtuar el derecho a la presunción de inocencia, porque exista una ruptura de la cadena de custodia o por la manipulación de las evidencias, circunstancia esta última a la que me he referido más arriba.

Junto a esta problemática existen otros supuestos, como el elevado coste económico de examinar e interpretar la información contenida en una evidencia digital con la elaboración del informe pericial informático, lo que afecta a multitud de casos en los que se denuncian hechos o se interpone una querella por un particular por un delito de no excesiva gravedad, que debe acudir a peritos privados para garantizar la eficacia de la prueba para acreditar el hecho delictivo o, al menos, los indicios que motiven la incoación del proceso penal; o las dificultades de obtención de la prueba digital por el fenómeno transnacional de la ciberdelincuencia, la desterritorialización o supraterritorialidad y el carácter transfronterizo de estos delitos, cuando se comete

el delito en varios países (y múltiples servidores) para evitar la acción policial y judicial, siendo la incorporación de las pruebas al proceso penal poco menos que imposible, sobre todo cuando se necesita la colaboración de países que se encuentran fuera del ámbito europeo y con los que no existen Convenios de cooperación judicial internacional.

1. *Ilicitud de la prueba electrónica por vulneración de derechos fundamentales*

La admisibilidad de la prueba electrónica debe cumplir los requisitos exigidos a cualquier otro medio de prueba: pertinencia, utilidad y licitud. Decía antes que una de las características de la prueba digital es que puede ser intrusiva, de forma que las medidas de investigación tecnológica y la obtención de cualquier evidencia de este tipo debe llevarse a cabo respetando íntegramente los derechos y libertades fundamentales de las personas, que protege nuestra Constitución, ya que si no se hace así se convierte en prueba ilícita, cuyo concepto se remonta a la Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre, cuando se prohibió expresamente la aportación de pruebas al proceso que hubieran sido obtenidas mediante la vulneración de derechos fundamentales. El año siguiente, la Ley Orgánica del Poder Judicial, tuvo que regular esta circunstancia en su artículo 11.1. En él se menciona que "toda prueba que se obtenga por violación de un derecho fundamental ha de ser considerada nula" y, por tanto, no puede valorarse ni los Tribunales podrán tenerla en cuenta para basar en ella una Sentencia condenatoria.

Se convertiría en una prueba digital envenenada. Todas las limitaciones o restricciones a los derechos fundamentales, en consecuencia, por exigencia constitucional, deben ser proporcionadas a los fines perseguidos por el ordenamiento. Por ello, debe fundarse en esta exigencia constitucional, por una parte, el principio de culpabilidad penal[29] y, por otra, la ilegitimidad constitucional de todas aquellas sanciones que deriven de una investigación que no guarde una lógica correlación valorativa con la gravedad de cada ilícito, porque si las medidas limitativas de un derecho fundamental adoptadas resultan desproporcionadas para la defensa del bien jurídico que da origen a la restricción, ésta deviene contraria a Derecho.

En este sentido, cuando hablamos de vulneración de derechos fundamentales que se producen en la obtención de las evidencias derivadas bien un proceso comunicativo o bien de un proceso tecnológico, puede llegar a producirse una injerencia, esencialmente en el derecho al secreto de las comunicaciones y a la intimidad personal y familiar, sin perjuicio de la afectación que puede producirse en otros derechos como el honor, propia imagen, inviolabilidad domiciliaria o el derecho fundamental al propio entorno virtual, de nueva generación, que protege la información digital que va

[29] Una exposición magistral de los problemas derivados de este principio, marginal ahora al desarrollo del texto, puede verse en CÓRDOBA RODA, 1977.

generando el usuario a través de las nuevas tecnologías[30], pudiendo considerarlo dentro del derecho genérico a la intimidad y privacidad digital.

La vulneración en el derecho al secreto de las comunicaciones se produce, por ejemplo, cuando las intervenciones telefónicas se practican sin la debida autorización judicial (como los supuestos de conversaciones telefónicas grabadas por el particular que luego aporta al procedimiento, lo que constituye, como es lógico, la mayor de las injerencias) o, aun cuando exista autorización judicial, si se siguen practicando intervenciones sin que se hayan prorrogado en plazo, o cuando se haya acordado con una motivación insuficiente del Auto habilitante o por falta de proporcionalidad. Así, por ejemplo, tenemos la Sentencia del Tribunal Supremo 296/2022, de 24 de marzo[31], que anula las intervenciones telefónicas por falta absoluta de motivación que las sustentara (y sin referencia, siquiera, a los Oficios policiales en que se instaban), en sendos delitos de receptación y falsedad; la Sentencia del Tribunal Supremo 699/2021, de 16 de septiembre[32], que confirma la nulidad de las intervenciones telefónicas acordadas para la investigación de tramas defraudatorias de IVA en operaciones intracomunitarias, al considerar que carecía de proporcionalidad al ser un delito fiscal cuya prueba es, esencialmente, de carácter documental y que, por tanto, podía obtenerse por otros medios; o la Sentencia del mismo Tribunal 2/2018, de 9 de enero[33], que confirma la nulidad porque en el Auto habilitante no se especificaron los indicios objetivos suficientes de la posible existencia de una organización criminal dedicada al tráfico de drogas, como también ocurrió en la Sentencia de la Audiencia Provincial de Madrid 345/2018, de 3 de mayo, en un famoso caso de corrupción policial[34].

Y este derecho resulta, también, conculcado, motivando la ilicitud de la prueba, cuando se llevan a cabo las medidas de investigación en el ámbito digital sin autorización judicial cuando afectan a los datos de tráfico asociados y a las comunicaciones. En relación con ello, la Sentencia del Tribunal Supremo 16/2014, de 30 enero[35] determinó la ilicitud de la prueba electrónica aportada (correos electrónicos entre los acusados, en un supuesto de cohecho, y las periciales derivadas de ellos) por considerar que las solicitudes formuladas directamente por la Policía a las compañías Microsoft (de acceso y extracción de datos de los correo electrónicos intercambiados, y de datos relativos a las conexiones IP) y Movistar (de informe sobre los datos relativos a las conexiones IP respecto a la cuenta de correo electrónico atribuida al acusado) sin obtener la autorización judicial previa, eran ilícitas porque afectaban al secreto de las comunicaciones. En la actualidad, la Sección 3ª del capítulo V del Título

[30] Vid. el análisis que efectúa de este derecho ARRABAL PLATERO, 2019, pp. 168 a 172.
[31] ECLI:ES:TS:2022:1097.
[32] ECLI:ES:TS:2021:3431.
[33] ECLI:ES:TS:2018:707.
[34] ECLI:ES:APM:2018:3565. Esta Sentencia fue revocada parcialmente por el Tribunal Supremo (Sentencia 55/2020, de 18 de febrero, ECLI:ES:TS:2020:383).
[35] ECLI:ES:TS:2014:217.

