UNIVERSIDAD MIGUEL HERNÁNDEZ

Facultad de ciencias sociales y jurídicas de Elche

GRADO EN SEGURIDAD PÚBLICA Y PRIVADA

Trabajo fin de grado

LAS PRUEBAS TECNOLÓGICAS EN EL PROCESO

ILICITUD PROBATORIA Y AFECTACIÓN A LOS DERECHOS FUNDAMENTALES

AUTOR

Sergio Arreal Burgos

TUTORA

Profa. Dra. Olga Fuentes Soriano

Catedrática de Derecho Procesal

CURSO ACADÉMICO

2024-2025

Biblioteca
UNIVERSITAS Miguel Hernández

ÍNDICE DE CONTENIDOS

RESUMEN

El presente Trabajo de Fin de Grado tiene por objeto el estudio de las pruebas tecnológicas en el ámbito del proceso penal, en el que se analiza desde una perspectiva garantista su configuración como elemento probatorio y la ilicitud de dichas pruebas derivada de la posible afectación a derechos fundamentales durante su obtención. Este examen se estructura en los dos grandes bloques que se detallan a continuación.

El primer bloque se centra en el concepto y características de las pruebas tecnológicas, las cuales presentan una serie de rasgos distintivos que las diferencian sustancialmente de las acuñadas como tradicionales. Asimismo, se examinan las fuentes más comunes presentadas los particulares ante los Tribunales, consideradas como tal por su presencia creciente en los procesos judiciales actuales.

El segundo bloque analiza las pruebas tecnológicas ilícitas o prohibidas, es decir, aquellas obtenidas con vulneración de derechos fundamentales, en especial aquellos derechos reconocidos en el artículo 18 de la Constitución Española. En este sentido, se tratan las teorías que justifican su exclusión o no del proceso penal, y paralelamente, se estudian los derechos fundamentales susceptibles de afectación durante la obtención de estas pruebas tecnológicas, como son los recogidos en el mencionado artículo 18 de la Carta Magna.

El trabajo pretende tratar los criterios que permiten armonizar la eficacia de la investigación penal con el respeto a las garantías constitucionales, esto es, a los derechos fundamentales sustantivos. Para ello se determina en qué casos la ilicitud en la obtención de la prueba tecnológica debe conllevar su exclusión del proceso, a fin de garantizar el derecho a la tutela judicial efectiva y a un proceso con todas las garantías, ambos recogidos en el artículo 24 de la Constitución Española.

Palabras clave

Pruebas tecnológicas, prueba ilícita, vulneración derechos fundamentales

ABSTRACT

The purpose of this Final Degree Project is to study technological evidence in criminal proceedings, analyzing its use as evidence from a guarantee-based perspective, as well as the illegality of such evidence due to the potential violation of fundamental rights during its collection. This project is structured into the two main sections detailed below.

The first section focuses on the concept and characteristics of technological evidence, which presents a series of distinctive features that substantially differentiate it from traditional evidence. It also examines the most common sources presented by individuals before the courts, considered as such due to their increasing presence in current judicial proceedings.

The second section analyzes illegal or prohibited technological evidence, that is, evidence obtained in violation of fundamental rights, especially those recognized in Article 18 of the Spanish Constitution. In this regard, the theories justifying its exclusion or exclusion from criminal proceedings are discussed, and at the same time, the fundamental rights that may be affected during the collection of this technological evidence are studied, such as those set forth in the aforementioned Article 18 of the Constitution.

This paper aims to address the criteria that allow for harmonizing the effectiveness of criminal investigations with respect for constitutional guarantees, that is, substantive fundamental rights. To this end, it determines in which cases the illegality of obtaining technological evidence should lead to its exclusion from the proceedings, in order to guarantee the right to effective judicial protection and a trial with full guarantees, both enshrined in Article 24 of the Spanish Constitution.

Keywords

Digital evidence, unlawful evidence, violation of fundamental rights

ABREVIATURAS

ART./ARTS.	Artículo/Artículos
ATS	Auto del Tribunal Supremo
BOE	Boletín Oficial del Estado
CDFUE	Carta de los Derechos Fundamentales de la UE
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CP	Código Penal
DUDH	Declaración Universal de los Derechos Humanos
E2EE	*End-to-End Encryption* (cifrado de extremo a extremo)
FFCCS	Fuerzas y Cuerpos de Seguridad
FGE	Fiscalía General del Estado
IP	Internet Protocol (Protocolo de Internet)
LAJ	Letrado de la Administración de Justicia
LEC	Ley de Enjuiciamiento Civil
LECrim	Ley de Enjuiciamiento Criminal
LFE	Ley de Firma Electrónica
LO	Ley Orgánica
LOHIP	Ley Orgánica de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen
LSEC	Ley de Servicios Electrónicos de Confianza
Op. Cit.	Obra citada
P./PP.	Página/Páginas
RAE	Real Academia Española
RGPD	Reglamento General de Protección de Datos
SAP	Sentencia de la Audiencia Provincial
SITEL	Sistema Integrado de Interceptación Telefónica
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
TIC	Tecnologías de la Información y Comunicación
TC	Tribunal Constitucional
TS	Tribunal Supremo

1. Introducción

Es una obviedad afirmar que la era digital ha cambiado por completo la forma en que los ciudadanos interactúan con su entorno, ya que han incorporado el uso de las nuevas tecnologías a prácticamente todas las facetas de su vida cotidiana. Este fenómeno no puede orientarse meramente al uso de las herramientas tecnológicas, sino que también ha supuesto una transformación conductual del ser humano, donde dispositivos como smartphones, tablets y ordenadores se han convertido en una extensión de nuestra identidad. Esta mutación del comportamiento se ha manifestado en actividades diarias tan básicas como las transacciones online, las relaciones sociales, el intercambio de información en plataformas digitales, las comunicaciones laborales a través de mensajería instantánea o correo electrónico, el envío de archivos multimedia e incluso la captación de imágenes o vídeos de conductas ajenas. En definitiva, el mundo digital se ha convertido en un espacio donde hoy en día se desarrollan actividades que antes tenían lugar exclusivamente en el plano físico.

Este mundo digital, si bien es cierto que ha aportado innegables ventajas en el desarrollo de nuestro quehacer diario, también hay que reconocer que ha generado nuevos riesgos jurídico-penales en gran medida desconocidos para buena parte de la sociedad. La facilidad con la que se generan, almacenan y comparten datos digitales ha creado un nuevo escenario en el que las fronteras entre lo lícito y lo ilícito se difuminan con frecuencia, incluso para usuarios que, sin intención delictiva alguna, realizan ciertas actividades ilícitas ignorando sus posibles consecuencias penales. Al mismo tiempo, este problema se ha visto agravado con el auge de la ciberdelincuencia, donde hechos delictivos como el phishing, el ransomware o el robo de identidad han evidenciado cómo los delitos tradicionales han evolucionado al entorno digital, multiplicando exponencialmente el número víctimas potenciales, especialmente para aquellas más vulnerables por su falta de conocimientos básicos sobre estos delitos.

Paralelamente, encontramos a aquellos ciudadanos que, en su condición de víctimas o incluso testigos, pueden incurrir en irregularidades durante la obtención de pruebas digitales. Se trata de aquellos casos en los que particulares, al intentar acreditar un hecho presuntamente delictivo, recaban evidencias mediante propias grabaciones, capturas de pantalla o accesos no autorizados a dispositivos electrónicos, no reparan en que estas actuaciones

pueden vulnerar derechos fundamentales protegidos constitucionalmente como la intimidad, el secreto de las comunicaciones o la protección de datos. El resultado de ello es que, al presentar dichas pruebas ante el órgano judicial competente, existe una alta probabilidad de ser declaradas ilícitas y, en consecuencia, excluidas del proceso, dejando en desamparo a las posibles víctimas. Esta problemática refleja la existencia de un profundo desconocimiento sobre los límites legales durante la obtención y uso de pruebas digitales, así como sobre las garantías que protegen a los ciudadanos frente a intromisiones arbitrarias en su esfera privada.

Ante este panorama, el presente Trabajo de Fin de Grado tiene como objetivo situar al lector ante una realidad que, pese a su creciente relevancia, sigue siendo en gran medida desconocida para el público general. A través de un análisis riguroso del marco jurídico-penal, se busca destacar la importancia de promover un conocimiento más amplio y accesible sobre las pruebas tecnológicas, así como las consecuencias derivadas del uso indebido de las nuevas tecnologías. La ilicitud de estas pruebas no solo afecta a la eficacia de la investigación penal, sino que también plantea serios interrogantes sobre cómo conciliar la necesidad de combatir la criminalidad con el respeto irrenunciable a los derechos fundamentales sustantivos. Solo así será posible preservar tanto la seguridad jurídica como la integridad del sistema de justicia en un contexto cada vez más digitalizado.

2. Las pruebas tecnológicas

En la actualidad, las pruebas tecnológicas se han convertido en elementos esenciales en un elevado número de procesos judiciales, llegando incluso a constituir en mucho de ellos la base probatoria fundamental del caso al haberse desarrollado el ilícito penal únicamente en el espacio digital, lo que justifica y motiva el desarrollo del presente estudio.

Partiendo de la base de que el desarrollo tecnológico ha transformado los elementos de prueba en el ámbito jurídico, cabe señalar que las pruebas digitales, entendidas como aquellos elementos probatorios creados o contenidos en soportes electrónicos que contienen información relevante para determinar hechos ilícitos en un proceso judicial, presentan una serie de características singulares que las diferencian de las pruebas tradicionales.

Debido a su peculiar naturaleza, se analizará su definición desde distintos enfoques doctrinales, destacando según OLIVA LEÓN su inmaterialidad por su formato digital y naturaleza binaria, su facilidad de alteración, su capacidad de reproducción ilimitada y la necesidad de utilizar instrumentos técnicos para su interpretación[1]. Por todo esto el autor se centra en la importancia de la cadena de custodia de dichas pruebas tecnológicas, afirmando que deberán establecerse *protocolos legislados que determinen un proceso tasado acerca de cómo se debe proceder a la ejecución de esa captación de prueba electrónica y esa conservación hasta su enjuiciamiento*[2].

Asimismo, se analizarán las principales fuentes de prueba tecnológicas que, como señala FUENTES SORIANO, pueden investigarse *utilizando instrumentos comunes que la ciudadanía tiene al alcance de la mano*[3], permitiendo su aportación tanto por parte de particulares como del Estado. Las más relevantes son las comunicaciones digitales, como correos electrónicos, mensajes instantáneos e interacciones en redes sociales, junto con los archivos multimedia, como imágenes fotográficas y grabaciones videográficas digitales.

---

[1] OLIVA LEÓN, R., *La prueba electrónica, validez y eficacia procesal*, Editorial Juristas con futuro, 2016, pp. 45-138.

[2] OLIVA LEÓN, R., *La prueba electrónica…*, Op. Cit., p. 164.

[3] FUENTES SORIANO, O., *La prueba prohibida. Viejos problemas procesales de las nuevas tecnologías*. Capítulo de libro. En PRIORI POSADA. G. (Coord.), Justicia y proceso en el S. XXI. Desafíos y tareas pendientes, Ed. Palestra, Perú, 2019, p. 3.

En definitiva, el presente apartado tiene como objetivo aportar un análisis completo de dichas pruebas tecnológicas, abarcando desde su conceptualización hasta sus rasgos distintivos y formatos más frecuentemente utilizados en procesos judiciales iniciados por particulares. Y como advierte FUENTES SORIANO, la integración de las nuevas tecnologías en el quehacer diario ha dado lugar a un nuevo contexto en el que se han visto modificados sustancialmente los modos de relación social y jurídica, manifestándose particularmente a través de nuevas modalidades de afectación a los Derechos Fundamentales *hasta hace pocos años tan desconocidas como inimaginadas*[4].

2.1. Concepto y naturaleza jurídica

En la época que nos encontramos en la actualidad, propiamente conocida como la era digital o de la información [5], el desarrollo tecnológico ha experimentado un notable crecimiento y junto a éste el uso generalizado de las Tecnologías de la Información y la Comunicación, las cuales han transformado radicalmente las relaciones económicas, políticas y sociales [6]. Esta transformación ha generado de forma simultánea nuevas oportunidades para la comisión de ilícitos, o como afirma LÁZARO HERRERO, *los delincuentes han encontrado en los medios tecnológicos un firme aliado para la comisión de crímenes*, y en el que los *delitos tradicionales han aprovechado estos nuevos canales de comunicación, dando lugar a nuevas categorías delictivas*[7].

Esta evolución de los modelos de comunicación interpersonal y de las dinámicas delictivas contemporáneas ha permitido ampliar de forma exponencial tanto el número de delitos cometidos mediante el uso de las TIC como el de víctimas potenciales[8], las cuales han permitido sobrepasar fronteras físicas y jurídicas debido a la transnacionalidad del ciberespacio. Paralelamente, ha provocado una reconfiguración significativa de los modelos empresariales,

---

[4] FUENTES SORIANO, O., *La prueba prohibida…*, Op. Cit., p. 3.

[5] CASTELLS OLIVÁN, M., *La era de la información. Economía, sociedad y cultura* (Vol. 3), Alianza Editorial, 2001.

[6] MIRÓ-LLINARES, F., *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, 2012, p. 26.

[7] LÁZARO HERRERO, C., *Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad: Un proyecto europeo*, vol.5, Nº 2, 2008, p. 140.

[8] CUADRADO SALINAS, C., *Registro informático y prueba digital: estudio y análisis comparado de la ciberinvestigación criminal en Europa,* La Ley Penal, nº 107, 2014, p. 1.

trasladando su centro de negocio al mundo virtual[9], con los consiguientes riesgos de vulnerabilidad que esto conlleva.

La omnipresencia de dispositivos electrónicos en nuestra sociedad y la digitalización de sus actividades cotidianas se han manifestado en actos tan usuales como la filmación por particulares, con sus propios teléfonos móviles, de ilícitos acaecidos en espacios públicos, o de sistemas de videovigilancia públicos y privados. Asimismo, observamos la facilidad para cometer hechos delictivos tradicionales a través de las TIC, denominados por MIRÓ-LLINARES como cibercrímenes réplica [10], entre los que encontramos las amenazas o las ciberestafas como el phishing y la suplantación de identidad, entre otros. A esto se suma la aparición de nuevas modalidades delictivas digitales como el hacking, malware o la difusión ilícita de contenidos[11]. Este escenario ha generado que los registros digitales de delitos no solo puedan incorporarse al proceso judicial como soportes probatorios tecnológicos, sino incluso constituir el origen mismo de la acción penal, transformando así la naturaleza de la investigación criminal.

La revolución digital ha afectado a las pruebas tecnológicas de tal forma que ha hecho que adquieran una gran relevancia en el ámbito del derecho procesal penal, especialmente con la incorporación de las nuevas herramientas tecnológicas en los procesos judiciales que permiten obtener información digital precisa y detallada sobre diferentes tipos delictivos. Estas pruebas difieren significativamente de las fuentes de prueba tradicionales, por lo que resulta indudable que estas innovaciones tecnológicas requieren de un gran esfuerzo, particularmente en lo relativo a la preservación de las garantías procesales[12].

Previo al examen de las diversas definiciones sobre la prueba tecnológica, es conveniente especificar la diferencia entre las fuentes y los medios de prueba.

---

[9] PINTO PALACIOS, F., PUJOL CAPILLA, P., *La prueba en la era digital*, Wolters Kluwer, 2017, p. 19.

[10] MIRÓ-LLINARES, F., *El cibercrimen…*, Op. Cit., p. 68. El autor denomina cibercrímenes réplica a los ataques que ya se materializaban en el espacio físico y cuya comisión ahora se desarrollan en la Red, siendo este último *el nuevo medio a través del cual se comete una infracción que utilizaba anteriormente otros medios para llevarse a cabo*.

[11] MIRÓ-LLINARES, F., *El cibercrimen…*, Op, Cit., p. 52. El autor denomina cribercrímenes puros a *los únicos que podrían ser denominados como tales en el caso de que la condición de pertenencia fuera que solamente deben ser posibles en el ciberespacio. Y esto es así porque en ellos las TIC no sólo constituyen el medio comisivo de tales ataques, sino que son el único posible, en cuanto que son medio y objetivo, y no es posible producir la esencia de ilicitud de estas infracciones si no es en el ciberespacio.*

[12] SIGÜENZA LÓPEZ, J., *Proceso civil y nuevas tecnologías*, Thomson Reuters Aranzadi, Pamplona, 2021, pp. 22-24

Las primeras, las fuentes de prueba, si tenemos en cuenta la etimología de la palabra "fuente", proveniente del latín "*fontis*", "*fons*", se refiere a aquello que establece un punto de origen desde el que mana algo, quiere decir, principio, fundamento u origen de algo[13]. Y particularmente, las fuentes de prueba tecnológicas versan acerca de la información contenida o que ha sido transmitida a través de los medios electrónicos[14] que, *siendo ajena al proceso y teniendo por tanto carácter extrajurídico, se incorpora a éste con la finalidad de servir a la conformación de la convicción judicial*[15]. Asimismo, se puede añadir que son elementos que existen en la realidad sensible de forma previa y ajena al proceso[16] y que son, por definición, ilimitadas. Mientras que los segundos, los medios de prueba, se refieren a la forma a través de la cual dicha información entra al proceso con el fin de generar la certeza del juzgador[17], concretamente, las actividades necesarias para incorporar las fuentes de prueba a la causa. Éstas, a diferencia de las anteriores, son limitadas por el legislador[18] y, por tanto, sí que forman parte del proceso judicial. Estos medios se encuentran regulados por la LEC en su Capítulo VI, que versa sobre los medios de prueba y las presunciones, y concretamente en su art. 299 LEC, clasificados por PÉREZ PALACÍ[19] como medios tradicionales[20] en su apartado primero, y modernos en el segundo, los cuales se tratarán a continuación.