VIII de la Ley de Enjuiciamiento Criminal, que recoge en sus artículos 588 ter k) a m) el "acceso a los datos necesarios para identificación de usuarios, terminales y dispositivos de conectividad", y el artículo 588 ter j, que regula la incorporación al proceso de datos de tráfico o asociados que se encuentren vinculados a procesos de comunicación, que establece que la incorporación de los datos obrantes en archivos automatizados de los prestadores de servicios requerirán siempre autorización judicial, establece los límites que tienen los investigadores de la Policía Judicial en sus solicitudes a esos prestadores, aportando más claridad de la que existía antes de 2015 en este ámbito para impedir que las diligencias se conviertan en nulas por vulneración de derechos fundamentales. A su vez, la Circular 2/2019 de la Fiscalía General del Estado a que antes me he referido, ahonda en esta cuestión y de ella se desprende la obligatoriedad de ser cauto en la incorporación al proceso penal de forma indiscriminada y generalizada de los datos de tráfico asociados a las comunicaciones de los que pudiera disponer el prestador de servicios, por la gran injerencia que tienen en el derecho al secreto de las comunicaciones del investigado, debiendo justificarse especialmente la proporcionalidad y la necesidad para la investigación de delitos que requieran cierta gravedad, lo que deja fuera –y determinaría la ilicitud de la prueba, aun contando con autorización judicial- muchos delitos cometidos a través de las nuevas tecnologías que, aunque en el artículo 588 ter a) se prevén expresamente, no cumpliría el juicio de proporcionalidad rector de estas medidas. Ello, con independencia, de la monitorización de conductas sospechosas que puede llevar a cabo el propio prestador de servicios en supuestos de pornografía infantil, a raíz de la aprobación del Reglamento del Parlamento Europeo y del Consejo 2021/1232, de 14 de julio de 2021[36].

Otro de los derechos fundamentales cuya vulneración puede producirse en la investigación tecnológica es el derecho a la intimidad, en el que deben distinguirse dos escenarios: cuando la prueba digital la presenta un particular y cuando se incorpora al proceso a través de las medidas de investigación policiales.

En el primer caso, cuando se trata de pruebas digitales aportadas por terceros que acreditan la comisión de un delito, aunque en principio afecten a la intimidad o desvelen datos privados de la vida del denunciado, prima el fin superior, que es el descubrimiento del delito, aunque se esté vulnerando su derecho a la intimidad. A este respecto, son relevantes las tan conocidas Sentencias del Tribunal Supremo 116/2017, de 23 de febrero[37] sobre la validez de la lista Falciani publicada para descubrir delitos fiscales de determinadas personas, o la 214/2018, de 8 de mayo[38], sobre

[36] En este sentido, el citado Reglamento del Parlamento Europeo y del Consejo 2021/1232, de 14 de julio de 2021 (llamado "Chatcontrol") supone una limitación a otra de las importantes Directivas sobre protección de datos, la Directiva ePrivacy (Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002) al permitir que los proveedores de servicios de comunicaciones interpersonales tengan acceso y monitoricen los mensajes sospechosos de tener este contenido delictivo de pornografía infantil.

[37] ECLI:ES:TS:2017:471.

[38] ECLI: ES:TS:2018:1551.

el caso FITUR, que declara válidas las grabaciones realizadas por un particular que denunció la trama Gürtel. Por el contrario, la Sentencia 489/2018, de 23 de octubre[39], dictada en el caso Trimarine, declara prueba ilícitamente obtenida los correos de un trabajador aportados por una empresa para acreditar una apropiación indebida porque se considera que existía una injerencia en la intimidad. Esta última resolución es clara al advertir (conforme a la STEDH caso Barbulescu) que para que sea legítima la intromisión del empresario en la intimidad del trabajador debe haberse advertido previamente de que el uso de los medios informáticos ha de limitarse estrictamente a tareas profesionales y la posibilidad de acceso a ellos por parte de la empresa[40].

Pero también la Sentencia del Tribunal Supremo 786/2015, de 4 de diciembre[41], plantea la licitud de una condena por un delito de pornografía infantil cuya prueba provenía del análisis del ordenador del acusado por parte de la Policía Judicial cuando acudió a ella el encargado de repararlo, quien descubrió de forma casual el contenido pedófilo, considerando válida la prueba porque " su propia intimidad debía quedar desplazada ante la concurrencia de un fin constitucionalmente legítimo, en este caso, la investigación y descubrimiento de delitos de incuestionable gravedad" (Fundamento Jurídico Primero). O la Sentencia del mismo Tribunal 864/2015, de 10 de diciembre[42], que confirma la validez, como prueba de un delito de abuso sexual, de los datos obtenidos por una madre de la cuenta abierta por su hija menor de edad en Facebook, considerando que, aunque la menor no hubiera otorgado su permiso al respecto, la madre actuó ante la sospecha de que la niña pudiera estar siendo víctima de ciberacoso y para protegerla (lo que ha sido corroborado por el mismo Tribunal en el Auto 653/2022, de 16 de junio[43]).

Por otro lado, cuando las medidas de investigación se producen en el seno de un procedimiento judicial, el derecho a la intimidad puede verse comprometido cuando por ejemplo, en las entradas y registros en domicilios particulares o de sociedades -en los que se autoriza, también, el análisis y registro de dispositivos informáticos- se produce la incautación de todos los dispositivos sin distinción alguna, aun cuando sean titularidad de terceros (familiares o no), tratando de justificar la incautación masiva en indicios muy débiles y desproporcionados (como después se confirma cuando se produce el clonado y análisis y no se encuentra información relacionada con el hecho delictivo); o cuando en el Auto de entrada y registro no se prevé, de forma expresa, la incautación de dispositivos; o cuando, una vez incautados, no existe autorización para el concreto registro y acceso a los datos contenidos en ellos y, aun así, se accede. Pero las más graves injerencias que se producen en la intimidad

[39] ECLI: ES:TS:2018:3754.