Tras realizar un análisis del marco normativo vigente sobre la prueba tecnológica, resulta oportuno señalar que en la LECrim no encontramos regulación expresa sobre la prueba electrónica. Ahora bien, si nos dirigimos a la

---

[13] Definición de "fuente" obtenida del Diccionario de la Lengua Española de la RAE, recuperado el 20 de abril de 2025 de https://dle.rae.es/fuente?m=form

[14] BANACLOCHE PALAO, J., *La prueba en el proceso penal*, Aspectos fundamentales del Derecho Procesal Penal, editorial La Ley (2.ª edición), Madrid, 2011, p. 273.

[15] FUENTES SORIANO, O., *La intervención de las comunicaciones tecnológicas tras la Reforma de 2015*, en *El nuevo proceso penal tras las reformas de 2015*, Atelier, 2016, p. 263.

[16] MENESES PACHECO, C., *Fuentes de prueba y medios de prueba en el proceso civil*, Revista *Ius et Praxis*, vol. 14, nº 2, 2008, p. 57.

[17] MONTERO AROCA, J., *La prueba en el proceso civil*, Thomson – Civitas (4ª edición), Navarra, 2005, pp. 133-137.

[18] ABEL LLUCH, X., RICHARD GONZÁLEZ, M., *Estudios sobre prueba penal*, Wolters Kluwer, Madrid, 2013.

[19] PÉREZ PALACÍ, J.E., *La prueba electrónica: consideraciones*, Universitat Oberta Catalunya, 2014, p. 3.

[20] Artículo 299, apartado primero, de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, publicada en el BOE núm. 7, de 8 de enero de 2000, dispone que " *Los medios de prueba de que se podrá hacer uso en juicio son el interrogatorio de las partes, los documentos públicos, los documentos privados, el dictamen de peritos, el reconocimiento judicial y el interrogatorio de testigos*", recuperado de https://www.boe.es/eli/es/l/2000/01/07/1/con

LEC, la cual será de aplicación supletoria[21], y más concretamente al citado art. 299.2 LEC, se cita textualmente que *se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido o la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevada a cabo con fines contable de otra clase, relevantes para el proceso*[22]. Por otra parte, dicho artículo refuerza el uso de cualquier otro medio de prueba futuro mediante un *numerus apertus* en su apartado tercero, reseñando que el Tribunal, a instancia de parte, podrá admitir como prueba cualquier otro medio que no haya sido expresamente previsto en la ley y del que se pudieran obtener certeza sobre hechos relevantes, siempre que se adopten las medidas pertinentes para garantizar su validez[23].

La anterior norma se ve complementada por la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza, ya que en su art. 3.1 LSEC sobre los efectos jurídicos de los documentos electrónicos, establece que los *documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable*[24].

En la Ley 59/2003 de firma electrónica, en su art. 3.5 LFE especifica que se considera documento electrónico *la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*[25].

En último lugar, en lo que respecta al documento se trata el Código Penal, y concretamente en su art. 26 CP se considera como tal todo *soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o*

[21] Artículo 4 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, sobre el carácter supletorio de la Ley de Enjuiciamiento Civil, dispone que "*En defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Le*y".

[22] Artículo 299, apartado segundo, de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

[23] Artículo 299, apartado tercero, de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

[24] Artículo 3, apartado primero, de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de Confianza, publicada en el BOE núm. 298, de 12 de noviembre de 2020, recuperado de https://www.boe.es/eli/es/l/2020/11/11/6/con

[25] Artículo 3, apartado quinto, de la Ley 59/2003, de 19 de diciembre, de firma electrónica, publicada en el BOE núm. 304, de 20 de diciembre de 2003, recuperado de https://www.boe.es/eli/es/l/2003/12/19/59/con

cualquier tipo de relevancia jurídica [26], sin hacer mención específica al documento electrónico o digital.

En cuanto a la doctrina, encontramos que la prueba, como manifiesta ROMÁN PUERTA, es la *actividad procesal que tiene por objeto conseguir la convicción del juzgador sobre la realidad de los hechos en que se fundamentan las pretensiones de las partes a las que aquél que debe dar una respuesta fundada en Derecho*[27]. Y, en concreto, la prueba tecnológica adquiere diferentes denominaciones por parte de la doctrina, entre los que encontramos el término prueba electrónica, comúnmente utilizado por ésta, se define como *perteneciente o que funciona mediante la electrónica* [28], y el cual ha sido adoptado como título por PÉREZ PALACÍ en una de sus publicaciones[29].

Otras de las locuciones utilizadas es la de prueba informática, definido como el *conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras* [30], enfocado especialmente a los delitos informáticos[31] como por ejemplo refiere DE URBANO CASTRILLO. También encontramos el uso de prueba digital, *dicho de un dispositivo o sistema que crea, presenta, transporta o almacena información mediante la combinación de bits*[32], nombrado de esta forma por DELGADO MARTÍN[33]. Y, por último, prueba tecnológica, el cual hace referencia a aquello perteneciente o relativo a la tecnología[34], utilizada por ARRABAL PLATERO[35] y

[26] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicada en el BOE núm. 281, de 24 de noviembre de 1995, recuperado de https://www.boe.es/eli/es/lo/1995/11/23/10/con

[27] ROMÁN PUERTA, L., *La prueba en el proceso penal*, Revista Aldaba, núm. 24, 1995, p. 47.

[28] Definición de "electrónica" obtenida del Diccionario de la Lengua Española de la RAE, recuperado el 20 de abril de 2025 de https://dle.rae.es/electr%C3%B3nico?m=form

[29] PÉREZ PALACÍ, J. E., *La prueba…*, Op. Cit., p. 1.

[30] Definición de "informática" obtenida del Diccionario de la Lengua Española de la RAE, recuperado el 20 de abril de 2025 de https://dle.rae.es/inform%C3%A1tico?m=form

[31] DE URBANO CASTRILLO, E., *Los delitos informáticos tras la reforma del CP de 2010*, en *Delincuencia informática: tiempos de cautela y amparo*, Thomson Reuters, Madrid, 2012.

[32] Definición de "digital" obtenida del Diccionario de la Lengua Española de la RAE, recuperado el 20 de abril de 2025 de https://dle.rae.es/digital?m=form

[33] DELGADO MARTÍN, J., *La prueba digital. Concepto, clases, aportación al proceso y valoración*, Diario La Ley, nº 6, Sección Ciberderecho, Wolters Kluwer, 2017.

[34] Definición de "tecnológica" obtenida del Diccionario de la Lengua Española de la RAE, recuperado el 20 de abril de 2025 de https://dle.rae.es/tecnol%C3%B3gico?m=form

[35] ARRABAL PLATERO, P. *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, 2020.

por la reforma procesal llevada a cabo *para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*[36].

Si se pretende adoptar una definición de carácter general para la prueba electrónica, podría entenderse ésta como *toda información con valor probatorio incluida o transmitida por un medio electrónico*[37], así como aquella que se refiere a *cualquier clase de información contenida dentro de medios electrónicos, capaz de acreditar hechos dentro de un proceso*[38].

Por el contrario, una definición con mayor precisión técnica correspondería a la formulada por BUENO DE MATA, el cual la identifica como *cualquier prueba presentada informáticamente,* y cuyo autor considera que se encuentra formada por dos elementos*,* el *hardware* y el *software.* El primero de ellos es material*,* es decir, *la parte física y visible de la prueba para cualquier usuario de a pie,* poniendo como ejemplos la carcasa de un Smartphone o de la memoria USB. El segundo es intangible o inmaterial, como *los metadatos y archivos electrónicos modulados a través de unas interfaces informáticas*[39].

Por su parte, CASEY ofrece otra definición técnica, pero orientada hacia un campo específico diferente, al señalar que las evidencias digitales son aquellos datos que se obtienen de dispositivos electrónicos y que, mediante técnicas forenses, pueden ser utilizados para reconstruir hechos o establecer vínculos entre delito y autor[40]. Estas técnicas permitirán garantizar la autenticidad, integridad e inalterabilidad de las pruebas.

Ahora bien, HERNÁNDEZ GIMÉNEZ ofrece una de las definiciones más esenciales sobre las pruebas tecnológicas al referirse a ellas como *toda información con valor probatorio incluida o transmitida por un medio*

---

[36] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, publicada en el BOE núm. 239, de 6 de octubre de 2015, pp. 90192-90219, recuperado de https://www.boe.es/eli/es/lo/2015/10/05/13

[37] HERNÁNDEZ GIMÉNEZ, M., *Inteligencia artificial y derecho penal*, Actualidad jurídica iberoamericana, 10, 2019, p. 813.

[38] MUÑOZ RODRÍGUEZ, A.B., *El impacto de la Inteligencia Artificial en el Proceso Penal*, Universidad de Extremadura, 36, 2020, pp. 695-728, recuperado de https://revista-afd.unex.es/index.php/AFD/article/view/489/572

[39] BUENO DE MATA, F., BUJOSA VADELL, L. M., *Prueba Electrónica y Proceso 2.0,* Tirant lo Blanch, 2014, p. 130.

[40] CASEY, E., *Digital evidence and computer crime* (3ª edición), Elsevier, 2011.

electrónico[41], adoptada por MEDINA MARTÍN, y quien subraya que éstas son incorporadas al proceso judicial como pruebas documentales. Este último autor realiza una precisión sobre dichas pruebas, y es que, aunque se generan y almacenan en medios electrónicos, su valor probatorio depende de su conversión a un formato admisible como son los correos electrónicos, mensajes, grabaciones o documentos digitales. Asimismo, añade que, para garantizar su fiabilidad sería esencial que se realizara un dictamen pericial informático que certifique su autenticidad, así como la ausencia de alteraciones[42].

Finalmente, ARRABAL PLATERO ofrece una definición basada en una característica distintiva de las pruebas tecnológicas al señalarlas como aquel archivo informático que contiene metadatos, los cuales define como *un grupo de datos ocultos que se almacenan en forma de ceros y unos que exigen de su transformación en información legible y que describen el contenido informativo de un elemento digital y que, por tanto, aportan información adicional al archivo en el que se encuentren*[43]. Es por lo que contendrán mucha más información que aquellas pruebas que no tengan relación alguna con las TIC.

2.2. Características

Las pruebas tecnológicas poseen una serie de características que las diferencian sustancialmente de los medios probatorios conocidos como tradicionales, particularidades que derivan de su propia naturaleza digital y que no solo influyen en su obtención y tratamiento, sino también en su valoración dentro del proceso judicial. En contraposición a la materialidad de las pruebas físicas, en multitud de ocasiones requerirán la intervención de conocimientos técnicos especializados para preservar y garantizar su autenticidad e integridad, lo que exige un tratamiento jurídico específico.

La doctrina ha abordado las particularidades de las pruebas tecnológicas desde perspectivas complementarias. En este sentido, la selección de los dos enfoques que se desarrollan en este apartado se justifica por su capacidad para articular de manera exhaustiva las características definitorias de la prueba digital.

---

[41] HERNÁNDEZ GIMÉNEZ, M., *Inteligencia artificial y derecho penal*, Actualidad jurídica iberoamericana, 10, 2019, p. 813.

[42] MEDINA MARTÍN, E., *La inteligencia artificial y su encuadre como medio de prueba*, *El Criminalista Digital. Papeles De Criminología*, (12), 2024, pp. 33–51.

[43] ARRABAL PLATERO, P., *La prueba…*, Op. Cit., p. 40.

Primeramente, ARRABAL PLATERO establece una serie de rasgos inherentes y definitorios de dichas pruebas digitales tales como la heterogeneidad, facilidad de manipulación, huella digital, ubicuidad, media electrónica y publicidad[44], planteando cada una de ellas diferentes desafíos específicos para el derecho procesal, especialmente en lo que respecta a la protección de los derechos fundamentales y a la garantía de la fiabilidad de las pruebas. Por su parte, PÉREZ PALACÍ analiza propiedades funcionales derivadas de su comportamiento dinámico en entornos tecnológicos, identificando como sus principales características la intangibilidad, volatilidad, delebilidad, parcialidad e intrusividad. Todas estas características demuestran la complejidad que supone gestionar las pruebas tecnológicas en el ámbito jurídico.

Comenzando con las características referidas por la primera autora, refiere que la heterogeneidad constituye el rasgo más distintivo de las pruebas tecnológicas, y como señala MARTÍNEZ GALINDO, esta diversidad proviene de la variedad de fuentes que generan pruebas electrónicas. Esta pluralidad de pruebas conlleva que coexistan diferentes formas de incorporación al proceso de las evidencias[45]. Por ejemplo, el contenido de una página web, mensajes de texto remitidos por medio de aplicaciones de mensajería instantánea más usuales como *WhatsApp* o *Telegram*, publicaciones en redes sociales, imágenes captadas por cámaras de videovigilancia, direcciones IP asociadas a actividades ilícitas, correos electrónicos, entre otros. Por supuesto, dicha variedad implicará que el tratamiento jurídico según el tipo de prueba que se trate pueda variar significativamente. Esto es debido a que su obtención y tratamiento puede afectar a distintos derechos fundamentales y que, además, requerirá un análisis individualizado de cada caso para su admisión, práctica y valoración.

Otra característica fundamental es su facilidad de manipulación, particularidad ampliamente reconocida tanto por la doctrina como por la jurisprudencia. Especialmente, esta cuestión se aborda en la sentencia de 19 de mayo de 2015 del Alto Tribunal, donde hace expresa mención a *la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese*

[44] ARRABAL PLATERO, P., *La prueba…*, Op. Cit., pp. 41-54.

[45] MARTÍNEZ GALINDO, G., *Problemática jurídica de la prueba digital y sus implicaciones en los principios penales*, Revista Electrónica de Ciencia Penal y Criminología, núm. 24-23, 2022, pp. 1-38.

intercambio de ideas, forma parte de la realidad de las cosas[46]. En mi parecer, considero que las pruebas electrónicas no pueden ser alteradas con relativa facilidad para lograr el anonimato mediante la creación de una identidad ficticia, sino que este proceso requerirá de unos conocimientos informáticos mínimos que no están a la mano de cualquiera. Por ello será de vital importancia la participación de peritos informáticos para certificar, mediante el informe pertinente, la autenticidad de las pruebas aportadas en el procedimiento mediante el algoritmo de autenticación y resultado[47], siempre que se haya impugnado previamente por la contraparte, de no ser así *la fuente aportada podría alcanzar pleno valor probatorio*[48].

La huella digital es la tercera característica reseñada por la citada autora, también denominada *HASH*. ARRABAL PLATERO se refiere a la huella digital como aquellos rastros que deja toda actividad realizada a través de dispositivos digitales o metadatos asociados a dicha prueba[49]. Estos metadatos pueden almacenarse en servidores remotos o en los propios dispositivos, y son especialmente útiles en la investigación de delitos informáticos o en aquellos que involucran elementos digitales, como correos electrónicos o direcciones IP.

Por otra parte, BENDER puntualiza que el valor entregado por el HASH *es único para determinado conjunto de datos,* y que *cualquier cambio en estos datos, así sea en uno de sus caracteres, entrega un hash diferente*[50], asegurando la integridad de los datos. En este sentido, en la sentencia núm. 559/2017 del Tribunal Supremo se hizo uso de la identificación *HASH* de los ficheros tratados en la investigación policial, describiendo este concepto como una huella digital única creada utilizando un *algoritmo matemático criptográfico*[51].

Si bien es cierto que, el acceso a esta información no es tarea sencilla puesto que en muchas ocasiones llegar a dicha información puede ser inaccesible, y que junto a la posibilidad de haber sido alterado el *HASH*, limita la eficacia de las periciales informáticas.

---

[46] STS 300/2015, de 19 de mayo, FD 4.
[47] MIRKOUSKI, D. O., *Prueba electrónica: nociones generales*, Revista Pensamiento Penal, (480), 2023.
[48] FUENTES SORIANO, O., *La intervención…*, Op. Cit., p. 279.
[49] ARRABAL PLATERO, P., *La prueba…*, Op. Cit., pp. 45-46.
[50] BENDER, A., *El correo electrónico como prueba en la jurisprudencia*, Thomson Reuters, 2013.
[51] STS 559/2017, de 13 de julio, HP único.

La ubicuidad de la prueba digital se refiere a la capacidad de este tipo de pruebas para estar presentes en múltiples ubicaciones simultáneamente. Esto es debido gracias a su naturaleza digital y a la infraestructura global de las TIC, la cual permite que los datos de correos electrónicos o publicaciones en redes sociales puedan almacenarse y accederse desde lugares muy distantes sin ningún tipo de limitación geográfica. Esta característica de omnipresencia genera complicaciones de competencia territorial y cooperación internacional. Por este motivo existen instrumentos internacionales, como el Convenio de Budapest sobre Ciberdelincuencia[52], que facilitan la cooperación entre Estados, como por ejemplo mediante el acceso transfronterizo a datos almacenados cuando haya consentimiento o cuando se encuentren a disposición del público en fuentes abiertas. Pese a ello, la falta de armonización normativa sigue siendo un obstáculo importante, lo que se traduce en retrasos y dificultades en la obtención de dichas pruebas, pudiendo afectar a la eficacia de las investigaciones, así como a la tutela de los derechos fundamentales.