[40] Esta resolución, junto con la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, motivó un cambio importante en la forma de tratar los datos obrantes en los dispositivos tecnológicos entregados a los trabajadores.

[41] ECLI:ES:TS:2015:5362.

[42] ECLI:ES:TS:2015:5809.

[43] ECLI:ES:TS:2022:9902A.

son en el ámbito de las grabaciones de comunicaciones orales y en el registro remoto sobre equipos informáticos o el denominado hacking legal o judicial.

Si la instalación de micrófonos para llevar a cabo la captación de comunicaciones orales se realiza sin justificar debidamente la injerencia en este derecho fundamental, es evidente que debe declararse su ilicitud. Antes de introducir el artículo 588 quáter c) en la Ley de Enjuiciamiento Criminal ésta se declaraba radicalmente nula, como se apreció, por ejemplo, en las Sentencias del Tribunal Supremo 747/2015, de 19 de noviembre y 491/2019, de 16 de octubre[44] y en la Sentencia del Tribunal Constitucional 145/2014, de 22 de septiembre. En la actualidad, sin embargo, aunque está prevista, siendo una medida tan gravosa solo puede autorizarse en supuestos extremadamente excepcionales y exigiendo una motivación y justificación muy exhaustiva. Y ello porque no sólo afecta a la intimidad del investigado sino de terceras personas.

Así, si esas grabaciones se producen en lugares públicos (un restaurante, un bar, en el interior de un vehículo[45], en la calle o, incluso, en una oficina abierta al público) podemos encontrar planteamientos de nulidad bien porque la autorización llega después de haberse grabado, o porque se hace una diligencia indicando que el Juez ha autorizado verbalmente, o no se motiva suficientemente, o porque los indicios que había para autorizarla eran inválidos. Debe considerarse en principio, que se trata de pruebas electrónicas o digitales que, justificadas, no suponen una injerencia excesiva en el derecho a la intimidad, pero mayor cuidado debe tenerse en un domicilio particular, en una consulta médica o en un despacho profesional u oficina no abierta al público, es decir en un ámbito cerrado, íntimo y privado, donde se desarrolla el núcleo duro de la intimidad.

A este respecto, en relación con la instalación de micrófonos y captación de comunicaciones orales en un domicilio, la Sentencia del Tribunal Supremo 718/2020, de 28 de diciembre[46], declaró nula la prueba digital obtenida con la grabación de reuniones en un domicilio en las que se estaban diseñando estrategias de tráfico de drogas a gran escala, afirmando en su Fundamento Jurídico Segundo que la colocación de micrófonos en el domicilio "desborda con creces aquello que pueda resultar de interés para el delito investigado". En este caso, se consideró que existía no solo vulneración del derecho a la intimidad, sino a la inviolabilidad domiciliaria, considerando que "no se trata de una prueba más", sino que el grado de injerencia en la privacidad de quien cierra la puerta de su domicilio es tan grande no solo para el

[44] ECLI:ES:TS:2015:5087 y ECLI:ES:TS:2019:3232, respectivamente.

[45] En relación con las grabaciones de conversaciones mantenidas en vehículos, la Sentencia del Tribunal Constitucional 99/2021, de 10 de mayo, desestima el amparo por considerar que no existe vulneración a la intimidad de los investigados, realizando una interpretación extensiva de las medidas. Resulta de interés el comentario sobre esta Sentencia que efectúa RODRÍGUEZ LAINZ, 2021.

[46] ECLI: ES:TS:2020:4436.

investigado, sino para su familia, que el Estado debe ser muy cuidadoso porque "desnuda su propia vida familiar, lo coloca a merced de los investigadores, que se convierten en privilegiados conocedores de una información generada en el día a día y que desborda con creces aquello que pueda resultar de interés para el delito investigado".

Asimismo, cuando se trata de un despacho profesional como despachos de abogados, asesores fiscales, o dependencias cerradas en las que existen varios profesionales trabajando en su actividad, el problema es que el contenido afecta a datos reservados de terceros, de clientes que son ajenos a la investigación, y de los que el profesional se convierte en custodio. Las Sentencias del Tribunal Supremo 974/2012, de 5 de diciembre, 508/2015, de 27 de julio o la 89/2022, de 4 de febrero[47], han indicado que, aunque un despacho profesional no tiene la consideración de domicilio, sí debe exigirse una especial cautela por la actividad que en ellos se desarrolla. Y en este sentido, el Tribunal Europeo de Derechos Humanos se pronunció sobre esta cuestión, entre otras, en la Sentencia de 20 de julio de 2021 (caso Zoltán Varga contra Eslovaquia) y de 16 de noviembre de 2021 (caso Särgava contra Estonia) en las que se estima conculcado el artículo 8 del Convenio Europeo y, en consecuencia, el derecho a la intimidad y privacidad. En la primera, por haber colocado de micrófono oculto por parte de servicios de inteligencia en el interior de apartamento usado no solo por la persona objeto de concreto seguimiento, sino por terceras personas. Y, en la segunda, porque se efectuó el registro en el despacho y domicilio de un abogado, y de sus dispositivos electrónicos, al existir indicios de que el Letrado estaba relacionado con una trama de blanqueo de capitales, pero en la resolución que establece la orden de registro emitida por el Juez de instrucción no contenía ninguna disposición para salvaguardar el material de terceros protegido por el secreto profesional.

También puede plantearse que las grabaciones se autoricen judicialmente de forma restrictiva para algo muy concreto y que, posteriormente, sin cumplir los presupuestos exigidos por esa resolución, sino excediéndose, se aproveche la instalación de los micrófonos para investigar cualquier actividad y grabar todas las reuniones, dejando los dispositivos siempre en modo grabación, lo que obviamente debe ser nulo, pues no puede considerarse equiparable a las intervenciones telefónicas, que están siempre activadas y lo que se produce es el expurgo de lo que no sirva como prueba.

En relación con el registro remoto de equipos y la intervención o vigilancia técnica monitorizada que sigan los agentes facultados judicialmente, como indica VELASCO NÚÑEZ, tiene mucho interés "para obtener información dinámica sobre los centros delictivos de actividad criminal organizada y grupal en que sea crucial saber la forma en que se comunican y conocer su tráfico de llamadas, y aquellas

[47] ECLI:ES:TS:2012:8701, ECLI:ES:TS:2015:3699 y ECLI:ES:TS:2022:441, respectivamente.

conductas individualizadas graves en que sea preciso conocer además de las comunicaciones realizadas a través de ordenador (correo-e, chats y foros, así como Webs que se visitan, intercambio de comunicaciones…) aspectos tan importantes como averiguar sus IPS, localizar exactamente sus contactos, y conocer las transferencias de datos y archivos de audio, vídeo, imagen y texto que realizan por Internet"[48]. Sin embargo, se trata de una actividad muy intrusiva que invade una de las formas más íntimas y actuales del desarrollo comunicativo humano y plantea muchos problemas en relación con el método a través del cual se efectuaría esa vigilancia (por ejemplo, la instalación de troyanos, es decir, el hacking legal), por lo que aunque no contamos, aún, con jurisprudencia que analice esta medida o su injerencia extrema en el derecho al secreto de las comunicaciones, debe realizarse de un modo excepcional y procurar que los requisitos exigidos de proporcionalidad y necesidad estén aún más motivados, si cabe[49].

Y también la vigilancia GPS (balizas en vehículos) o la geolocalización a través de los datos móviles que tiene la operadora de telefonía móvil constituye una intromisión en la intimidad. En relación con ello la Sentencia del Tribunal Europeo de Derechos Humanos de 8 de febrero de 2018 (asunto Ben Faiza contra Francia), contemplaba que la colación del receptor de GPS en el vehículo del investigado y el tratamiento de los datos así obtenidos conlleva injerencia en su vida privada que, aunque sea menos intrusiva en la intimidad que la interceptación de las conversaciones telefónicas, debe conllevar también todas las garantías. Y a este respecto la Sentencia del Tribunal Supremo 493/2022, de 20 de mayo anuló esta medida en un delito de robo porque el Auto era estereotipado y de motivación suficiente[50].

Finalmente, la figura del agente encubierto informático puede vulnerar también el secreto de las comunicaciones, pues cualquier dato obtenido podría anularse al entrar en canales cerrados de comunicación si se efectúa sin la preceptiva autorización judicial. En este sentido, según la Sentencia del Tribunal Supremo 277/2016, de 6 de abril[51] hay que diferenciar la prueba recogida por el funcionario de policía en un primer momento, en calidad de testigo, con los primeros contactos previos (que se limita a recabar indicios de que se está llevando a cabo una eventual actividad delictiva), que sería válida, de la que (una vez comprobado el medio comunicación y el hecho

[48] VELASCO NÚÑEZ, 2011, p. 1.

[49] En el momento de elaboración de este artículo se encuentra de actualidad, precisamente, la noticia de los supuestos espionajes mediante el denominado programa "Pegasus", a líderes independentistas catalanes por parte del CNI que, según se ha publicado, fueron autorizados por el Magistrado del Tribunal Supremo adscrito a ese organismo pero que, de no haber sido así, adolecerían de nulidad radical y supondría la comisión de un delito de descubrimiento y revelación de secretos del artículo 197.1 del Código Penal. Y, asimismo, sobre sistemas de vigilancia secreta, hay que destacar la Sentencia del Tribunal Europeo de Derechos Humanos de 11 de enero de 2022 (caso Ekimdzhiev y otros contra Bulgaria) en la que declaraban nulas las informaciones obtenidas con un sistema de vigilancia secreta y de retención y acceso a datos de comunicaciones, considerando que vulneraron el derecho al respeto a la vida privada y familiar de los investigados.

[50] ECLI: ES:TS:2022:1999.

[51] ECLI:ES:TS:2016:1546.

delictivo) se obtiene por el agente encubierto. En este último caso, el agente debe solicitar autorización judicial para mantenerse en el canal, intercambiar, vender o compartir contenidos ilícitos para seguir obteniendo pruebas de la investigación si no quiere arriesgarse a la declaración de ilicitud posterior[52].

La consecuencia de una prueba digital ilícita es la prohibición de ser valorada en juicio, tanto la prueba primaria como la secundaria que se obtuvo a partir de ella y, por ende, el Tribunal no deberá tenerlas en cuenta, haciendo una valoración del resto de pruebas para considerar si solo ellas son aptas para desvirtuar el derecho a la presunción de inocencia. Es la clásica teoría del fruto del árbol envenenado desarrollada por el Tribunal Supremo de los Estados Unidos en 1920 (caso Silverthorne Lumber Company contra Estados Unidos[53]), siendo utilizado el término "the fruit of the poisonous tree" por primera vez en la Sentencia de 1939 del caso Nardone contra Estados Unidos[54], para considerar inválida toda la información descubierta a partir de investigaciones que afectaban a derechos fundamentales[55].

2. *Infracción de la cadena de custodia en las evidencias digitales*

En informática, como se ha indicado, cualquier elemento es manipulable, directa o indirectamente, con intención o sin ella. Por ello, la cadena de custodia cobra una especial relevancia en el ámbito de la prueba digital, porque es un procedimiento fundamental que hay que establecer dentro del proceso de aseguramiento de la evidencia electrónica para preservar fielmente la información sobre la que después se realizará una pericia[56].

La cadena de custodia no garantiza su inalterabilidad, porque como señalan las Sentencias del Tribunal Supremo 587/2014, de 18 de julio y 656/2015, de 10 de noviembre[57], la cadena de custodia no es prueba en sí misma y la irregularidad en ella por no respetar las garantías del procedimiento no afecta a ningún derecho fundamental de forma directa, sino a la valoración de la prueba practicada sin las debidas garantías. Por ello, si la evidencia se considera prueba de cargo y no se ha garantizado la cadena de custodia se produce una infracción del derecho a la presunción de

[52] Sobre esta figura, vid. GÓMEZ SIERRA, 2020.

[53] En este caso, tras un registro, los agentes del Gobierno entraron en las oficinas de la empresa Silverthorne Lumber y detuvieron a sus principales directivos por la información proporcionada por los libros de contabilidad hallados e incautados en dicho registro. Posteriormente el directivo apeló y acogiéndose a la cuarta enmienda de la Constitución americana logró que el tribunal declarara ilegal todas las pruebas obtenidas por considerar que había existido allanamiento y la entrada en el registro había sido ilegal.