En cuanto a la media electrónica, facilita el anonimato al permitir generar identidades ficticias o la suplantación de identidades ajenas. Gracias a las TIC los usuarios pueden actuar bajo perfiles falsos, o incluso suplantar la identidad de otras personas, ya sean físicas o jurídicas. Esto dificulta en gran medida la exitosa identificación de los responsables de actividades ilícitas, generando no solo problemas probatorios, sino también posibles vulneraciones de derechos fundamentales, como la intimidad o la propia imagen. Todo ello, como indica FUENTES SORIANO, potenciado por la *asombrosa facilidad con la que las comunicaciones telemáticas pueden ser falseadas, inventadas o incluso efectivamente mantenidas pero realizadas con suplantación de la personalidad de alguno de los comunicantes*[53].

Para terminar, la última de las características señaladas en relación con las pruebas tecnológicas es la publicidad. Esta particularidad se manifiesta exclusivamente en pruebas tecnológicas obtenidas de fuentes abiertas, como

[52] Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Ratificación publicada en el Boletín Oficial del Estado, núm. 226, sec. I, de 17 de septiembre de 2010, p. 78847, recuperado de https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

[53] FUENTES SORIANO, O., *Las comunicaciones telemáticas: aportación y valoración de la prueba*, en El proceso penal. Cuestiones fundamentales, Tirant Lo Blanch, Valencia, 2017, pp. 277-301.

son las redes sociales o páginas web, donde la información publicada voluntariamente por los usuarios de plataformas digitales puede ser recopilada y empleada como medio de prueba en sede judicial, siempre que su obtención cumpla con los requisitos legales pertinentes. Esto se debe a que, al tratarse de datos compartidos de forma consciente y voluntaria en fuentes abiertas, no se considera vulneración del derecho a la intimidad[54], pues como refiere VELASCO NÚÑEZ acerca de *la red, Internet, es ese gran escaparate público en que el que voluntariamente quiere cuelga contenidos, delictivos o no, arriesgándose a que le encuentren las pistas que vaya abandonando, queriendo o sin querer*[55], y cuyo análisis detallado se desarrollará posteriormente.

Centrándonos ahora en el análisis de PÉREZ PALACÍ sobre las pruebas tecnológicas, las define como intangibles, ya que al encontrarse en formato electrónico, son fácilmente reproducibles, pudiendo realizarse copias que dificulten la distinción entre estas últimas y las originales pese a que tengan distinta fecha de creación; volátiles, puesto que las mismas son mudables y manipulables, pudiendo ser modificadas respecto a su origen, por lo que podría ser exigible una pericial informática para acreditar su autenticidad y originalidad si la prueba fuera impugnada por la parte contraria; delebles o destruibles, siendo sumamente sencillo que sean borradas, o incluso que el soporte original que las contiene sea destruido, haciendo imposible su acceso; parciales, ya que en muchas ocasiones las evidencias electrónicas tan solo se encuentran accesibles para aquellas personas que ostentan su titularidad, pudiendo ser la parte contraria o acusada o un tercero, tanto en soporte físico como virtual; y por último, intrusivas, puesto que en algunas ocasiones para su acceso, y por consiguiente recogida, pueden verse afectados derechos fundamentales como la intimidad, el secreto de las comunicaciones, la protección de datos de carácter personal e incluso la inviolabilidad domiciliaria[56].

---

[54] STS 236/2008, de 9 de mayo, FJ 2. En dicha sentencia el Alto Tribunal cita textualmente que "*no se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma*".

[55] VELASCO NÚÑEZ, E., *Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica*, Diario La Ley, Nº 8183, Sección Doctrina, 4 de noviembre de 2013, p. 7.

[56] PÉREZ PALACÍ, J. E., *La prueba*…, Op. Cit., p. 13.

2.3. Principales fuentes de prueba tecnológica

Para el análisis de las pruebas electrónicas, este trabajo se acoge a la clasificación propuesta por PINTO PALACIOS y PUJOL CAPILLA, afirmando que las aportadas con más habitualidad en los Tribunales son el documento electrónico, el correo electrónico, los SMS, las páginas web, las grabaciones de sonido, las fotografías digitales y la videograbación[57]. Esta categorización se ha seleccionado por considerarla la más completa y actualizada, incorporando también las nuevas formas de comunicación digital como son la mensajería instantánea y las redes sociales, ya que estas dos últimas se erigen como los instrumentos probatorios más novedosos empleados en los procesos judiciales.

2.3.1. Documentos electrónicos

Los documentos electrónicos se definen como *todos aquellos objetos materiales en los que puede percibirse una manifestación de voluntad o representativos de un hecho de interés para el proceso que pueda obtenerse a través de los modernos medios reproductivos, como la fotografía, la fonografía, la cinematografía, el magnetófono, las cintas de vídeo, los discos de ordenador y cualesquiera otros similares*. Según ABEL LLUCH, será todo aquel en cuya producción haya intervenido de cualquier forma la informática, o en cualquiera de sus fases haya intervenido un equipo o herramienta informática, o que esté contenido o almacenado en soportes informáticos[58].

Asimismo, este último autor especifica que el documento electrónico está compuesto por elementos como el soporte, siendo éste el dispositivo físico que se facilitará a la autoridad judicial, tales como discos duros, CD o pendrives; el contenido, es decir, la información que alberga dicho soporte físico y que almacena mediante un sistema de codificación binaria, siendo necesario un sistema intermediario para su interpretación y visualización; el autor, tarea de gran complejidad la de averiguar la identidad de su creador, siendo más común la identificación del dispositivo concreto que ha generado tal archivo; y la fecha y firma, marca temporal asignada automáticamente por el sistema o programa

[57] PINTO PALACIOS, F., PUJOL CAPILLA, P., *La prueba…*, Op. Cit., pp. 38-62.
[58] ABEL LLUCH, X., PICÓ i JUNOY, J., *La prueba electrónica*, J.M. Bosch, 2010.

que lo haya generado, complementado con la firma electrónica que acredite la identificación de la persona o entidad que ha emitido un documento concreto[59].

2.3.2. Correo electrónico

El correo electrónico es un sistema de intercambio de textos digitalizados a través de Internet[60], siendo considerado el más antiguo desde que existe Internet. Sus mensajes son almacenados en un servidor concreto mediante un buzón asociado a una dirección electrónica determinada a la que se accederá mediante contraseña privada. Su acceso como prueba en un proceso suele realizarse mediante su impresión en papel, si bien, pueden incorporarse mediante acta notarial que refuerce su eficacia probatoria, acreditando los mensajes enviados, las direcciones de los usuarios y las fechas de remisión. La jurisprudencia considera el mismo como prueba documental[61], sin obviar que se deberá garantizar que la copia es idéntica al original para ser valorada como tal mediante la correspondiente prueba de autenticación[62].

Una vez impreso en papel, se obtiene una copia del correo electrónico en el que, en su cabecera, se detallarán todos los datos que hacen referencia a su contenido, así como remitentes, destinatarios, sistemas y dispositivos intervinientes. Y, aunque los mismos pueden ser modificables, tendrán mayor nivel de solidez y garantía, ya que quedará reseñada la dirección de correo electrónico del emisor, y fecha y hora de entrada y salida del dispositivo, registrándolo con una identidad alfanumérica[63].

El pronunciamiento del Tribunal Supremo de 23 de julio de 2020 reconoce el correo electrónico como prueba documental, afirmando que el hecho de que muchos documentos se presenten en un procedimiento judicial a través de soportes electrónicos debido al desarrollo tecnológico no supone la exclusión de su naturaleza de prueba documental. Pero detalla que dicho reconocimiento *no supone que todo correo electrónico acredite el error fáctico de instancia, al igual*

---

[59] ABEL LLUCH, X., PICÓ I JUNOY, J., *La prueba electrónica*, Colección de Formación Continua Facultad de Derecho ESADE, Serie estudios prácticos sobre medios de prueba, J. M. Bosch editor, 2011, pp. 37-40.

[60] GIMENO SENDRA, V., *Fundamentos del derecho procesal*, Civitas, 1981.

[61] STS 330/2023, de 9 de mayo, FJ 1.

[62] STS 706/2020, de 23 de julio, FD 4.5.

[63] RICHARD GONZÁLEZ, M., *Valor como prueba de los mensajes y comunicaciones electrónicas en los procesos de familia*, Problemática actual de los procesos de familia. Especial atención a la prueba, J.M. Bosch Editor, 2018, pp. 199-250.

que sucede con los documentos privados, para ello será necesario valorar si se ha impugnado su autenticidad por la parte a quien perjudique; si ha sido autenticado, en su caso; y si goza de literosuficiencia[64].

2.3.3. SMS (Short Message Service)

Los SMS son un sistema que permite enviar mensajes cortos de texto, tal y como indica su nombre "*Short Message Service*". Estos son remitidos desde un número de teléfono, y se alojan en un servidor que automáticamente reenvía al destinatario de este. Es un sistema que ha quedado prácticamente obsoleto con la aparición de aplicaciones de mensajería instantánea como *Whatsapp* o *Telegram*, que permiten la comunicación bidireccional mediante el envío de palabras, imágenes, sonidos y archivos, y las cuales se tratarán más adelante.

Dichas pruebas pueden ser determinantes en una causa, pese a que la parte contraria tenga la potestad de impugnar las mismas si se cuestionan los requisitos de autenticidad e integridad, debiendo establecer razonamientos o argumentos lógicos, creíbles y serios. Por ello será conveniente que se acredite la transmisión del SMS, el contenido del mensaje, la confirmación de recepción, la fecha y hora de remisión, así como el emisor y receptor, además de corroborar la veracidad de esta mediante la práctica de pruebas instrumentales. Aun así, el órgano juzgador aplicará igualmente las reglas de la sana crítica teniendo en cuenta el contexto del mensaje[65].

Una forma de acreditar el envío de SMS sería mediante los denominados SMS certificados, los cuales operan a través de un intermediario entre el remitente y destinatario. Este sistema registra la entrega del mensaje corto de texto, fecha y hora de entrega, confirmación de la recepción de este por parte del destinatario, e incluso su lectura. Para ello utiliza tecnologías como el *blockchain*, garantizando la integridad e inmutabilidad de los mensajes, el *timestamping* o sellado de tiempo, reseñando todos los eventos que se producen durante el envío, y la firma digital para autenticar la identidad del remitente. Esta modalidad ha sido aceptada por el Tribunal Supremo como prueba mediante Auto de 21 de marzo de 2013, en el que establece como efectiva la *notificación*

---

[64] STS 706/2020, de 23 de julio, FD 4.5.

[65] NEFTALÍ NICOLÁS GARCÍA, J., *Las nuevas tecnologías y la prueba electrónica en el proceso judicial*, Proceso civil y nuevas tecnologías, 2021, pp. 310-311.

y requerimiento en forma telemática, con los certificados electrónicos acreditativos de la práctica de ello emitidos por un prestador de servicios de certificación […], *los actos de comunicación podrán efectuarse por aquellos medios, con el resguardo acreditativo de su recepción que proceda*[66].

En la sentencia de 26 de noviembre de 2014, el Alto Tribunal entendió como prueba lícita los SMS obtenidos del teléfono de una víctima fallecida, y aportados por sus herederos legítimos. Consideró que *las copias de los mensajes recibidos y transmitidos por la menor, […], equivalen a la correspondencia que pueda ser conservada por la menor entre sus papeles privados*. Gracias a esto fue posible la identificación del número de teléfono titularidad del acusado. Asimismo, señaló que el art. 18.3 CE, en referencia al secreto de las comunicaciones, *no garantiza el secreto de los pensamientos que una persona ha transmitido a otra, por lo que el receptor es libre de transmitir estas comunicaciones a terceros* [67].

2.3.4. Páginas web

Las páginas web constituyen una *clase de documento informático accesible a través de Internet previa identificación de un enlace*[68], acceso que se lleva a cabo mediante un navegador. Su contenido presenta una notable volatibilidad, por lo que resulta aconsejable documentar su estado en un momento determinado mediante la intervención de un tercero imparcial. Entre los mecanismos disponibles para este fin destaca la certificación notarial, *en la que el fedatario público pueda navegar por la web a fin de dar fe de su existencia y contenido en un momento y día determinado*[69].

Se trata de una fuente de información infinita[70], concretamente, un espacio virtual en el que un número indeterminado de usuarios comparten un sinfín de contenidos en tiempo real. Entre estos contenidos encontramos ideas, opiniones, experiencias, fotografías digitales, vídeos, archivos, entre otros. Este espacio permite una comunicación permanente con independencia de su ubicación geográfica, siempre y cuando tengan acceso a la red de Internet.

---

[66] ATS, de 21 de marzo de 2013, FD 2.

[67] STS 850/2014, de 26 de noviembre, FD 9.

[68] ABEL LLUCH, X., *Régimen jurídico de la prueba electrónica*. Colección de Formación Continua Facultad de Derecho ESADE, J.M. Bosch Editor, Barcelona, 2011.

[69] PINTO PALACIOS, F., PUJOL CAPILLA, P., *La prueba…*, Op. Cit., p. 46.

[70] GIL NOGUERAS, L.A., *La valoración de la prueba electrónica en el proceso civil*, práctica de Tribunales, núm. 130, Wolters Kluwer, 2018, p. 12.

La sentencia núm. 450/2019 de la Audiencia Provincial de Zaragoza, reconoce como prueba admisible la acreditación de los contenidos de Internet archivados por terceros imparciales fiables. Como ejemplo menciona el archivo digital público "*WayBack Machine*" gestionado por la organización sin ánimo de lucro "*The Internet Archive*". El Tribunal considera que *presenta garantías suficientes para beneficiarse de una presunción de fuente de información fiable y de confianza*, siempre que se acrediten con acta notarial que dé fe de su consulta, verificando la información publicada en una fecha concreta[71].

2.3.5. Grabaciones de sonido

Las grabaciones de sonido en soporte electrónico deben cumplir rigurosas garantías de admisibilidad para su inclusión en el proceso. Entre estas garantías se encuentran la protección a la intimidad, así como la puesta a disposición de los soportes de registro y verificación de su autenticidad. Esto se podrá llevar a cabo mediante el cotejo de voces para certificar que el registro fonográfico coincide con la persona determinada, además de la identificación de los participantes en la conversación mediante métodos de acústica forense.

De especial relevancia es la sentencia núm. 114/1984 del Tribunal Constitucional, que establece que la grabación de una conversación ajena atentará contra el derecho a la intimidad. Caso contrario sería si el que graba es parte en la conversación, siempre y cuando la finalidad sea dejar constancia fidedigna de lo tratado, pudiendo emplearse como medio probatorio válido en un procedimiento judicial[72]. Tal extremo es ratificado por el Tribunal Supremo en su sentencia núm. 298/2013, en el que afirma que *la escucha o grabación por un tercero sin autorización de ninguno de los comunicantes ni de la autoridad judicial convierte en inutilizable ese medio probatorio*[73].

Además, este último órgano jurisdiccional, en su sentencia de 6 de abril de 2020, precisó que las grabaciones de sonido por sí solas no tienen naturaleza de prueba documental ni, en consecuencia, eficacia revisora de hechos probados. Se trata de medios de reproducción de sonido que, aunque son válidos como prueba durante un juicio oral, y por lo que fueron admitidos en

[71] SAP Zaragoza 450/2019, de 31 de mayo, FJ 9.
[72] STC 114/1984, de 29 de noviembre, FJ 7.
[73] STS 298/2013, de 13 de marzo, FD 1.

primera instancia, carecen de eficacia para modificar hechos ya declarados probados en recursos extraordinarios al no ser consideradas pruebas documentales. Para adquirir esta consideración, la grabación debe haber sido autenticada como documento electrónico, por ejemplo, mediante dictamen pericial o reconocimiento de la parte contraria[74].

2.3.6. Fotografía digital

La fotografía digital, como fuente de prueba tecnológica en el ámbito judicial, ha adquirido una relevancia significativa debido a su capacidad para capturar y reproducir de manera fehaciente un hecho concreto. Dichas imágenes, almacenadas en la memoria interna de un dispositivo electrónico o en elementos externos como las tarjetas de memoria, pueden transferirse a otros soportes digitales, como ordenadores o *pendrives*, para su reproducción o edición mediante programas especializados.

En cuanto a su valor probatorio, este radica en su poder persuasivo, ya que permiten acreditar visualmente situaciones o hechos relevantes para el proceso. Sin embargo, su incorporación a éste ya sea en formato físico o digital, requiere la constatación de la autenticidad e integridad de la prueba electrónica[75], tal y como se recoge en el art. 230.2 LOPJ.