[54] En esta Sentencia, se condenó a una persona en base a la información obtenida de una conversación telefónica interceptada por funcionarios del Gobierno, siendo considerada ilegal dicha interceptación y, por tanto, toda la información obtenida a partir de ella.

[55] En extenso sobre esta cuestión, vid. MARTÍNEZ GARCÍA, 2003, pp. 63 a 75.

[56] La Sentencia del Tribunal Supremo 808/2012, de 24 de octubre (ECLI:ES:TS:2012:7370) establece, en relación a la cadena de custodia, que su finalidad es garantizar la exacta identidad de lo incautado y de lo analizado. Tiene por tanto un valor instrumental para garantizar que lo analizado fue lo mismo que lo recogido.

[57] ECLI:ES:TS:2014:3086 y ECLI:ES:TS:2015:4803.

inocencia y el derecho a un proceso con las debidas garantías. En ese caso, como indica MESTRE DELGADO, debe impugnarse el contenido y practicarse la oportuna prueba, como el interrogatorio de los agentes que han participado en las diversas fases de la custodia de esos instrumentos o vestigios del delito, o han realizado las periciales[58].

Igual que ocurre en relación con los métodos de obtención de las evidencias digitales, en relación con la cadena de custodia existe también un limbo legal, pues la Ley Procesal no determina las directrices del procedimiento de cadena de custodia y sus fases, a pesar de su importancia, por lo que ha sido la realidad policial y la jurisprudencia, con las resoluciones en las que se resolvían impugnaciones, la que ha ido creando unas normas no escritas y protocolos para garantizar la cadena de custodia[59].

Lo primero que debe velarse es porque la aportación de la evidencia sea de la forma más temprana posible para intentar garantizar la autenticidad, inalterabilidad e indemnidad de la prueba digital y que todas las tareas de traspaso y operaciones que se realicen sobre el material objeto de prueba desde que se incauta hasta la pericia permanezca sin modificar. A esto podríamos considerar que se refiere el tercer párrafo del artículo 482 de la Ley de Enjuiciamiento Criminal cuando afirma –aunque dentro de la práctica de la pericial- de que el Juez "adoptará las precauciones convenientes para evitar cualquier alteración en la materia de la diligencia pericial".

Cuando se incautan dispositivos informáticos en una entrada y registro, los investigadores, junto con el Letrado de la Administración de Justicia, tienen que reseñar en el Acta cada uno de los dispositivos incautados, mencionándose la marca, el modelo, capacidad de almacenamiento, número de serie, IMEI y contraseñas (en el caso de smartphones/tablets), color del dispositivo y cualquier información que permita que ese dispositivo se pueda identificar inequívocamente en cualquier momento. Después, cada uno de ellos (o varios en grupo) serán introducidos en un sobre o envase adecuado para su preservación, siendo precintados y anotados los datos del contenedor en el acta de entrada y registro, comenzando así la diligencia de cadena de custodia de los mismos por parte de los agentes del cuerpo policial responsables

[58] Vid. MESTRE DELGADO, 2015, p. 69.

[59] ESPÍN LÓPEZ, 2021, online, epígrafe 4, indica, junto con GUTIÉRREZ SANZ, 2016, p. 59, que resulta incomprensible que en la reforma operada en 2015 para introducir en la Ley de Enjuiciamiento Criminal las medidas de investigación tecnológica no se incorporaran estos protocolos sobre cadena de custodia. Sin perjuicio de ello, cabe la esperanza de que sea introduzca finalmente, pues así figura en el Anteproyecto de la Ley de Enjuiciamiento Criminal de 2020, artículos 444 a 447, en los que se hace referencia a las garantías de las fuentes de prueba, la cadena de custodia, el procedimiento de gestión de muestras y los efectos de la cadena de custodia, concretando ESPÍN LÓPEZ, mismo epígrafe 4, que "debería incluirse la creación de un organismo adecuado con la finalidad de auxiliar a los tribunales en las funciones jurisdiccionales de recogida, depósito y preservación de los equipos electrónicos y la prueba digital, como sería un Instituto de Informática Forense que se encontraría servido por un cuerpo de informáticos forenses, teniendo en cuenta principalmente que, aun cuando la prueba digital no tenga menos importancia que cualquier pieza de convicción que no se encuentre bajo la impronta de las TIC, existe un peligro de pérdida de la misma que no puede predicarse de otros efectos relacionados el delito".

del registro[60]. Es más, en las evidencias digitales, para evitar el borrado en remoto deben utilizarse las bolsas o jaulas de Farady, que son diseñadas especialmente para que formen un blindaje sobre los dispositivos inalámbricos dejándolos sin ningún acceso a la red y bloqueando las señales wifi para evitar que se pueda borrar en remoto la información que contienen.

Y después de la incautación debe hacerse el clonado de dispositivos (por investigadores policiales o privados –en cuyo caso se debe realizar ante Notario-) siendo el uso de hashes criptográficos en los procesos forenses de copia de información, esencial para garantizar la cadena custodia y garantizar que ésta no ha sido alterada[61].

En este sentido, la Sentencia del Tribunal Constitucional 170/2003, de 29 de septiembre, precisamente anuló la prueba digital incorporada al proceso por considerar que no se garantizaba la cadena de custodia en un supuesto en el que los soportes informáticos no sólo no fueron identificados para determinar el domicilio en el que fueron intervenidos, sino que tampoco se procedió a su correcto sellado y precintando, aparte de que existía una significativa discordancia numérica entre ellos[62]. Debe tenerse, por tanto, exquisito cuidado en la custodia policial y control judicial del material intervenido sobre el que, posteriormente, se va a realizar la pericia, a los efectos de que no pueda existir duda sobre si la pericia se ha efectuado sobre los mismos soportes intervenidos o si éstos hubieran podido ser manipulados en cuanto a su contenido, porque el mero cambio de lugar de las evidencias, la falta de visibilidad de los sellos del Juzgado en los sobres o la presentación, un clonado de un archivo informático o un dispositivo requisado sin el hash, o cualquier conexión en remoto a un dispositivo incautado, implica una ruptura de la cadena de custodia que invalida la evidencia.

Pero también si se trata de volcado de información de los servidores, registro remoto de equipos o, incluso, de agente encubierto informático, deben tomarse en consideración los protocolos para asegurar la cadena de custodia, teniendo que entregar en el primer caso, la compañía en la que están alojados los contenidos (ya sean comunicaciones como correos electrónicos, webs, comentarios en redes sociales o cualquier contenido obrante en el ciberespacio) una copia a una fecha determinada certificando la integridad de esa información. Y en el registro remoto o agente encubierto, identificarse todos los pasos que se llevan a cabo y plasmarlos en el correspondiente informe pericial para asegurar la integridad de la información.

Otro problema que puede plantearse dentro de la cadena de custodia, al que en

[60] Vid., sobre cadena de custodia, DEL POZO PÉREZ, 2014 y FIGUEROA NAVARRO, 2011.

[61] Por este motivo, es inútil la asistencia de los Letrados a las eternas diligencias de clonado en el Juzgado, como ya se pronunció el Tribunal Supremo en la Sentencia 256/2008, de 14 de mayo (ECLI:ES:TS:2008:2809), pues el número hash asegura la garantía de originalidad, con independencia de las personas que asistan a la diligencia.

[62] En semejantes términos se pronunciaron, también, la Sentencia de la Audiencia Provincial de Pontevedra 28/2009, de 18 de junio (ECLI:ES:APPO:2009:1583) y la de la Audiencia Provincial de Cuenca 108/2010, de 16 de noviembre (ECLI:ES:APCU:2010:449).

cierta medida me he referido al hablar de la manipulación de las evidencias, es la garantía de la cadena de custodia respecto de la información obtenida en las conversaciones telefónicas o las comunicaciones orales intervenidas, en las que, sin perjuicio de la posibilidad de alteración informática a través de procesos complejos de las evidencias, lo que está claro es que la cadena de custodia se debe garantizar con el proceso a través del cual queda reflejado el día y hora en que se llevaron a cabo, los sistemas de grabación empleados, el terminal y los interlocutores y su constancia a través del oportuno proceso pericial técnico-informático.

Finalmente, en cuanto al momento para impugnar la cadena de custodia, la irregularidad debe denunciarse desde que tenga conocimiento la parte a quien afecte y, en cualquier caso, hasta el acto del Juicio Oral ya sea en fase de cuestiones previas o durante los interrogatorios practicados a los encargados de garantizarla, siempre antes de la fase de informe para evitar indefensión a las demás partes. Y si bien la prueba de la alteración de la cadena de custodia resulta a veces inviable, es evidente que corresponde a quien la ponga en duda, que debe argumentarlo de forma suficiente y fundada, sin que se limite a una impugnación genérica, de tal modo que el Tribunal quede obligado a dar una respuesta motivada.

IV. **Errores en la valoración de las pruebas digitales por parte de los tribunales de justicia**

Aunque va aumentando el conocimiento judicial de las pruebas digitales y su admisión, validez y eficacia, en atención a las características que deben cumplirse y las fases por las que tiene que pasar hasta adquirir fuerza probatoria e incidencia en la culpabilidad, siguen cometiéndose ciertos errores en los Tribunales por la propia obsolescencia del sistema judicial español y los medios al alcance de la Administración de Justicia, que todavía está un paso por detrás del avance tecnológico.

Pese a los requisitos tan exhaustivos que deben mantenerse para garantizar la integridad de la prueba, es incomprensible que no se aporte el documento de cadena de custodia de la prueba digital junto al informe que se efectúe, cuando se trata de periciales de la Policía Judicial, lo que sería imprescindible por la facilidad de que la prueba digital sea manipulada, como antes he indicado. En muchos casos sólo se examina el precintado de los sobres que contienen los dispositivos informáticos físicos, pero no de su contenido, que puede ser alterado en remoto sin romper esos precintos físicos. Nuestros Tribunales, por el contrario, siguen confiando en el examen y análisis de las evidencias que se efectúa por los cuerpos y fuerzas de seguridad del Estado, y no suele dudarse del testimonio de un agente que acude como perito (o testigo-perito) en el Juicio, a pesar de que no goza de presunción de veracidad, sino que constituye una prueba más, eximiéndole del deber de acreditar origen, autenticidad e integridad de las pruebas digitales incautadas y del proceso que ha llevado a

cabo en la obtención y análisis, a pesar de que, en muchas ocasiones se pregunta de forma insistente por los Letrados, incluso cuando existen informes periciales contradictorios de parte (a los que, por el contrario, sí se les exige un deber de acreditar esos extremos), que en ocasiones tienen mayor cualificación técnica que la Policía Judicial.

Esto plantea una especial problemática porque a la hora de proceder a la valoración judicial de la prueba digital, y conforme a las reglas del principio de libre y conjunta valoración de la prueba que haya sido practicada en juicio oral, público y contradictorio, la especialidad y características intrínsecas que tienen las pruebas digitales hace que deban aplicarse unas particulares reglas de la sana crítica y que nos encontremos con alteraciones. Es evidente que el Juez o Tribunal no dispone de conocimientos técnicos suficientes[63], con todas las eventualidades que pueden producirse y sus particularidades, por lo que debe estar exclusivamente supeditada la conclusión que obtenga el Tribunal a la valoración técnica aportada en juicio, bien por los peritos informáticos de parte, bien por los de la Policía Judicial, o, en caso de que no se considere necesario o no se efectúe una pericial, por los agentes de Policía que han llevado a cabo las investigaciones tecnológicas, lo que implica, en la práctica, una desviación de la valoración judicial de la prueba electrónica hacia profesionales que carecen de las garantías jurídicas, lo que no debería producirse, en aras al derecho de defensa y a la tutela judicial efectiva.