Añadir que, el requisito pertinente para garantizar el principio de inmediación es el visionado directo de la prueba digital en sede judicial. Si bien, la sentencia núm. 285/2016 del Tribunal Supremo demuestra que, siendo *imposible el visionado, porque no reconoce los discos el aparato de reproducción disponible,* haciendo imposible la observación directa o adveración por parte del LAJ, no invalida su valor probatorio. Esto quedó sustentado mediante el *informe elaborado por especialistas que refleja el contenido de los discos duros y que recoge algunas de las imágenes y fotogramas*, y que además cuya posesión fue reconocida mediante declaración del acusado, ya que dicho informe fue ratificado en el acto del juicio oral y, en consecuencia, sometido a contradicción[76].

---

[74] STS 325/2022, de 6 de abril, FD 3 y FD 4.

[75] Artículo 230, apartado segundo, de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, publicada en el BOE núm. 157, de 2 de julio de 1985, dispone que "2. *Los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad e integridad y el cumplimiento de los requisitos exigidos por las leyes procesales*", recuperado de https://www.boe.es/eli/es/lo/1985/07/01/6/con

[76] STS 285/2016, de 6 de abril, FD 2.

Además, uno de los principales problemas que plantean las fotografías digitales es la dificultad para acreditar con certeza la fecha y lugar en que fueron tomadas, pudiendo dar lugar a impugnaciones por parte de las partes involucradas. Para ello, se podría solicitar dictamen pericial informático que certifique que los archivos fotográficos no han sido alterados y que corresponden a los originales capturados en un momento específico. Esto le otorgaría la condición de prueba preconstituida documental sin necesidad de ratificación en juicio oral[77]. O incluso se puede hacer uso de plataformas de certificación digital, como *SafeStamper*, que permiten garantizar la autenticidad de las imágenes mediante sellos temporales en las evidencias electrónicas[78].

2.3.7. Videograbaciones

En cuanto a las videograbaciones, estas consisten en la captación y grabación de imágenes a través de dispositivos electrónicos, como cámaras de videovigilancia o teléfonos móviles. Su uso en el ámbito judicial está sujeto a una regulación específica que varía en función de quién realiza la grabación y el contexto en que se obtiene, aspectos que se analizan a continuación.

Las grabaciones en lugares públicos realizadas por parte de las Fuerzas y Cuerpos de Seguridad están reguladas por la Ley Orgánica 4/1997, que establece el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima, y la necesidad de un riesgo razonable para la seguridad ciudadana[79]. En este sentido, el Tribunal Supremo sostiene que las imágenes captadas en la vía pública sobre escenas desarrolladas en espacios abiertos no requieren autorización judicial, ya que la policía actúa con plena legitimidad en su labor investigativa, amparada por el art. 282 LECrim y la Ley Orgánica 2/1986 de Cuerpos y Fuerzas de Seguridad del Estado[80].

Es en su obtención en el ámbito privado sería donde se pueden generar conflictos relacionados con la vulneración de derechos fundamentales, como el derecho a la intimidad o a la propia imagen recogidos en el art. 18 CE. Esto

[77] STC 128/1990, de 5 de Julio.

[78] SAFE STAMPER, *¿Qué es Safe Stamper?,* s. f., recuperado el 27 de abril de 2025 de https://www.safestamper.com/?lang=es

[79] Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, publicada en el BOE núm. 186, de 5 de agosto de 1997, pp. 23824-23828, recuperado de https://www.boe.es/eli/es/lo/1997/08/04/4

[80] STS 299/2006, de 17 de marzo, FD 1.

ocurre especialmente en grabaciones o capturas realizadas sin consentimiento. Empero, el Alto Tribunal sí ha validado como prueba las grabaciones de cámaras de videovigilancia instaladas en el exterior de un establecimiento, considerando que no vulneran el derecho a la intimidad ni a la propia imagen del acusado, ya que las imágenes captadas en espacios públicos o de acceso común, con fines de seguridad y prevención del delito, tienen un valor probatorio objetivo y directo, equiparable o superior al testimonio humano, siempre que se respeten los principios de proporcionalidad y legalidad en su obtención y uso[81].

Por otro lado, las videograbaciones realizadas por Seguridad Privada están reguladas por la Ley 5/2014. Esta ley restringe su uso a fines de seguridad y establece criterios específicos para la conservación y custodia de las grabaciones, con el fin de garantizar su validez como prueba en investigaciones policiales o judiciales[82]. En este contexto, el Tribunal Supremo en su sentencia de 14 de abril de 2016, ha señalado que es perfectamente lícito que la convicción judicial sobre la participación de individuos en hechos delictivos se base en imágenes obtenidas de grabaciones realizadas en establecimientos privados abiertos al público, como los accesos de un banco, siempre que el Tribunal haya verificado que la filmación refleja fielmente los hechos ocurridos y que se ajusta a lo enjuiciado en cada caso concreto[83].

Finalmente, las grabaciones realizadas por particulares, especialmente mediante cámaras ocultas, han sido objeto de debate jurisprudencial. Aunque inicialmente se consideraba que primaba el derecho a la intimidad sobre el derecho a la información, la jurisprudencia reciente del Tribunal Supremo ha reconocido la validez de estas grabaciones cuando aportan pruebas relevantes en procedimientos penales, siempre que se respeten los derechos fundamentales. Esto lo matiza al precisar que *la jurisprudencia constitucional no permite afirmar que una cámara oculta conlleve siempre y en todo caso una vulneración de los principios y derechos que convergen en el proceso penal de esas imágenes grabadas*[84].

---

[81] STS 649/2019, de 20 de diciembre, FD 3.

[82] Ley 5/2014, de 4 de abril, de Seguridad Privada. Publicada en el BOE núm. 83, de 5 de abril de 2014, recuperado de https://www.boe.es/eli/es/l/2014/04/04/5/con

[83] STS 315/2016, de 14 de abril, FD 2.

[84] STS 167/2020, de 19 de mayo, FD 4.

2.3.8. Mensajería instantánea

Al referirse a la mensajería instantánea, es inevitable pensar en *WhatsApp* y *Telegram* al ser las dos aplicaciones más utilizadas en la actualidad, las cuales superan los dos mil millones y los mil millones de usuarios activos mensuales respectivamente [85]. Estas aplicaciones permiten el intercambio de datos e información con otras personas, concretamente de texto, fotografías, videos, audios, contactos o localización en tiempo real, de forma ilimitada y gratuita mediante conexión a Internet, lo que lleva a cabo con un teléfono móvil, ordenador o análogo[86].

La aplicación *WhatsApp* destaca por su cifrado de extremo a extremo usado por defecto, denominado "*end-to-end* "[87] o sistema *E2EE*. Este sistema asegura que tan solo los participantes de la conversación puedan leer el contenido de los mensajes, ya que los mismos se almacenan en los propios dispositivos de los interlocutores, accediendo a ellos mediante un código/llave que tan solo disponen éstos, siendo ininteligibles incluso tanto para la propia compañía *Meta*, propietaria de *Whatsapp*, como para las FFCCS si tratan de realizar su interceptación mediante la plataforma SITEL[88]. No obstante, este sistema encuentra un punto de vulnerabilidad en los metadatos asociados a dichas interacciones, los cuales no se encuentran cifrados y son almacenados por la compañía *Meta*. Ésta registra los datos de los usuarios de las comunicaciones, la frecuencia de los mensajes, las marcas de tiempo y las direcciones IP desde donde se conectan[89].

Por su parte, la aplicación *Telegram*, en contraposición, tan sólo hace uso del sistema *E2EE* en chats secretos previamente iniciados por los interlocutores. Ahora bien, en aras de garantizar la privacidad y seguridad de los titulares de las cuentas, ofrece un sistema de inicio de conversaciones basado exclusivamente en nombres de usuario, es decir, sin requerir la exposición de datos personales

---

[85] GARCÍA, M., *Telegram supera los 1000 millones de usuarios activos al mes*, Zona Movilidad, 5 de abril de 2025, recuperado el 27 de abril de 2025 de https://www.zonamovilidad.es/telegram-supera-1000-millones-usuarios-activos-mes

[86] NEFTALÍ NICOLÁS GARCÍA, J., *Las nuevas tecnologías…*, Op. Cit., p. 310.

[87] DELGADO MARTÍN, J., *La prueba del Whatsapp*, Diario La Ley, nº 8605, Sección Tribuna, 2015.

[88] PINTO PALACIOS, F., PUJOL CAPILLA, P., *La prueba…*, Op. Cit., p. 95.

[89] ANÓNIMO, *Los metadatos: La puerta trasera de la ciberseguridad de WhatsApp*, Panda Security, 15 de octubre de 2024, recuperado el 27 de abril de 2025 de https://www.pandasecurity.com/es/mediacenter/metadatos-puerta-trasera-de-ciberseguridad-de-whatsapp/

como los números telefónicos. Esta característica contrasta con el modelo de *WhatsApp*, cuya funcionalidad depende necesariamente de la divulgación previa del número de teléfono del usuario, generando así mayores riesgos para la protección de datos personales[90].

Desde sus creaciones, en 2009 *Whatsapp*[91] y 2013 *Telegram*[92], es incuestionable que el uso de estas aplicaciones de mensajería instantánea ha aumentado exponencialmente. Este crecimiento ha sido impulsado por la digitalización global y el aumento de uso de las TIC por parte de la sociedad y, por ende, también se ha visto incrementada su presencia en procesos judiciales con su participación en éstos en forma de pruebas tecnológicas.

Ahora bien, su admisibilidad probatoria requiere superar rigurosos criterios de autenticidad y fiabilidad, tal como exige la jurisprudencia. Un ejemplo de ello se encuentra en la sentencia núm. 754/2015 del Tribunal Supremo, en la que se afirma que *únicamente con un informe pericial que identifique el teléfono emisor de los mensajes delictivos, a salvo de cumplido reconocimiento, o prueba testifical que acredite su remisión, pueden dar cobertura probatoria a la autenticidad del mensaje.* El Tribunal lleva a cabo esta apreciación ya que, como continúa manifestando en la sentencia, *las posibilidades de manipulación son muy variadas y el órgano jurisdiccional tiene que ponerse en guardia con todas las cautelas que sean recomendables ante la posibilidad de una superchería*[93].

2.3.9. Redes sociales

El desarrollo de Internet ha propiciado el surgimiento de las redes sociales[94], creadas a mediados de los años noventa del siglo pasado como plataformas de comunicación para poner en contacto a antiguos compañeros de estudios[95]. Estas han evolucionado hasta convertirse en espacios digitales en

---

[90] VALERO, C., *Whatsapp vs Telegram: ¿cuál es mejor?*, ADSL Zone, 8 de enero de 2025, recuperado el 27 de abril de 2025 de https://www.adslzone.net/reportajes/seguridad/whatsapp-vs-telegram/

[91] GIL, C., *Historia de Whatsapp: cómo se creó la app que ha revolucionado la comunicación social*, Marketing4eCommerce, 14 de noviembre de 2023, recuperado el 27 de abril de 2025 de https://marketing4ecommerce.net/historia-de-whatsapp/

[92] JIMÉNEZ, R., *Historia de Telegram, considerada una de las plataformas más seguras del mundo*, El Comercio, 28 de agosto de 2024, recuperado el 27 de abril de 2025 de https://www.elcomercio.com/tecnologia/telegram-pavel-durov-plataforma-historia.html

[93] STS 754/2015, de 27 de noviembre, FD 3.

[94] AGUSTINOY GUILAYN, A., MONCLÚS RUIZ, J., *Aspectos legales de las redes sociales*, Editorial Bosch, Barcelona, 2016, p. 18.

[95] PINTO PALACIOS, F., PUJOL CAPILLA, P., *La prueba…*, Op. Cit., p. 62.

los que un gran número de usuarios interactúan entre sí compartiendo información en múltiples formatos, por ejemplo, mediante la publicación de comentarios, opiniones, fotografías, audios o vídeos[96]. Para ello, tan sólo tendrán que crear un perfil o cuenta sin la necesidad de que el usuario se identifique por ningún medio oficial, permitiendo el anonimato a aquellos que así lo deseen.

Al igual que las aplicaciones de mensajería instantánea, las redes sociales constituyen un medio de comunicación que, a diferencia de las primeras, se caracterizan por tener principalmente una difusión pública o semipública de sus contenidos. Esta particularidad favorece en muchos supuestos la obtención y aportación lícita de estos elementos probatorios al proceso judicial. Al mismo tiempo, tiene especial relevancia en el ámbito de los derechos fundamentales, ya que la publicidad inherente a estas plataformas minimiza las limitaciones sobre derechos como la intimidad y el secreto de las comunicaciones en comparación con los medios de carácter privado del apartado anterior. Incluso, si se llevase a cabo un análisis de sus rastros digitales se podrían *aportar pruebas o indicios muy valiosos no solamente de hechos ocurridos en dichas redes, sino también de hechos cometidos en el mundo físico*[97].

Si bien, como refiere la citada sentencia núm. 300/2015 del Alto Tribunal, *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*. Asimismo, refiere que el anonimato que garantizan este tipo de plataformas, sumado a la ausencia de controles rigurosos en la creación de cuentas, hace posible que un mismo usuario genere interacciones ficticias en las que, mediante el uso de identidades falsas o suplantadas, pueda crear la apariencia de un diálogo entre diversas personas, cuando en realidad está manteniendo una conversación consigo mismo. Es por lo que el Tribunal afirma que, para impugnar la autenticidad de las conversaciones telemáticas, *cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria.* Por todo lo anterior, llega a la conclusión de que, en tales supuestos, *será indispensable la práctica de una*

[96] VALLE MUÑOZ, F. A., *Las redes sociales como medio de prueba en el proceso laboral*, Revista de Estudios Jurídico-Laborales y de Seguridad Social, núm. 6, 2023, p. 120.
[97] ABEL LLUCH, X., PICÓ I JUNOY, J., *La prueba electrónica*…, Op. Cit., p. 201.

prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido[98].

Para comprender la relevancia jurídica de las redes sociales como escenario delictivo de las que obtener elementos probatorios, en la sentencia del Tribunal Supremo núm. 547/2022, se reconoce como "lugar de comisión del delito" a los espacios virtuales de encuentro y comunicación de Internet como son las redes sociales. El Tribunal establece que e*l ciberespacio ofrece un marco digital diferenciado de la realidad puramente física como espacio del delito,* especificando que las redes sociales, además de ser un instrumento para cometer delitos de diferente índole*, pueden ser también el escenario en el que el delito se comete, ya sea durante todo su desarrollo, ya en la ejecución de sólo algunos de los elementos del tipo*[99]. En este caso, se impuso conforme al art. 48 CP una pena de prohibición de acudir al lugar del delito[100], es decir, una red social.

Biblioteca
UNIVERSITAS Miguel Hernández

[98] STS 300/2015, de 19 de mayo.

[99] STS 547/2022, de 2 de junio, FD 3.3.

[100] Artículo 48, apartado primero, de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicada en el BOE núm. 281, de 24 de noviembre de 1995, dispone que: "*1. La privación del derecho a residir en determinados lugares o acudir a ellos impide al penado residir o acudir al lugar en que haya cometido el delito, o a aquel en que resida la víctima o su familia, si fueren distintos"*, recuperado de https://www.boe.es/eli/es/lo/1995/11/23/10/con

3. La prueba tecnológica ilícita

En el presente apartado se analiza la estrecha relación establecida en el proceso penal entre la licitud en la obtención de las pruebas tecnológicas, y la salvaguarda de los derechos fundamentales de las partes implicadas. Por ello se realiza un examen pormenorizado de las pruebas de origen ilícito, así como de la creciente facilidad con la que las nuevas tecnologías permiten vulnerar tales derechos, sobre todo los recogidos en el art. 18 CE.

En primer término, se profundiza en la distinción conceptual entre prueba ilícita, irregular y prohibida, cuestión que genera algunas discrepancias doctrinales y jurisprudenciales, concretamente en lo que respecta a las pruebas ilícitas. En términos generales se puede afirmar que las pruebas irregulares *serían aquellas obtenidas, propuestas o practicadas con infracción de la normativa procesal que regula el procedimiento probatorio, pero sin afectación nuclear de derechos fundamentales* y, por tanto, permitiendo su *subsanación y/o convalidación*[101]. En cambio, las pruebas ilícitas se diferencian esencialmente por surgir de la *violación de las normas constitucionales tuteladoras de los derechos fundamentales*[102]. El resultado derivado de estas últimas sería lo que se denomina pruebas prohibidas, *sancionándose con la expulsión del proceso a la prueba ilícitamente obtenida*[103].

Paralelamente, el examen de los derechos fundamentales afectados por estas pruebas, como el derecho a la intimidad, a la inviolabilidad del domicilio, al secreto de las comunicaciones y a la protección de los datos personales, revela la necesidad de conciliar la búsqueda de la verdad material con las garantías constitucionales de éstos. Como señala el Tribunal Constitucional, los derechos fundamentales no solo protegen esferas individuales frente al Estado, sino que también operan en relaciones entre particulares, configurándose como pilares del Estado social y democrático de derecho[104].

---

[101] MIRANDA ESTRAMPES, M., *La prueba ilícita: la regla de exclusión probatoria y sus excepciones*, Revista Catalana de Securetat Pública, núm. 22, mayo 2010, p. 133.

[102] GINER ALEGRÍA, C. A., *Prueba prohibida y prueba ilícita*. Anales de derecho. Universidad de Murcia, número 26, 2008, p. 579.