Es decir, la prueba electrónica aportada debe analizarse, como cualquier medio probatorio ordinario o convencional, bajo los principios de oralidad, contradicción, concentración, publicidad e inmediación, y el sistema de valoración aplicable a la prueba electrónica, como regla general, es de acuerdo a las máximas de experiencia y conforme a las reglas de la sana crítica junto con el restante material probatorio, que debe realizarse de un modo objetivo y sin que tengan cabida los métodos puramente intuitivos o derivados de la conclusión policial o pericial simplemente porque, como afirma la Sentencia del Tribunal Supremo 293/2020, de 10 de junio[64], "lo contrario supondría alejar el proceso penal y las técnicas de valoración probatoria de su verdadero fundamento racional" (Fundamento Jurídico Primero). Y ello sin que la libre valoración de las pruebas implique arbitrariedad, pues los Tribunales deben exteriorizar en la Sentencia, con fundamentos jurídicos, el proceso para llegar al convencimiento expresado como soporte de la decisión adoptada, debiendo ser conforme a las reglas de la lógica y experiencia, aunque hagan referencia a los conocimientos científicos contenidos en los informes periciales que hubieren podido practicarse en el Juicio. De esta forma, como afirma VELASCO NÚÑEZ, se aleja el papel del Juez

[63] BUENO DE LA MATA, 2014, p. 262, indica que el baremo valorativo del juzgador sobre esta prueba es reducido por estar supeditado a los peritos informáticos. En contra de esa idea, ARRABAL PLATERO, 2019, p. 416, afirma que "las máximas de la experiencia permiten a los Jueces realizar un razonamiento sensato sobre el conjunto de la prueba practicada, con independencia de su naturaleza técnica".

[64] ECLI:ES:TS:2020:1720.

"del mero automatismo, obligándole a adoptar siempre una posición crítica, aun cuando las pericias tengan mucho peso en ocasiones por su valor de convicción, en bastantes ocasiones en consonancia con el carácter científico y cuasiaxiomático de las mismas"[65].

Es esencial, por tanto, para garantizar el derecho de defensa, la apreciación conjunta de la prueba, no solamente de la digital, sino de otras que la complementen y el juicio de valor conjunto del material probatorio existente[66], sin basarse en la pericial informática exclusivamente[67], a pesar de la importancia que tiene, o en el resultado de las diligencias tecnológicas, dándole a estas el mismo valor que el resto de pruebas y, ante posibles contradicciones, que sean resueltas por el Juez a través de un motivado proceso intelectual expuesto en la Sentencia, para condenar o declarar una absolución.

V. **Conclusiones**

La prueba electrónica o digital en el proceso penal, en el que más fuertemente se despliegan las garantías constitucionales y los principios de legalidad, culpabilidad y presunción de inocencia, posee menos certezas de las que aparentemente pensamos. Y esto incide, directamente, en el fundamento del derecho a castigar del Estado. Es una prueba frágil, que puede modificarse o desaparecer con relativa facilidad sin dejar rastro aparente que la detecte, siendo en la actualidad la más sospechosa de ilicitud o ineficacia, pues es fácilmente manipulable o modificable. La falta de cobertura legal específica que determine en el proceso penal la incorporación de la evidencia digital como medio de prueba, hace que estemos ante una prueba con enormes problemas en su admisión y valoración y con muchas posibilidades de impugnación, al no disponer de un régimen de adopción de cautelas y precauciones específicas para su obtención, creación, conservación e incorporación al proceso penal, lo que incide, directamente, en la aplicación de la norma penal y la determinación de la culpabilidad del autor. Por ello, resulta necesaria una regulación específica de las pruebas digitales ya que poseen características muy particulares, a fin de dotarlas de un mayor grado de seguridad jurídica en el ejercicio del ius puniendi del Estado.

Mientras tanto y hasta que se promueva una regulación especial, resultan de apli-

[65] Vid. VELASCO NÚÑEZ, 2021, p. 676.

[66] Vid. DELGADO MARTÍN, 2018, p.87.

[67] En todo caso, como criterios valorativos de la pericial informática se tendrá en cuenta por parte del Tribunal la cualificación del perito y su concreta especialización, la metodología aplicada, la vinculación del perito con las partes y sus posibles implicaciones en la imparcialidad del mismo, la acreditación del cumplimiento de la cadena de custodia en la obtención y conservación de los datos y el contenido del propio informe técnico, teniendo en cuenta su coherencia interna, si incurre en contradicciones, si justifica sus conclusiones, si cuenta con omisiones manifiestas, si es congruente con las peticiones que le fueron formuladas, y si es inteligible.

cación las normas referidas a los medios probatorios procesales actualmente reflejados en la legislación procesal y por mucho que la prueba digital vaya a ser valorada por los Tribunales junto con el resto de elementos probatorios (de modo que no deben olvidarse los demás medios de prueba que existen en Derecho para desvirtuar una impugnación sobre la veracidad de una fuente tecnológica, como puede ser cualquier testifical de la persona que haya tenido conocimiento de los hechos contenidos en esos elementos digitales, que será valorada como las demás pruebas), solamente tendrá eficacia en cuanto a su originalidad y garantía de autenticidad cuando se incorpora al proceso mediante una prueba pericial informática - tanto en pruebas de parte como en diligencias derivadas de investigaciones policiales-, pues es la única que puede acreditar con visos de seguridad y fiabilidad la información los datos que puedan estar almacenados en cualquier tipo de soporte o evidencia digital. No acudir a ella puede suponer la impugnación del contenido de la evidencia y del documento o soporte que la contiene en una fase de Juicio Oral en la que ya impide a la acusación reaccionar. Por ello, la fase de preparación y presentación de la prueba puede marcar definitivamente el éxito o fracaso en un proceso judicial.

Asimismo, con el estado actual de la técnica y la gran cantidad de herramientas que permiten la manipulación de las evidencias digitales para ser incorporadas al proceso, los Tribunales no pueden otorgar garantía, eficacia y presunción de veracidad inmediata al contenido que se refleja por la Policía Judicial en los atestados, Oficios o informes en los que se analiza el resultado de las diligencias de investigación tecnológicas, pues debe garantizarse su integridad y originalidad a través de un proceso pericial informático para que se respeten los principios penales básicos. Si no se hace así, la prueba no sería eficaz para desvirtuar el derecho a la presunción de inocencia, lo que afectaría, por ende, a la culpabilidad del sujeto acusado y a la aplicación de la norma penal con todas las garantías.

A ello se añaden los problemas que existen en la obtención de la prueba digital que se incorpora al proceso con vulneración de los derechos fundamentales y notable desproporción entre el tipo penal y la sanción prevista, como son, esencialmente, la intimidad y el secreto de las comunicaciones. Debe tenerse especial cuidado en la aportación al proceso de pruebas digitales por particulares; y, a su vez, en las investigaciones con medidas tecnológicas, la Policía Judicial debe extremar las precauciones en exigir, siempre, y ante la duda, la oportuna autorización judicial que sea especialmente motivada y proporcionada con argumentos específicos del caso que se está investigando, dada la facilidad con la que, en una investigación, puede producirse una intromisión ilegítima en la privacidad del investigado o terceros con motivaciones generales e inconcretas que sirven para cualquier investigación. En este proceso es esencial, además, incorporar al procedimiento penal, para la validez de la prueba, la cadena de custodia acreditada de las evidencias digitales.