[103] FUENTES SORIANO, O., *La prueba prohibida*…, Op. Cit., p. 11.

[104] STC 18/1984, de 7 de febrero, FJ 3.

La interdependencia entre la ilicitud probatoria y la protección de derechos se manifiesta en que la obtención de pruebas tecnológicas debe respetar siempre los límites constitucionales. Como indica FUENTES SORIANO, la imposibilidad de valorar pruebas obtenidas con vulneración de derechos fundamentales responde a la necesidad de preservar la integridad del proceso judicial, *impidiendo que a la verdad se llegue obviando el respeto que merecen estos derechos desde su preminente posición en el ordenamiento*[105].

3.1. Prueba ilícita o prohibida

Es muy posible que lo primero que llame la atención al lector sea el supuesto tratamiento como sinónimos de los términos "prohibida" e "ilícita". Si bien, tras realizar una aproximación al estudio sobre tales pruebas se observa que tanto en la doctrina como en la jurisprudencia se hace uso de diversa terminología para referirse a estas. Por ejemplo, las ya mencionadas pruebas prohibidas o ilícitas, y otras calificaciones comúnmente utilizadas como son pruebas ilegales, irregulares, nulas, viciadas o inconstitucionales.

A continuación, se van a tratar aquellas pruebas clasificadas por GINER ALEGRÍA según su criterio causal o material[106]. Este autor las cataloga según la causa que origina su ilicitud, distinguiéndolas entre las pruebas irregulares y/o ilegales y las pruebas obtenidas o practicadas con infracción de los derechos fundamentales de las personas, que denomina como inconstitucionales.

En cuanto a las pruebas denominadas irregulares, o también llamadas por el autor citado como defectuosas, no cabe confusión alguna entre la doctrina mayoritaria en definirlas como aquellas conseguidas *con vulneración de las normas de rango ordinario que regulan su obtención y práctica*[107]. Dicho concepto ha sido acogido por la FGE en su *Memoria de la Fiscalía General del Estado en 1996*, donde se definen como aquellas pruebas obtenidas habiendo transgredido la ley ordinaria o normativa procesal y/o habiéndose practicado sin las formalidades reglamentarias[108]. Su irregularidad no afecta a derechos fundamentales, pero puede limitar su valor probatorio.

---

[105] FUENTES SORIANO, O., *La prueba prohibida…*, Op. Cit., p. 18.
[106] GINER ALEGRÍA, C. A., *Prueba prohibida…*, Op. Cit., p. 587.
[107] GINER ALEGRÍA, C. A., *Prueba prohibida…*, Op. Cit., p. 587.
[108] Fiscalía General del Estado. *Memoria de la Fiscalía General del Estado 1996*. Ministerio de Justicia, 1996.

No obstante, a diferencia de la prueba ilícita, el material probatorio obtenido mediante prueba irregular puede ser valorado en juicio, según jurisprudencia del Tribunal Supremo. Esta diferenciación adquiere relevancia en su aplicación concreta dentro del ámbito procesal *en la posibilidad de recuperación del material probatorio evidenciado por la prueba irregular, mediante su conversión en algún otro tipo de prueba subsidiaria, generalmente la testifical o la confesión, a modo de subsanación, posibilidad que es impensable en el caso de la prueba ilícita*[109]. Igualmente, ASENCIO MELLADO, especifica que son el resultado de la *contravención de una norma distinta, de inferior grado a la norma de rango constitucional que consagra un derecho fundamental*[110].

Al examinar el término pruebas ilícitas, encontramos diversas concepciones acerca de éstas, y que MIRANDA ESTRAMPES distingue entre amplias y restrictivas[111]. La concepción amplia no aborda el concepto de forma unánime, pudiendo encontrar un tratamiento heterogéneo. Por ejemplo, un sector doctrinal señala que atentan contra la dignidad de las personas[112], derecho fundamental reconocido tanto en el art. 1 DUDH, donde cita que *todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros*[113], como en el art. 10.1 CE, en el que se reconoce la *dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social*[114].

Continuando con esta primera concepción, MONTÓN REDONDO desplaza el foco hacia la intencionalidad, refiriéndose a aquella prueba obtenida de forma fraudulenta a través de una conducta ilícita[115], siendo el dolo lo que conduce a

[109] STS 115/2015, de 5 de marzo, FD 1.

[110] ASENCIO MELLADO, J. M., FUENTES SORIANO, O., *Derecho procesal penal* (3ª edición), Tirant lo Blanch, 2024, p. 173.

[111] MIRANDA ESTRAMPES, M., SERRA DOMINGUEZ, M., *El concepto de prueba ilícita y su tratamiento en el proceso penal* (2ª edición), Bosch Editor, 2004, pp. 19-24.

[112] SILVA MELERO, V., *La prueba procesal*, Tomo I, Revista de Derecho Privado, Madrid, 1963, p. 69.

[113] Artículo 1 de la Declaración Universal de los Derechos Humanos, Resolución 217 A (III), proclamada por la Asamblea General de las Naciones Unidas, París, 10 de diciembre de 1948, recuperado de https://www.un.org/es/about-us/universal-declaration-of-human-rights

[114] Artículo 10 de la Constitución Española.

[115] MONTÓN REDONDO, A., *Los nuevos medios de prueba y la posibilidad de su uso en el proceso*, Salamanca, Departamento de Derecho Procesal de la Universidad, 1977, p. 174.

su ineficacia. Por su parte, DEVIS ECHANDÍA las describe como *aquellas que están expresa o tácitamente prohibidas por la ley o atentan contra la moral y las buenas costumbres del respectivo medio social o cortara la dignidad y libertad de la persona humana o violan sus derechos fundamentales*[116].

La concepción restrictiva, defendida también por la FGE en la memoria citada con anterioridad, se refiere a pruebas en cuyo *origen y/o desarrollo se ha vulnerado un derecho o libertad fundamental* [117]. GONZÁLEZ MONTES establece los límites del derecho debiendo tratarse de una infracción del mismo nivel, es decir, *aquellos medios de prueba en cuya obtención se hubiere violado un derecho fundamental del mismo rango al menos o superior que el derecho a la prueba*[118]. Se considera que tienen rango de fundamental los recogidos entre los artículos 14 y 29 de la Constitución Española, ambos inclusive, redactados bajo el epígrafe de la Sección 1ª *de los derechos fundamentales y de las libertades públicas*, y que gozan de amparo constitucional. Esta postura se apoya en la sentencia del Tribunal Constitucional núm. 114/1984, en la que se hace mención expresa de las pruebas ilícitas, proclamando con carácter absoluto *la inadmisibilidad procesal de las pruebas obtenidas violentando los derechos o libertades fundamentales, […], imposibilidad de admisión de estas pruebas deriva de la posición preferente de los derechos fundamentales en el ordenamiento jurídico y de su condición de inviolables*[119].

Por lo tanto, como refiere COSTA TORNÉ, uno de los requisitos elementales de la actividad probatoria es la licitud. Esto conlleva que las pruebas aportadas tanto por la acusación como por la defensa *deben ser licitas y no ser contrarias ni vulnerar los derechos garantizados por la Constitución Española en los artículos 14-29*[120].

En definitiva, la ineficacia de la prueba supondrá la imposibilidad de que se incorpore al procedimiento por ningún medio. Al ser señalada como ilícita conllevará su exclusión por el órgano judicial competente y, por tanto, se prohíba

---

[116] DEVIS ECHANDÍA, H., *Teoría general de la prueba judicial* (5º edición), Buenos Aires, 1981, p. 539.

[117] Fiscalía General del Estado. *Memoria de Fiscalía General del Estado 1996*. Ministerio de Justicia, 1996.

[118] GONZÁLEZ MONTES, J. L., *La prueba obtenida ilícitamente con violación* de los derechos fundamentales (el derecho constitucional a la prueba y sus límites), Revista Derecho Procesal, 1990, p. 31.

[119] MIRANDA ESTRAMPES, M., SERRA DOMINGUEZ, M., *El concepto…*, Op. Cit., p. 24.

[120] COSTA TORNÉ, M. C., *La prueba ilícita por violación de Derechos Fundamentales y sus excepciones*, Revista de Derecho UNED, Nº11, 2012, p. 139.

la valoración del resultado probatorio en la sentencia, esto es, su ineficacia como prueba[121]. Esta ineficacia constituye un elemento distintivo frente a la prueba irregular, al excluir toda posibilidad de subsanación posterior.

El debate, según ROCA MARTÍNEZ, no gira en torno a la veracidad de los hechos objeto de investigación*, sino sobre los límites que el respeto a los derechos fundamentales puede o deben imponer a la actuación investigadora y probatoria en el proceso penal* [122]. En consonancia con ello, FUENTES SORIANO matiza que dicha expulsión del proceso *lo hace con la finalidad de garantizar la preminencia de los Derechos Fundamentales y de preservarlos frente a posibles injerencias de terceros,* independientemente de que dicha injerencia provenga del Estado o de un particular[123].

En lo que respecta a las pruebas prohibidas, esta última autora detalla que como consecuencia de la ilicitud de las pruebas *supondrá la prohibición de utilizar en el proceso cualquier posible información probatoria directa o indirectamente derivada de ella* [124]. ASENCIO MELLADO afirma que tal vulneración se ha producido en el transcurso de la *actividad de búsqueda y obtención del material probatorio que pretende ser incorporado al proceso por resultar útil al conocimiento o averiguación de los hechos objeto de enjuiciamiento*[125], y que su expulsión del proceso deberá ser inmediata.

En el mismo sentido, la ya citada *Memoria* de la FGE las define como *consecuencia de la prueba ilícita, esto es, aquella prueba que no puede ser traída al proceso puesto que en su génesis ha vulnerado derechos o libertades fundamentales*[126]. En ampliación de esto, PICÓ JUNOY considera más correcta para denominar *las consecuencias o efectos prohibitivos que la prueba ilícita comporta, esto es, la prohibición de admisión y la prohibición de valoración*[127].

---

[121] GIMENO SENDRA, V., *Derecho procesal penal* (2ª edición), Editorial Aranzadi, 2015, p. 807.

[122] ROCA MARTÍNEZ, J. M., NIETO MORALES, C., *Procesos y Prueba Prohibida*, Dykinson, 2022, p. 143.

[123] FUENTES SORIANO, O., *La prueba prohibida…*, Op. Cit., p. 11.

[124] FUENTES SORIANO, O., *El valor probatorio de los correos electrónicos*. Capítulo del libro: Justicia Penal y Nuevas formas de delincuencia, (Dir. ASENCIO MELLADO, Coord. Fernández López), Ed. Tirant lo Blanch, Valencia 2017, p. 6.

[125] ASENCIO MELLADO, J. M., FUENTES SORIANO, O., *Derecho…*, Op. Cit., pp. 173-174.

[126] RIVES SEVA, A. O., *La intervención de las Comunicaciones en la jurisprudencia penal*, Editorial Aranzadi, Pamplona, 2000, p. 221.

[127] PICÓ JUNOY, J., *El derecho a la prueba en el proceso civil*, Bosch Editor, Barcelona, 1996, p. 290.

VELASCO NÚÑEZ, explica la consecuencia de su ilicitud, y es que el conocimiento de dicha prueba no puede generar, de modo directo ni indirecto, perjuicio alguno para el investigado. En consecuencia*, si la prueba ilícita es la única incriminatoria, no existirá otra solución jurídica que el archivo de la causa penal o la absolución de quien fuera acusado basándose en ella*[128].

En los siguientes apartados se va a analizar las principales teorías que fundamentan la ilicitud probatoria de las pruebas tecnológicas en el proceso penal. Estas tres teorías son denominadas teoría directa, teoría de los frutos del árbol envenenado y, por último, teoría de la antijuridicidad. Este desarrollo teórico permitirá comprender los distintos grados de afectación a las garantías procesales y los mecanismos de exclusión probatoria aplicables a las evidencias digitales obtenidas con vulneración de derechos fundamentales.

3.1.1. Teoría directa

Con la aprobación de la Ley Orgánica del Poder Judicial[129] se reguló en su art. 11.1 LOPJ la prohibición de valoración de pruebas ilícitas, concretamente las *adquiridas, directa o indirectamente, con violación de derechos fundamentales, aplicable a todos los órdenes jurisdiccionales y a todas las pruebas*[130].

En el año anterior a dicha norma, el Tribunal Constitucional ya había adoptado una concepción restrictiva de la prueba ilícita[131]. Pese a no realizar distinción alguna entre las pruebas directas e indirectas, declaró que su obtención vulnerando derechos o libertades fundamentales supondría la inadmisibilidad de éstas, así como su práctica a través de cualquier medio probatorio. Esto se debe a que podría verse vulnerado el derecho a un proceso con todas las garantías[132], recogido en el art. 24.2 CE, quedando *garantizada su*

---

[128] VELASCO NÚÑEZ, E., *Investigación procesal…*, Op. Cit., p. 2.

[129] Artículo 11, apartado primero, de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, publicada en el BOE núm. 157, de 02 de julio de 1985, dispone que "*1. En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales*", recuperado de https://www.boe.es/eli/es/lo/1985/07/01/6/con

[130] ARRABAL PLATERO, P., *La prueba…*, Op. Cit., p. 62.

[131] STC 114/1984, de 29 de noviembre.

[132] Artículo 24, apartado segundo, de la Constitución Española, dispone que "*2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia*".

aplicación tanto a la prueba obtenida por el Estado como a la obtenida por particulares[133].

Desde una perspectiva esencial, lo que la norma establece es que cualquier medio probatorio obtenido mediante la vulneración de derechos fundamentales debe ser considerado nulo. Por tanto, *su valoración, apreciación o toma en consideración vedada o, lo que es lo mismo, en caso alguno los Tribunales podrán tenerla en cuenta para basar en ella una sentencia condenatoria*[134].

Esta invalidez es denominada como regla de exclusión, la cual no debe entenderse en sentido absoluto ya que, de forma progresiva en el tiempo se han introducido excepciones. En esta línea doctrinal, DELGADO DEL RINCÓN afirma que éstas han de darse únicamente en circunstancias excepcionales que justifiquen apartarse del criterio general de exclusión*, pues de lo contrario se corre el riesgo de que la regla general de la prohibición de la prueba ilícita se convierta en excepción y las excepciones en regla general*[135]. Por ello, los Tribunales deberán acudir a la motivación determinada y al principio de proporcionalidad para conceder la eficacia a la prueba alcanzada de forma ilícita.

La prohibición de valoración referida anteriormente y citada como regla de exclusión, tiene su origen en la doctrina de la Corte Suprema de los Estados Unidos. Esta fue denominada inicialmente como *exclusionary rule*, y el Tribunal Constitucional español hace referencia a la misma para afirmar que, *en cuya virtud, en términos generales, no puede admitirse judicialmente el material probatorio obtenido con violación de la IV Enmienda a la Constitución*[136].

En lo que respecta al ordenamiento jurídico español, el uso de pruebas conculcando derechos fundamentales implica *per se* una vulneración del derecho a un proceso con todas las garantías. Asimismo, en segunda instancia, y únicamente cuando la sentencia condenatoria se sustente de manera exclusiva

---

[133] FUENTES SORIANO, O., *La prueba prohibida aportada por particulares a la luz de las nuevas tecnologías*. Derecho probatorio y otros estudios procesales. Liber amicorum Vicente Gimeno Sendra, ASENCIO MELLADO (Dir.), Castillo de Luna. Ediciones jurídicas, Madrid, 2020, p. 729.

[134] ASENCIO MELLADO, J. M., *Derecho procesal penal* (7ª edición), Tirant lo Blanch, 2015, p. 112.

[135] DELGADO DEL RINCÓN, L. E., *La regla de exclusión de la prueba ilícita, excepciones y eficacia*, Dialnet, 2013, p. 412.

[136] STC 114/1984, de 29 de noviembre, FJ 2.

en dicha prueba ilícita o en aquellas derivadas de esta, también se verá afectado el derecho a la presunción de inocencia[137], ambos recogidos en el art. 24.2 CE.

En este ámbito, CAMPANER MUÑOZ define de forma concisa la prueba directa afirmando ser *el resultado inmediato de la violación de un derecho fundamental*[138]. Esta definición es muy similar a la que ofrece LÓPEZ YAGÜES al diferenciar las pruebas irregulares de las ilícitas. Dicha autora afirma que las ilícitas *nacen de la infracción de un precepto constitucional que tutela un derecho fundamental*[139]. También añade que, aparte de considerarse nula, su falta de capacidad probatoria se hará extensiva a otras pruebas lícitas pero derivadas de las primeras y, en consecuencia, supondrá su inadmisión e imposible valoración.

Esta teoría lleva a la conclusión de que, como ya se citó en la sentencia de 14 de junio de 1960 del Tribunal Supremo Federal de Alemania (BGH), *no hay principio alguno del ordenamiento procesal penal que imponga la investigación de la verdad a cualquier precio*[140]. O como expone LÓPEZ YAGÜES, la tarea de buscar o averiguar la verdad *no puede desarrollarse sin límite a través de la práctica de actos o diligencias de investigación que, inevitablemente, implican la restricción de la esfera de derechos del sujeto investigado*[141].

3.1.2. Teoría de los frutos del árbol envenenado

La teoría de los frutos del árbol envenenado, también llamada indirecta o refleja, deriva de la doctrina norteamericana que la denominó originalmente "*the fruit of the poisonous tree doctrine*". Esta metáfora escenifica el fundamento de la teoría estableciendo que, si el árbol se encuentra envenenado, los frutos que emanen de éste también lo estarán. O como explica MARTÍNEZ RODRÍGUEZ, si el *resultado probatorio es ilegítimo y su nulidad insubsanable, arrastrará a todas aquellas otras pruebas relacionadas y derivadas*[142].

---

[137] STC 81/1998, de 2 de abril, FJ 3.

[138] CAMPANER MUÑOZ, J., *La confesión precedida de la obtención inconstitucional de fuentes de prueba*, Tesis Doctoral, Universidad Complutense de Madrid, Facultad de Derecho, 2015, p. 29.

[139] LÓPEZ YAGÜES, V., *El procedimiento probatorio y valoración de la prueba en el marco del proceso penal. Introducción al derecho procesal*, editado por ASENCIO MELLADO, J. M., y FUENTES SORIANO, O., Tirant lo Blanch, 2019, p. 266.

[140] Sentencia de 14 de junio de 1960 (BGHS 14, 358, 365).

[141] LOPEZ YAGÜES, V., *El procedimiento*…, Op. Cit., p. 265.

[142] MARTÍNEZ RODRÍGUEZ, J. A., *La doctrina del fruto del árbol envenenado*, Noticias Jurídicas, 31 de marzo de 2015, recuperado el 13 de mayo de 2025 de https://noticias.juridicas.com/conocimiento/articulos-doctrinales/8944-ladoctrina-del-fruto-del-arbol-envenenado/

De igual manera, MIRANDA ESTRAMPES sostiene que la prohibición de valoración debe extenderse *no sólo la prueba obtenida ilícitamente sino también a todas aquellas pruebas que aun obtenidas o practicadas de forma lícita tengan su origen en la primera*[143]. Así, la nulidad de la prueba obtenida de forma ilícita también deberá tener efectos de ineficacia sobre aquellas que, aún obtenidas lícitamente, provienen o toman su origen en informaciones alcanzadas a partir de una prueba viciada, suponiendo su inadmisibilidad pese a su presunta licitud.

Como sucedió anteriormente, CAMPANER MUÑOZ realiza una definición concisa sobre las pruebas derivadas o reflejas, considerándolas como *una prueba en sí misma lícita, pero que se apoya o deriva de otra obtenida de forma inconstitucional*. Y en este mismo sentido, FERNÁNDEZ ENTRALGO cita que *carecen de toda eficacia probatoria los actos que vulneren garantías constitucionales*[144]. Por consiguiente, la nulidad se hará extensiva a todas las pruebas que no se hubieran podido obtener sin la vulneración de derechos fundamentales sustantivos y, por tanto, fueran consecuencia necesaria de ella.

Además, a partir de esta teoría se deriva la exigencia de una *relación de causalidad directa e inmediata entre la ilicitud en la adquisición de la prueba y el resultado logrado a partir de aquella*[145], es decir, la prueba derivada o refleja[146]. Para ello se deberá probar que existe un nexo de conexión incuestionable con la diligencia probatoria viciada en origen.

Si bien, pocos años después se produjo una modificación significativa en referencia a esta última sentencia citada, pues el mismo Tribunal Constitucional, en su sentencia de 2 de abril de 1998, admitió como válidas las pruebas derivadas. En esta se reconocía la posibilidad de que el juzgador valorase dichas pruebas para fundamentar la correspondiente sentencia[147]. Además, añade que, en todo caso, para determinar la extensión de la prohibición de valoración de estas pruebas resulta necesario acreditar la existencia de un vínculo directo e indubitado con aquellas que vulneraron originariamente el derecho fundamental

[143] MIRANDA ESTRAMPES, M., SERRA DOMINGUEZ, M., *El concepto…*, Op. Cit., p. 113.
[144] FERNÁNDEZ ENTRALGO, J., *Las reglas del juego. Prohibición de hacer trampas: la prueba ilegítimamente obtenida*, Cuadernos de Derecho Judicial, C.G.P.J., Madrid, 1996, p. 167.
[145] ASENCIO MELLADO, J. M., FUENTES SORIANO, O., *Derecho…*, Op. Cit., p. 177.
[146] STC 85/1994, de 14 de marzo.
[147] STC 81/1998, de 2 de abril, FJ 4.

sustantivo. Al mismo tiempo, indica que *habrá que establecer un nexo entre unas y otras que permita afirmar que la ilegitimidad constitucional de las primeras se extiende también a las segundas*[148]*,* denominándolo conexión de antijuridicidad, el cual se tratará en el apartado siguiente.

En su caso, el Alto Tribunal en su sentencia núm. 113/2014 se pronuncia sobre las pruebas derivadas estableciendo como criterio general que la exclusión probatoria comprende no solo aquella evidencia obtenida mediante la vulneración de un derecho fundamental, sino también aquellas otras que, *habiéndose obtenido lícitamente, se basan, apoyan o deriven de la anterior, para asegurar que la prueba ilícita inicial no surte efecto alguno en el proceso*[149]*.* Es por lo que, este mismo Tribunal en su sentencia de 18 de abril de 2013, señala que sería incongruente invalidar la aplicación directa de los medios probatorios ilícitos cuando se tolera su utilización de forma derivada o refleja. Esta situación *vacía la norma de contenido efectivo, pues la utilización de procedimientos inconstitucionales acaba indirectamente surtiendo efecto*[150].

El momento que puede considerarse más significativo para la mencionada Teoría fue la sentencia del Tribunal Constitucional núm. 97/2019, puesto que introdujo una nueva doctrina totalmente contraria a la seguida desde 1984. Y, aunque reconoce que *la interdicción constitucional de la valoración judicial de la prueba ilícitamente obtenida constituye una garantía objetiva de nuestro sistema de derechos fundamentales, vinculada a la idea de un proceso justo*[151], el Tribunal realiza un cambio de criterio sobre la Teoría examinada. Éste establece la necesidad de realizar un *juicio ponderativo tendente a asegurar el equilibrio y la igualdad de las partes, esto es, la integridad del proceso en cuestión como proceso justo y equitativo*[152]. Dicho análisis debe determinar si la admisión y valoración de pruebas ilícitas supondría una vulneración de las garantías procesales del art. 24.2 CE.

En esta última sentencia, el Tribunal confirmó el fallo condenatorio emitido por el Tribunal Supremo en la sentencia núm. 116/2017, conocida como el "Caso

[148] ASENCIO MELLADO, J. M., FUENTES SORIANO, O., *Derecho… Op. Cit.*, p. 178.
[149] STS 113/2014, de 17 de febrero, FD 10.
[150] STS 301/2013, de 18 de abril, FD 21.
[151] ASENCIO MELLADO, J. M., FUENTES SORIANO, O., *Derecho…*, Op. Cit., p. 180.
[152] STC 97/2019, de 16 de julio, FJ 2.

Falciani". En concreto, se desestimó una posible vulneración a los derechos fundamentales, a la presunción de inocencia y a un proceso con todas las garantías del art. 24.2 CE. Los hechos examinados involucraban elementos probatorios obtenidos ilícitamente por un particular, empleado del banco suizo HSBC Private Bank Suisse. La peculiaridad del caso radicaba en que dicho particular había obtenido la fuente de prueba *con absoluta desconexión de toda actividad estatal y ajena en su origen a la voluntad de prefabricar pruebas*[153].

El Alto Tribunal aclaró que esto no implica eximir con carácter general a los particulares de la aplicación de la regla de exclusión probatoria. Por el contrario, propone una aplicación flexible de la regla *que permita, previa ponderación, adaptarse a las circunstancias e intereses de cada caso*[154].

En la ya referida sentencia núm. 116/2017, establece una clara distinción entre los sujetos implicados en la obtención de los elementos probatorios. Específicamente, determina que cuando intervienen particulares *lo determinante es que nunca, de forma directa o indirecta, haya actuado como una pieza camuflada del Estado al servicio de la investigación penal*. Y, para despejar cualquier atisbo de duda, aclara que los agentes de policía encargados de la investigación del delito deben tener plena conciencia de que su labor probatoria quedará igualmente excluida de valoración *si las pruebas obtenidas lo han sido mediante el subterfugio de la utilización de un activo particular que, sabiéndolo o no, actúa a su servicio*[155].

En definitiva, el análisis doctrinal y jurisprudencial realizado permite concluir que las pruebas digitales obtenidas por particulares, por ejemplo los correos electrónicos, mensajes instantáneos o grabaciones audiovisuales reseñados en el apartado segundo de este trabajo, podrán ser admitidas en el proceso penal pese a que, aun habiéndose producido durante su obtención vulneraciones a derechos fundamentales como la intimidad, el secreto de las comunicaciones o la inviolabilidad domiciliaria, concurran los tres presupuestos esenciales establecidos jurisprudencialmente que se detallan a continuación.

[153] STS 116/2017, de 23 de febrero, FD 6.
[154] FUENTES SORIANO, O., *La prueba prohibida*…, Op. Cit., p. 733.
[155] STS 116/2017, de 23 de febrero, FD 7.

En primer lugar, es necesario que la obtención de dichos elementos probatorios se haya producido con total independencia de cualquier actuación estatal. En segundo término, debe acreditarse que el particular no haya actuado como prolongación encubierta de los agentes policiales encargados de la investigación penal. Y, por último, resulta imprescindible que no exista intencionalidad dirigida a la prefabricación de pruebas para el proceso penal.

Se reconoce así que, aunque las pruebas tecnológicas obtenidas ilícitamente o sus derivadas deben excluirse del proceso penal, se aplica un criterio flexible cuando éstas son obtenidas por particulares que actúan de propia mano, es decir, sin vinculación alguna con el Estado, evitando que se excluyan de forma automática. En tales casos, se exige un análisis ponderado que valore las circunstancias concretas de cada caso y, por tanto, su posible vulneración de derechos fundamentales, especialmente los protegidos en los arts. 18 y 24.2 CE.

3.1.3. Teoría de la conexión de antijuridicidad

En la sentencia del Tribunal Constitucional núm. 81/1998, citada recientemente, se hace referencia expresa a la *conexión de antijuridicidad*. En dicha sentencia se establece que, aunque *las pruebas reflejas, desde un punto de vista intrínseco, son constitucionalmente legítimas*[156], para reconocer su eficacia refleja también resultará necesario evidenciar la existencia de una "conexión de causalidad" entre las pruebas ilícita y derivada lícita. Este se trata de un requisito necesario, pero no suficiente, puesto que además se exigirá la concurrencia de una "conexión de antijuridicidad", *que añadiría un plus necesario también y suficiente para que tal prueba fuera considerada prohibida*[157]. Su valoración dependerá de *la índole y características de la vulneración originaria del derecho fundamental, así como de su resultado, y de las necesidades esenciales de tutela del derecho fundamental afectado por la ilicitud*[158].

Lo tratado anteriormente ha sido catalogado por el Tribunal Constitucional como perspectivas interna y externa respectivamente, ambas complementarias. En una primera instancia, se deberá analizar desde un punto de vista interno si la inconstitucionalidad de la prueba ilícita inicial se transmite a la prueba derivada

---

[156] STC 81/1998, de 2 de abril, FJ 4.

[157] GONZÁLEZ MONTES, J. L., *La prueba ilícita*, Revista Persona y Derecho, núm. 54, 2006, p. 371.

[158] ARMENTA DEU, T., *La verdad en el filo de la navaja (nuevas tendencias en materia de prueba ilícita)*, Revista Ius et Praxis, núm. 2, 2013, p. 364.

comprometiendo el proceso penal, según la naturaleza, características y gravedad de la vulneración del derecho fundamental implicado. En este marco, el Tribunal deberá analizar inicialmente si dicha vulneración se utilizó instrumentalmente para obtener pruebas al margen del orden constitucional y, en ausencia de tal instrumentalidad, determinar si el uso procesal del material probatorio obtenido presenta una intensidad lesiva jurídicamente inadmisible por vulnerar el *núcleo axiológico más primordial de nuestro orden de derechos fundamentales*[159]. Y finalmente, desde una perspectiva externa, considerar las necesidades de tutela esenciales que exige la realidad y efectividad del derecho fundamental protegido, de modo que excluir estas infracciones del ámbito sancionador podría generar un efecto que incentive su comisión. Para evitar tal contradicción, se pretende que la actuación de los funcionarios encargados de la investigación penal durante la obtención de la prueba no sea intencionalmente deliberada ni el resultado de una negligencia grave. Tal enfoque guarda cierta analogía con el efecto disuasorio y la excepción de buena fe del ordenamiento jurídico estadounidense[160].

Dicho de otro modo, COSTA TORNÉ aclara que para conocer si media conexión de antijuridicidad entre ambas pruebas será preciso analizar si la existencia de la prueba derivada depende de que preexista la primera, la prueba ilícita, y solo en el caso de que se considere una condición *sine qua non* concurrirá la nombrada conexión de antijuridicidad. De no ser así, si la prueba derivada carece de dependencia causal respecto de la prueba ilícita, *se puede admitir y valorar como prueba en el proceso al no depender de la existencia de esta y no estar contaminada por su ilicitud*[161].

Por otra parte, ARRABAL PLATERO expone una doble dimensión de la conexión de ilicitud entre la prueba ilícita inicial y la prueba derivada, pudiendo analizarse desde dos perspectivas complementarias, la natural y la jurídica[162]. En primer lugar, desde un enfoque natural, la autora establece que la nulidad se extiende a aquellas pruebas que son consecuencia material directa de un acto

[159] STC 97/2019, de 16 de julio, FJ 3.
[160] GONZÁLEZ MONTES, J. L., *La prueba ilícita*…, Op. Cit., p. 371.
[161] COSTA TORNÉ, M. C., *La prueba ilícita*…, Op. Cit., p. 145.
[162] ARRABAL PLATERO, P., *La prueba*…, Op. Cit., p. 85.

vulnerador inicial. Esto se refiere concretamente a la relación causa-efecto directa entre la prueba ilícita y las obtenidas posteriormente de forma legal, es decir, aquellas pruebas que surgen directamente de una primera prueba obtenida ilícitamente. En segundo lugar, la perspectiva jurídica trasciende de una relación material, considerándola nula por vulnerar derechos fundamentales. En esta ocasión es indiferente si existe una conexión directa o no entre la prueba ilícita y la derivada, simplemente es suficiente con que la prueba vulnere derechos fundamentales como los recogidos en el art. 18 CE, incluso cuando la investigación penal se vea perjudicada.

Volviendo a la sentencia del Tribunal Constitucional del 2 de abril de 1998, se especifica que para llegar a la apreciación de que la prohibición de valoración de las pruebas ilícitas se hace extensiva del mismo modo a las pruebas derivadas, *habrá de precisarse que se hallan vinculadas a las que vulneraron el derecho fundamental sustantivo de modo directo*[163]*.* Dicho de otro modo, será necesario establecer un nexo que reconozca que la ilegitimidad constitucional de las obtenidas en primera instancia se transpone de igual forma a las segundas.

MIRANDA ESTRAMPES participa que la teoría analizada *reformula el fundamento de la regla de exclusión de nuestro ordenamiento jurídico*[164]. Destaca que el efecto disuasorio, denominado por la jurisprudencia norteamericana como *deterrent effect*, se erige como núcleo central de aplicación de la regla de exclusión[165]. En el sistema estadounidense, este efecto se entiende principalmente como un instrumento para disuadir a los agentes de policía de cometer futuras vulneraciones de derechos, ya que la información obtenida sería inadmisible para sustentar una condena contra el investigado.

Como indica CUADRADO SALINAS, esto supone una *llamada de atención a la policía, disuadiéndole de repetir en el futuro conductas no apropiadas o ilícitas privándoles de los frutos de su ilícita actuación*[166]. Para ello se requerirá efectuar un análisis coste-beneficio donde el valor disuasorio prevalezca sobre los elevados costes de excluir la prueba. Este criterio únicamente será de

[163] STC 81/1998, de 2 de abril, FJ 4.

[164] MIRANDA ESTRAMPES, M., SERRA DOMINGUEZ, M., *El concepto…*, Op. Cit., p. 131.

[165] MIRANDA ESTRAMPES, M., *La prueba ilícita…*, Op. Cit., p. 137.

[166] CUADRADO SALINAS, C., *Fundamento y efectos de la exclusión de la prueba obtenida con vulneración de derechos fundamentales*, Valencia, Tirant lo Blanch, 2021, p. 40.

aplicación ante comportamientos en los que la *policía muestre un desprecio "deliberado", "imprudente" o "gravemente negligente*"[167].

En cambio, en la jurisprudencia se presenta como un elemento integrante de la necesaria tutela de los derechos fundamentales. El Tribunal Constitucional lo configura como un efecto disuasorio inverso, vinculando la protección de los derechos con la exclusión de las pruebas obtenidas ilícitamente. De esta forma evita crear incentivos perversos para futuras vulneraciones y, otorgando a la regla de exclusión una función esencialmente protectora de los derechos fundamentales [168]. Este mismo órgano jurisdiccional ha fundamentado la exclusión de la prueba ilícita en su efecto disuasorio, y *que para el aparato oficial del Estado representa tener plena conciencia de que nunca podrá valerse de pruebas obtenidas con vulneración de las reglas constitucionales en juego*[169].