Finalmente, para que se cumplan los límites penales y se aprecie un respecto a los

principios de legalidad, culpabilidad y proporcionalidad los operadores jurídicos debemos exigir que la valoración de la prueba digital en el proceso penal se aparte del mero automatismo o plasmación de las conclusiones de una prueba pericial o de una investigación tecnológica policial, pues la Sentencia debe adoptar, siempre, una posición crítica y el planteamiento de la duda antes de dar por válidas, sin más, las conclusiones que vienen plasmadas en un informe y considerarlas aptas para enervar el derecho a la presunción de inocencia del acusado. La sociedad digital demanda, cada vez más, soluciones y mediaciones a problemas judiciales en escenarios tecnológicos o digitales y debemos disponer de mecanismos certificados que ayuden a avanzar en este nuevo escenario delictivo cibernético que cada año se incrementa a pasos agigantados.

Bibliografía

ABAD, N. (2022), "Los 12 indicios que acorralan a Óscar, el sospechoso de la muerte de Esther López", en el diario digital *El Confidencial*, 21 de abril de 2022 actualizado el 27 de abril de 2022. Disponible en: bit.ly/36Xeiho (fecha de última consulta: 29 de abril de 2022).

ALCÁCER GUIRAO, R. (2021), "Algunas dudas sobre la duda razonable. Prueba de descargo, estándares de prueba e in dubio pro reo", en *Revista electrónica de ciencia penal y criminología*, nº 23, p. 2. Disponible en http://criminet.ugr.es/recpc/23/recpc23-09.pdf (fecha de última consulta: 24 de abril de 2022).

ARMENTA DEU, T. (2018), "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre", en *IDP, Revista de Internet, Derecho y Política*, nº 27, septiembre 2018.

ARRABAL PLATERO, P. (2019), *La prueba tecnológica. Aportación, práctica y valoración,* Valencia.

BUENO DE LA MATA, F. (2014), *Prueba Electrónica y Proceso 2.0*, Valencia.

CABEZUDO RODRÍGUEZ, N. (2016) "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", *Boletín del Ministerio de Justicia*, año LXX, nº 2186, febrero de 2016, pp. 7 a 60.

DEL POZO PÉREZ, M. (2014), *Diligencias de investigación y cadena de custodia*, Madrid.

DELGADO MARTÍN, J. (2015), "La prueba del whatsapp", *Diario La Ley*, nº 8605, Sección Tribuna, 15 de septiembre de 2015.

DELGADO MARTÍN, J. (2017), "La prueba digital. Concepto, clases y aportación al proceso", *Diario La Ley*, nº 6, Sección Ciberderecho, 11 de abril de 2017.

DELGADO MARTÍN, J. (2018), *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª edición, Madrid.

DELGADO MARTÍN, J. (2022), "Problemas actuales de la práctica y valoración de la prueba digital. Y un epílogo para abogados", *Diario La Ley*, nº 57, Sección Ciberderecho, 5 de enero de 2022.

ESPÍN LÓPEZ, I. (2021), "La cadena de custodia en el proceso penal. Propuestas en relación con el análisis y custodia de la prueba digital", *La Ley Penal*, nº 151, Julio-Agosto 2021.

FIGUEROA NAVARRO, C. (2011), "El aseguramiento de las pruebas y la cadena de custodia", en *La Ley Penal,* nº 84.
GARCÍA MESCUA, D. (2018), *Aportación de mensajes de WhatsApp a los procesos judiciales. Tratamiento procesal.* Albolote, 2018.
GÓMEZ SIERRA, P. L. (2020), "Infiltrados en el ciberespacio. Agente encubierto online", en *La Ley privacidad*, nº 6, Sección Ciberseguridad, Cuarto trimestre de 2020.
GUTIÉRREZ SANZ, M. R. (2016), *La cadena de custodia en el proceso penal español*, Cizur Menor (Navarra).
MAGRO SERVET, V. (2020), "Casuística práctica de la prueba digital en el proceso civil y penal", *Actualidad Civil*, nº 1, enero 2020.
MAGRO SERVET, V. (2021), en "¿Cómo aportar la prueba digital en el proceso penal?", *Diario La Ley*, nº 9824, 7 de abril de 2021.
MARTÍNEZ GALINDO, G. (2021), "La prueba pericial informática y tecnológica", en SANZ DELGADO/FERNÁNDEZ BERMEJO, (coords.): *Tratado de Delincuencia Cibernética*, Cizur Menor, pp. 741 a 771.
MARTÍNEZ GARCÍA, E. (2003), *Eficacia de la prueba ilícita en el proceso penal*, Valencia.
MESTRE DELGADO, E. (2015), "La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos", en Figueroa Navarro (dir.): *La cadena de custodia en el proceso penal*, Madrid, pp. 39 a 79.
RODRÍGUEZ LAINZ, J.L. (2015), "Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (A propósito de la STS, Sala 2.ª, 300/2015, de 19 de mayo)", en *Diario La Ley*, nº 8569, Sección Doctrina, 25 de junio de 2015.
RODRÍGUEZ LAINZ, J.L. (2021), "La interceptación de comunicaciones orales en la STC 99/2021 (Análisis crítico)", *Diario La Ley* nº 9956, de 19 de noviembre de 2021.
RUBIO ALAMILLO, J. (2016), "El correo electrónico como prueba en procedimientos judiciales", *Diario la Ley*, nº 8808, Sección Práctica Forense, 21 de julio de 2016.
SÁNCHEZ GONZÁLEZ, S. (2022), "Investigar y castigar la pornografía infantil gracias al agente encubierto informático", *La Ley Penal*, nº 154, enero-febrero 2022.
PINTO PALACIOS, F./PUYOL CAPILLA, P. (2017), *La prueba en la era digital*, Madrid.
VELASCO NÚÑEZ, E. (2011), "ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal", *La Ley Penal*, nº 82.
VELASCO NÚÑEZ, E. (2021), *Delitos tecnológicos*, Madrid.