Si bien, en el ordenamiento jurídico español, a diferencia del sistema norteamericano que ha establecido excepciones taxativas a la exclusión de pruebas derivadas de actuaciones ilícitas, ha optado por una concepción flexible de la conexión de antijuridicidad, operando como un criterio abierto que permite valorar caso por caso la extensión de la ilicitud probatoria. La amplia discrecionalidad que disponen los Tribunales españoles *ha introducido, en la práctica, una excesiva dosis de incertidumbre e inseguridad jurídica* [170], cuestionando el carácter absoluto de la eficacia refleja.

Entre las excepciones desarrolladas por la jurisprudencia española, influenciadas por el modelo norteamericano pero con fundamentos distintos, según los autores ARRABAL PLATERO [171] y MIRANDA ESTRAMPES [172] encontramos el descubrimiento inevitable, que autoriza la valoración de la prueba derivada cuando el hallazgo se hubiera producido igualmente por medios lícitos; el hallazgo casual, aplicable a pruebas obtenidas accidentalmente en investigaciones legítimas; la buena fe de los agentes, que exime de exclusión

---

[167] CARRILLO DEL TESO, A. E., *La prueba prohibida aportada por particulares al proceso penal: la evolución en el TS, Proceso y prueba prohibida* (1ª edición), editado por ROCA MARTÍNEZ, J. M. y NIETO MORALES, C., Dykinson, 2022, p. 174.

[168] STC 81/1998, de 2 de abril, FJ 6.

[169] STS 287/2017, de 19 de abril, FD 2.

[170] MIRANDA ESTRAMPES, M., SERRA DOMINGUEZ, M., *El concepto…*, Op. Cit., p. 133.

[171] ARRABAL PLATERO, P., *La prueba…*, Op. Cit., pp. 80-102.

[172] MIRANDA ESTRAMPES, M., *La prueba ilícita…*, Op. Cit., pp. 142-148.

cuando la vulneración de derechos fundamentales ha sido involuntaria y ajustada al ordenamiento; el nexo causal atenuado, que admite pruebas derivadas si la conexión con la ilicitud original es remota o no afecta gravemente al derecho vulnerado; y la confesión voluntaria del inculpado, que rompe el vínculo con la prueba ilícita previa cuando medie una información adecuada y ausencia de coacción. Estas excepciones, que no van a ser objeto de desarrollo en el presente trabajo, han sido introducidas por parte de los Tribunales españoles de forma paulatina y reiterada, pero sin haber sido reguladas expresamente.

En síntesis, la conexión de antijuridicidad exigida por el Tribunal Constitucional opera como un requisito necesario para extender la ilicitud de la prueba originaria a la derivada lícita, pero su aplicación se circunscribe a contextos específicos. Mientras que el *deterrent effect* del derecho estadounidense se articula como una herramienta disuasoria dirigida exclusivamente a conductas policiales, excluyendo por tanto las actuaciones de particulares en la obtención de pruebas digitales, su transposición al ámbito ajeno al estatal requiere un análisis diferenciado. En este sentido, la valoración de la ilicitud debe incorporar un examen coste-beneficio que, en el caso de pruebas obtenidas por particulares, pondere la gravedad de la vulneración del derecho fundamental frente a la necesidad de preservar la eficacia del proceso penal del art. 24.2 CE. Este equilibrio se aleja de la lógica del *deterrent effect* clásico, ya que no persigue corregir conductas estatales, sino evitar que la admisión de pruebas viciadas incentive vulneraciones futuras por cualquier actor, incluso privados. Así, la conexión de antijuridicidad actúa como filtro para excluir solo aquellas pruebas derivadas cuya dependencia causal con la ilicitud originaria suponga un menoscabo intolerable de las garantías constitucionales.

3.2. Derechos fundamentales susceptibles de afectación por una prueba tecnológica

Como se ha indicado anteriormente, y así también se cita en el Auto de 18 de junio de 1992 de la Sala de lo Penal del Tribunal Supremo, referido al caso Naseiro, *no existe norma alguna en el proceso penal que autorice la averiguación de la verdad a cualquier precio*[173], y que ASENCIO MELLADO Y LÓPEZ

[173] ATS 3773/1992 (Sala Segunda, de lo Penal), de 18 de junio.

YAGÜES explican claramente afirmando que *no todo es lícito en la investigación, ni todo puede justificarse por un pretendido interés general o por causa de la necesidad de mantener la paz social*[174]. En este mismo sentido, RUÍZ VADILLO matiza que, en contraposición a otros ámbitos jurisdiccionales donde prima la verdad formal o aparencial, *la verdad material o verdad histórica que, en principio, se pretende obtener en el proceso penal […] sólo puede alcanzarse dentro de las exigencias, presupuestos y limitaciones establecidos en el Ordenamiento jurídico*[175].

El descubrimiento de la verdad procesal no constituye un fin absoluto que justifique cualquier medio, sino que se encuentra delimitado por el respeto irrenunciable a los derechos fundamentales sustantivos, ya que como indica el Tribunal Constitucional, la posición preferente de éstos deriva de su condición de "inviolables"[176]. Únicamente aquellos métodos probatorios que preserven la esencia garantista del Estado de Derecho y resulten constitucionalmente admisibles podrán considerarse legítimos en la actividad probatoria.

En su sentencia núm. 25/1981, el Tribunal Constitucional establece que los derechos fundamentales tienen una doble naturaleza. Por un lado, son derechos subjetivos que *garantizan un status jurídico o la libertad en un ámbito de la existencia*. Por otro, funcionan como elementos esenciales del ordenamiento jurídico, garantizando una *convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado social de Derecho o el Estado social y democrático de Derecho*[177], fórmula definida en el art. 1.1 CE[178].

---

[174] ASENCIO MELLADO, J. M., y LÓPEZ YAGÜES, V., *Los derechos fundamentales en el proceso penal, Los límites de la investigación penal,* editado por ASENCIO MELLADO, J. M. y FUENTES SORIANO, O., *Derecho procesal penal* (3ª edición), Tirant lo Blanch, 2024, p. 165.

[175] RUIZ VADILLO, E., *Tribunal Supremo declara nulas pruebas 18/06/1992*, recuperado el 17 de mayo de 2025 https://www.losgenoveses.net/Asuntillos/casonaseiro/14.%20Caso%20Naseiro.%20Tribunal%20Supremo.%20Declara%20nulas%20pruebas.18.06.92.pdf

[176] STC 49/1999, de 5 de abril, FJ 12.

[177] STC 25/1981, de 14 de julio, FJ 5.

[178] Artículo 1, apartado primero, de la Constitución Española, dispone que "*1. España se constituye en un Estado social y democrático de Derecho, que propugna como valores superiores de su ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político*".

Al mismo tiempo, tales derechos fundamentales trascienden el ámbito de las relaciones entre los ciudadanos y los poderes públicos estatales, proyectándose igualmente en las relaciones entre particulares. En este mismo sentido lo establece el Tribunal Constitucional en su jurisprudencia, que al interpretar el art. 9.3 CE señala que esta concreción normativa constitucional no puede entenderse en el sentido de que *sólo se sea titular de los derechos fundamentales y libertades públicas en relación con los poderes públicos*. En el contexto de un Estado social y democrático de derecho, como el definido anteriormente, resulta jurídicamente insostenible afirmar que *el titular de tales derechos no lo sea en la vida social*[179].

Como consecuencia de que durante la obtención de fuentes de prueba para el descubrimiento de la verdad procesal se produzca una afectación de los derechos fundamentales podrá significar la ilicitud de éstas y, por ende, su inadmisión en el proceso. Por ello, resulta indispensable realizar un análisis de los derechos fundamentales que amparan a los ciudadanos para evaluar si el empleo de nuevos métodos de obtención de pruebas tecnológicas puede implicar un perjuicio desproporcionado de éstos, generando un conflicto latente entre la eficacia de la investigación y las garantías constitucionales.

Como refiere VELASCO NÚÑEZ en cuanto a los derechos afectados en la investigación penal tecnológica, *lo normal es que la investigación sobre o con medios tecnológicos afecte principalmente a ese conjunto de derechos fundamentales que englobamos bajo la denominación del derecho a nuestra vida privada*[180]. Este derecho es recogido por el art. 8.1 CEDH, en el que indica que *toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*[181]. En nuestro ordenamiento jurídico dicha intromisión tecnológica en la privacidad se protege mediante los derechos y libertades fundamentales del art. 18 CE que se desarrollan a continuación.

---

[179] STC 18/1984, de 7 de febrero, FJ 6.

[180] VELASCO NÚÑEZ, E., *Investigación*…, Op. Cit., p. 4.

[181] Artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente, ratificado por España el 4 de octubre de 1979, publicado en BOE núm. 243, p. 23565, recuperado de https://www.boe.es/eli/es/ai/1950/11/04/(1)

3.2.1. Derecho a la intimidad personal y familiar

En sus orígenes, el derecho tan solo ejercía su tutela frente a meras agresiones materiales contra la vida y la propiedad y, particularmente mediante la defensa de acciones por agresión violenta, con fuerza o con armas, conocido como *trespass vi et armis*. Según WARREN y BRANDEIS, el derecho a la vida únicamente protegía a la persona contra lesiones corporales. Por ejemplo, la libertad era entendida como la ausencia de restricción física, y el derecho de propiedad garantizaba las tierras y el ganado. Posteriormente, se reconoció la dimensión espiritual del ser humano, sus sentimientos e intelecto[182].

En el ámbito internacional, el derecho a la intimidad se encuentra reconocido en la Declaración Universal de Derechos Humanos. Este documento se constituye como *un ideal común para todos los pueblos y naciones*, siendo en su art. 12 DUDH en el que se dispone que *nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación*[183].

Y en relación con la DUDH, el art. 10.2 CE expone que *las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos*[184]. Esta disposición constitucional evidencia la voluntad del poder constituyente de otorgar a este instrumento un papel preeminente en nuestro sistema de garantías constitucionales.

Desde el punto de vista europeo, el derecho fundamental a la intimidad personal y familiar es reconocido en el art. 8 CEDH citado con anterioridad, así como a nivel nacional en el art. 18.1 CE, siendo en este último donde *se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*[185]. Conviene precisar que, pese a que en el presente apartado no se va a valorar en profundidad el derecho al honor ni a la propia imagen, resulta necesario realizar algunas precisiones conceptuales.

---

[182] WARREN, S. D., y BRANDEIS, L. D., *The Right to Privacy*, Harvard Law Review, Vol. IV, núm. 5, 15 de diciembre de 1890, recuperado de https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[183] Artículo 12 de la Declaración Universal de los Derechos Humanos, Resolución 217 A (III), proclamada por la Asamblea General de las Naciones Unidas, París, 10 de diciembre de 1948.

[184] Artículo 10, apartado segundo, de la Constitución Española.

[185] Artículo 18, apartado primero, de la Constitución Española.

Inicialmente el derecho a la propia imagen fue considerado como parte del derecho a la intimidad. Sin embargo, MARTÍNEZ OTERO aclara que *hoy es aceptado unánimemente como un derecho fundamental dotado de sustantividad propia*[186]. En este sentido el Tribunal Constitucional estableció en su sentencia núm. 139/2001 que, aunque se haya puesto de manifiesto la vinculación del derecho a la propia imagen con el derecho al honor y a la intimidad, también ha manifestado que *se trata de un derecho constitucional autónomo que dispone de un ámbito específico de protección*[187].

En el art. 1.3 de la Ley Orgánica 1/1982 se indica que el derecho al honor, a la intimidad personal y familiar y a la propia imagen es *irrenunciable, inalienable e imprescriptible*[188]. Concretamente, es un derecho personalísimo sólo previsto para las personas físicas, el cual se extingue con el fallecimiento[189]. Por lo tanto, también se hace extensible a extranjeros, en cambio, quedan excluidas las personas jurídicas por no ser titulares de vida personal o familiar[190].

A continuación, se va a tratar de forma individualizada el derecho a la intimidad. Según DÍEZ-PICAZO, el valor o bien jurídico protegido es un *ámbito propio y reservado de las personas […] que ha de quedar oculto a la mirada curiosa de los demás*[191]*, y cuya efectiva existencia es necesaria para alcanzar una calidad mínima de vida humana*, palabras que extrae de la sentencia de 2 de diciembre de 1988 del Tribunal Constitucional[192].

De esta premisa surge la problemática de delimitar con precisión el ámbito de la esfera privada a fin de establecer qué conductas han de considerarse como una intromisión ilícita a la intimidad personal. ZOCO ZABALA refiere que debe ser el propio titular el que establece tal delimitación puesto que, *lo que para una persona puede ser susceptible de la reserva más extrema, para otra puede ser un orgullo su conocimiento*[193]. Sin embargo, la jurisprudencia constitucional

---

[186] MARTÍNEZ OTERO, J. M., *Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento*, Revista Española de Derecho Constitucional, núm. 106, 2016, p. 123.

[187] STC 139/2001, de 18 de junio, FJ 4.

[188] Artículo 1, apartado tercero, de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[189] ARRABAL PLATERO, P., *La prueba…*, Op. Cit., p. 121.

[190] ATC 257/1985, de 17 de abril, FJ 2.

[191] DÍEZ-PICAZO, L. M., *Sistema de derechos fundamentales* (5ª edición), Tirant lo Blanch, 2021, p. 284.

[192] STC 231/1988, de 2 de diciembre, FJ 3.

[193] ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, Cizur, Navarra, 2015, p. 99.

citada en el presente párrafo ha optado por aplicar un criterio fundamentalmente material en la delimitación de la esfera privada. Este enfoque implica que según las *pautas sociales integrantes suele considerarse ajeno al legítimo interés de los demás*, esto es, *su extensión será tendencialmente la misma para todos*[194].

Este mismo órgano constitucional, en su sentencia núm. 115/2000, precisa que este derecho tiene como finalidad esencial *garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona, recogido en el art. 10.1 CE,* frente a cualquier intromisión, ya sea de poderes públicos o de particulares[195].

Como consecuencia, este derecho fundamental otorga a su titular la facultad de proteger ese espacio reservado, tanto individual como familiar, frente a intromisiones externas. Garantiza así la no divulgación de dicho ámbito privado por parte de terceros y evita su exposición pública no consentida. LEFEBVRE conceptualiza este derecho, en un lenguaje coloquial pero ilustrativo, como *el derecho a ser dejado en paz*[196]. Esta concepción tiene especial relación con la expresión *the right to be let alone*[197] de WARREN y BRANDEIS, que viene a significar, *el derecho a estar sólo,* siendo ésta una de las primeras definiciones esbozadas para el derecho a la intimidad.

Con la llegada de la era digital y la generalización del uso cotidiano de las TIC, se ha redefinido el concepto de intimidad personal, quedando expuesta a nuevas formas de vulneración. Un ejemplo sería el acceso a la información que contienen los dispositivos electrónicos personales, donde la información privada es vulnerable a potenciales intromisiones ajenas. La sentencia núm. 173/2011 del Tribunal Constitucional reconoce que la gran cantidad de datos sobre la vida privada y profesional almacenados en un ordenador personal no solo pertenecen al ámbito privado*, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano*[198].

---

[194] HUERTA NOVOA, M., *El derecho a la intimidad: regulación legal y desarrollo, Real Academia Asturiana de Jurisprudencia*, (s. f.), p. 11.

[195] STC 115/2000, de 10 de mayo, FJ 4.

[196] LEFEBVRE, F., *Derecho de las Nuevas Tecnologías*, Memento Práctico, Écija, 2017-2018, p. 337.

[197] WARREN, S. D., y BRANDEIS, L. D., *The Right*…, Op. Cit.

[198] STC 173/2011, de 7 de noviembre, FJ 3.

Otras sentencias relevantes incluyen la núm. 92/2023 del mismo Tribunal, que estableció la vulneración al derecho a la intimidad personal por parte de las Fuerzas y Cuerpos de Seguridad por la instalación de dispositivos de grabación de imágenes en un garaje comunitario[199]. Asimismo, la sentencia núm. 278/2021 del Tribunal Supremo consideró intromisión ilegítima la colocación de un dispositivo de localización y seguimiento mediante tecnología GPS en el automóvil del demandante[200].

En este sentido, la citada Ley Orgánica 1/1982, en su art. 7 LOHIP, hace referencia a la intromisión ilegítima del derecho tratado. Se entiende como tal la instalación no consentida de dispositivos de grabación o vigilancia en espacios privados, el uso de estos medios para captar, registrar o reproducir manifestaciones íntimas o comunicaciones privadas no destinadas al interceptor, la difusión pública de datos sobre la vida privada o documentos personales que afecten al honor, y la captación, reproducción o publicación no consentida de imágenes en contextos privados, salvo las excepciones legalmente previstas [201].

En definitiva, no habrá vulneración alguna al derecho a la intimidad cuando, por ejemplo, una de las partes intervinientes solicite que se admita como medio probatorio las conversaciones mantenidas entre ambos interlocutores de dicha conversación, ya sea por correo electrónico o teléfono móvil. Al aportarse voluntariamente por una de las partes implicadas, dichos contenidos adquirirán carácter público[202]. En correspondencia con esto se manifiesta el Tribunal Constitucional en su sentencia núm. 114/1984, concluyendo que *no constituye contravención alguna del secreto de las comunicaciones la conducta del interlocutor en la conversación que graba ésta, que graba también, por lo tanto, sus propias manifestaciones personales*[203].

Como conclusión, cabe analizar la intimidad como objeto jurídico de tutela penal en el actual Código Penal, puesto que la misma se encuentra amparada en el art. 197.1 CP. Este precepto establece textualmente que *el que, para*

[199] STC 92/2023, de 11 de septiembre.

[200] STS 278/2021, de 10 de mayo.

[201] Artículo 1, apartado tercero, de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[202] GONZÁLEZ I JIMÉNEZ, A., *Las diligencias policiales y su valor probatorio*, BOSCH, 2014, pp. 241- 242.

[203] STC 114/1984, de 9 de noviembre, FJ 8.

descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación[204].

El tipo penal citado presenta dos requisitos esenciales. En primer lugar, la ausencia de consentimiento por parte cualquiera de los interlocutores de la comunicación. En segundo término, la apropiación intencional del contenido, sin que se requiera el efectivo conocimiento de los datos contenidos en la misma. Esto es, *basta poner en peligro el referido bien jurídico con independencia que posteriormente el sujeto no llegue a la toma de conocimiento de datos íntimos*[205].

3.2.2. Derecho a la inviolabilidad del domicilio

El derecho a la inviolabilidad domiciliaria, igualmente que el derecho a la intimidad, viene recogido tanto en el art. 8 CEDH y art. 12 DUDH citados, como en el art.18.2 CE. En este último se establece de forma clara y concisa que el *domicilio es inviolable*, añadiendo que *ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo flagrante delito*[206].

Dicho derecho constituye un derecho fundamental de carácter esencialmente personal, orientado a la protección de la vida privada de la persona[207] desarrollada en el espacio denominado comúnmente como domicilio. Su concepto y protección constitucional se hallan regulados en dos normas fundamentales dentro de nuestro ordenamiento jurídico.

La primera de ellas, la LECrim, cuyo capítulo I se encarga de regular el procedimiento de entrada y registro en lugar cerrado. Si bien, dicho procedimiento no es de interés para el presente TFG, hay algunos conceptos recogidos en su articulado que deben ser abordados. Por ejemplo, el art. 545 LECrim establece que *nadie podrá entrar en el domicilio de un español o extranjero residente en España sin su consentimiento, excepto en los casos y en la forma expresamente previstos en las leyes*[208]. Por su parte, en el art. 554

[204] Artículo 197, apartado primero, de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
[205] HUERTA NOVOA, M., *El derecho…*, Op. Cit., pp. 7-8.
[206] Artículo 18, apartado segundo, de la Constitución Española.
[207] STC 94/1999, de 31 de mayo.
[208] Artículo 545 de la Ley de Enjuiciamiento Criminal.

LECrim se enumera todo aquel lugar cerrado que se reputa como domicilio. En concreto, en su apartado segundo, como el *edificio o lugar cerrado, o la parte de él destinada principalmente a la habitación de cualquier español o extranjero residente en España y de su familia*[209]; y en su apartado cuarto define como domicilio de personas jurídicas aquel *espacio físico que constituya el centro de dirección de las mismas, ya se trate de su domicilio social o de un establecimiento dependiente, o aquellos otros lugares en que se custodien documentos u otros soportes de su vida diaria que quedan reservados al conocimiento de terceros*[210].

En cuanto a la segunda norma que regula dicho término es el Código Penal que, en su capítulo II referente a los robos, conceptualiza el domicilio bajo la denominación de "casa habitada", y en particular en el art. 241.1 CP. Asimismo, en el apartado segundo del mismo artículo *se considera casa habitada todo albergue que constituya morada de una o más personas, aunque accidentalmente se encuentren ausentes*[211]. De ello se deduce que la condición de casa habitada no se extingue por la ausencia accidental de sus moradores, por lo que la residencia permanente no constituye un requisito indispensable para dicha calificación jurídica. Además, la consideración de casa habitada también se hace extensible, según el art. 241.3 CP, a *sus patios, garajes y demás departamentos o sitios cercados y contiguos al edificio y en comunicación interior con él, y con el cual formen una unidad física*[212].

En este mismo sentido, el Tribunal Constitucional, en su sentencia de 17 de octubre de 1985, afirma que la inviolabilidad del domicilio *constituye un auténtico derecho fundamental de la persona*, establecido para proteger el ámbito privativo de la misma dentro del espacio delimitado por su elección. Este debe caracterizarse precisamente por su inmunidad frente a intromisiones o agresiones externas, ya sean de particulares o de autoridades públicas.

Una perspectiva similar es la que realiza ARAGÓN REYES, concretando que lo protegido por la inviolabilidad domiciliaria es *la seguridad de un ámbito*

[209] Artículo 554, apartado segundo, de la Ley de Enjuiciamiento Criminal.
[210] Artículo 554, apartado cuarto, de la Ley de Enjuiciamiento Criminal.
[211] Artículo 241, apartado segundo, del Código Penal.
[212] Artículo 241, apartado tercero, del Código Penal.

físico inmune a la entrada no querida de otros[213]. Volviendo a lo referido por el Tribunal Constitucional, amplía el concepto citando que se trata de un *espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima*, por lo que, no solo se protege el espacio físico como tal, sino *lo que en él hay de emanación de la persona y de esfera privada de ella*[214]. En esta línea, GONZÁLEZ-TREVIJANO SÁNCHEZ, matiza la diferenciación conceptual entre intimidad y vida privada, estableciendo que *la intimidad se manifiesta como la parte o núcleo más "privado" de la vida privada*"[215].

Si bien, como refiere ESPÍN TEMPLADO, tanto coloquialmente como en el lenguaje jurídico, los conceptos intimidad y vida privada se emplean usualmente como sinónimos, si bien, en la Carta Magna tan solo se hace mención expresa del derecho a la intimidad en su art. 18 CE. Este artículo entiende que el conjunto de derechos protegidos por el mismo salvaguarda un bien constitucional más amplio, la vida privada. Por ello, *intimidad y vida privada habrían de contemplarse como la parte y el todo, en el sentido de que la intimidad constituiría el núcleo de la vida privada, esto es, su parte más esencial y característica*[216].

Por su parte, CABEZUDO BAJO realiza una apreciación del concepto de domicilio en la que deben cumplirse dos requisitos para que se entienda que en éste se desarrolla el derecho a la vida privada de la persona citado anteriormente por el Tribunal Constitucional. El primero de ellos, desde una perspectiva objetiva, deberá constituirse como un espacio idóneo para el desarrollo de los mencionados derechos fundamentales. Mientras que al mismo tiempo y, desde un enfoque subjetivo, deberá haber sido expresamente destinada por su titular para el desarrollo de tales derechos[217].

---

[213] ARAGÓN REYES, M., *La inviolabilidad del domicilio*, Revista Española de Derecho Constitucional, 1998, p. 352.

[214] STC 137/1985, de 17 de octubre, FJ 2.

[215] GONZÁLEZ-TREVIJANO SÁNCHEZ, P.J., *La inviolabilidad del domicilio*, Tecnos, Madrid, 1992, p. 130.

[216] ESPÍN TEMPLADO, E., *Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio*, Revista del Centro de Estudios Constitucionales, núm. 8, 1991, p. 44

[217] CABEZUDO BAJO, M.J., *La inviolabilidad del domicilio y el proceso penal* (1ª edición), Iustel Publicaciones, 2004, p. 119.

Como se mencionó respecto al art. 241.2 CP, la concepción de domicilio protegida por el art. 18.2 CE no se limita exclusivamente al lugar de residencia habitual y permanente de las personas, sino que comprende todo aquel lugar cerrado en el que se lleve a cabo cualquier actividad privada, con clara intención de excluir de él a terceros. Por tanto, se protege *cualquier espacio físico cerrado en el que se despliega el ámbito de privacidad de las personas, con independencia de que tenga carácter habitual, permanente o estable, o, transitorio, temporal o accidental*[218].

Sobre la base de lo anterior, el Tribunal puntualiza que será irrelevante la *intensidad, periodicidad o habitualidad* del uso privado que se haga del domicilio si, según su *situación, destino natural, configuración física u objetos* hallado en éste, pueda deducirse el *efectivo desarrollo de la vida privada en el mismo*[219]. Y en relación con esto, también especifica que no solo se considera como tal el lugar donde se pernocta con habitualidad o donde se llevan a cabo otras actividades cotidianas habituales*, sino también el ámbito cerrado erigido por una persona con objeto de desarrollar en él alguna actividad*[220].

Hasta este punto se puede evidenciar la ausencia de cualquier mención al derecho de propiedad y es que, pese a que entre ambos derechos puedan hallarse algunas vinculaciones, sus contenidos difieren sustancialmente como revela MATÍA PORTILLA. Esta autora afirma que la inviolabilidad del domicilio puede ser *vulnerada sin que se ponga en peligro necesariamente la propiedad del bien*, esto quiere decir que quizá el titular del derecho a la inviolabilidad domiciliaria no sea el propietario del mismo[221].

Por otra parte, la jurisprudencia ha asimilado al domicilio diferentes espacios en el caso de hacer un uso efectivo de éstos como morada y, por ende, extendiendo a los mismos la correspondiente protección constitucional. Entre estos se incluyen las habitaciones de hotel o similares[222], chabolas o tiendas de

[218] STC 10/2002, de 17 de enero, FJ 4.
[219] STC 10/2002, de 17 de enero, FJ 6.
[220] STS 538/1996, 11 de julio, FD 2.
[221] MATÍA PORTILLA, F. J., *El derecho fundamental a la inviolabilidad del domicilio*, McGraw-Hill Interamericana de España, Madrid, 1997, p. 15.
[222] STC 10/2002, de 17 de enero, FJ 4.

campaña[223], roulottes o autocaravanas[224], camarotes de embarcaciones[225], lavabos, baños o aseos de los establecimientos públicos[226], la rebotica de una farmacia[227], los locales de reunión[228], o la habitación de una residencia militar[229].

Respecto a los sujetos titulares del derecho tratado, cabe señalar que no todo espacio sobre cuyo acceso se ostente el poder de disposición ha de ser considerado domicilio protegido por el art. 18.2 CE. Según dispone el Tribunal Constitucional, el fundamento que justifica esta delimitación conceptual reside en que el derecho fundamental en cuestión no debe asimilarse a la *protección de la propiedad de los inmuebles ni de otras titularidades reales u obligacionales relativas a dichos bienes que puedan otorgar una facultad de exclusión de los terceros.* Asimismo, el derecho a la inviolabilidad del domicilio no queda restringido exclusivamente a las personas físicas, siendo *extensivo o predicable igualmente de las personas jurídicas*[230].

3.2.3. Derecho al secreto de las comunicaciones

El derecho al secreto de las comunicaciones, igualmente que el anterior derecho tratado, viene recogido tanto en el art. 8 CEDH reseñado, como en el art. 18.3 CE. En este último *se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*[231]. En su redacción se haya la primera diferencia sustantiva respecto al derecho a la intimidad, el requisito de resolución judicial que indica la propia Carta Magna.

Como ha señalado la jurisprudencia, esta decisión corresponde única y exclusivamente al Poder Judicial. En concreto, es el Juez de Instrucción quien debe valorar y equilibrar los intereses implicados *mediante un juicio acerca de la proporcionalidad y necesidad de la medida, el cual deberá expresarse en una resolución judicial motivada*[232]. Por lo tanto, es evidente que toda interceptación

---

[223] STS 1448/2005, de 18 de noviembre, FJ 3.
[224] STS 84/2001, de 29 de enero, FD 2.
[225] STS 624/2002, 10 de abril, FD 3.
[226] STS 937/1998, 7 de julio, FJ 6.
[227] STS 576/2002, 3 de septiembre, FD 11.
[228] STS 538/1996, 11 de julio, FD 2.
[229] STC 189/2004, de 2 de noviembre, FJ 2.
[230] STC 69/1999, de 26 de abril, FJ 2.
[231] Artículo 18, apartado tercero, de la Constitución Española.
[232] STS 171/2015, de 19 de mayo, FJ 3.

admisible de éstas reviste carácter excepcional y se encuentra sujeta a estrictos límites, requisitos y garantías, por tratarse de una medida que afecta a un derecho fundamental, *y solo el cumplimiento de esos requisitos y garantías permitirá que esa afectación no se convierta en vulneración*[233].

La sentencia núm. 16/2014 del Alto Tribunal establece que el bien jurídico protegido constitucionalmente mediante la garantía del secreto de las comunicaciones es la libertad comunicativa en su dimensión esencial, *siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto mediante la aprehensión física del soporte del mensaje, […], como por el simple conocimiento antijurídico de lo comunicado mediante apertura de la correspondencia ajena*. Además, añade que el concepto de secreto protege tanto el contenido de la comunicación, como la *identidad subjetiva de los interlocutores o de los corresponsales*[234].

De ello se infiere que la tutela jurídica se hace extensiva en partes iguales a ambos comunicantes, tanto a los emisores como a los receptores de la misma, siendo condición necesaria la efectiva realización del acto comunicativo para que pueda invocarse dicho derecho. Esta característica le distingue del derecho a la intimidad puesto que para su vulneración no presupone necesariamente interacción comunicativa alguna. En este mismo sentido, el Tribunal Constitucional, en su sentencia de 7 de noviembre de 2013, afirma que *el objeto directo de protección del art. 18.3 CE es el proceso de comunicación en libertad y no por sí solo el mensaje transmitido, cuyo contenido puede ser banal o de notorio interés público*[235].

En cuanto a la titularidad de este derecho, indica DÍAZ REVORIO que se trata *de un derecho de la esfera privada, vinculado directamente a la dignidad humana*, por lo que la misma corresponde universalmente a toda persona, con independencia de su nacionalidad, por lo que resulta inadmisible establecer excepciones, restricciones o limitaciones específicas aplicables únicamente a ciudadanos extranjeros. Este mismo autor hace referencia a las personas jurídicas, afirmando que tanto la jurisprudencia como la doctrina han reconocido

---

[233] DÍAZ REVORIO, F. J., *El derecho fundamental al secreto de las comunicaciones*, Derecho PUCP, Revista de la Facultad de Derecho, núm. 59, 2006, p. 159.
[234] STS 16/2014, de 30 de enero, FD 2.
[235] STC 170/2013, de 7 de noviembre, FJ 4.

de forma unánime que éstas también ostentan la titularidad del derecho al secreto de las comunicaciones, si bien este derecho corresponde específicamente a aquella *persona jurídica que formal y jurídicamente esté llevando a cabo la comunicación*, sin perjuicio de que en un mismo acto comunicativo puedan concurrir simultáneamente varias titularidades[236].

Como indica DÍEZ PICAZO, el carácter distintivo del derecho al secreto de las comunicaciones respecto al resto de derechos fundamentales, también compartido por el derecho a la inviolabilidad domiciliaria que se trató en el punto anterior, es la garantía formal de intangibilidad. Este rasgo esencial implica que, *lo decisivo no es el contenido, lo que se guarda en el domicilio o lo que se transmite en la comunicación, sino el continente, poder guardarlo o transmitirlo sin que lo sepan los demás, incluido el Estado*[237]. Como acertadamente conceptualiza JIMÉNEZ CAMPOS, se trata de un *derecho de prestación o, en otras palabras, un derecho al medio o al instrumento para realizarla*[238], en la que la protección constitucional recae sobre la restricción de acceso en sí misma, independientemente de cualquier consideración material.

Dado que el requisito indispensable es la existencia de una comunicación, cabe señalar que la RAE lo define como la *acción y efecto de comunicar o comunicarse*, así como el *trato, correspondencia entre dos o más personas*, y la *transmisión de señales mediante un código común al emisor y al receptor*[239]. Ahora bien, al analizar específicamente el proceso de comunicación protegido por la Constitución Española, ésta enumera una serie de formas de comunicación muy escueta, siendo evidente de que no se trata de una lista cerrada, por lo que se ha de entender que el derecho tratado ampara también otras formas de comunicación como las telemáticas, siendo éstas las realizadas a través de las TIC.

---

[236] DÍAZ REVORIO, F. J., *El derecho fundamental…*, Op. Cit., p. 161.

[237] DÍEZ-PICAZO, L. M., *Sistema de…*, Op. Cit., p. 302.

[238] JIMÉNEZ CAMPO, J., *La garantía constitucional del secreto de las comunicaciones*, Revista Española de Derecho Constitucional, núm. 20, 1987, p. 43.

[239] Definición de “comunicación” obtenida del Diccionario de la Lengua Española de la RAE, recuperado el 11 de mayo de 2025 de https://dle.rae.es/comunicaci%C3%B3n?m=form

La Fiscalía General del Estado reseña algunas de ellas en su Circular sobre interceptación de comunicaciones telefónicas y telemáticas[240], como son los mensajes de texto o SMS aun no leídos[241], o correos electrónicos enviados y recibidos, pero no leídos o en fase de transferencia[242], entre otros, incluyendo cualquier tipo de interceptación o captación ilegítima de las mismas.

La sentencia núm. 114/1984 del Tribunal Constitucional, tiene una especial transcendencia a la hora de abordar el derecho al secreto de las comunicaciones, puesto que, en las alegaciones presentadas por el Abogado del Estado, afirma que una conversación mantenida a través de las TIC, en este caso telefónica, *tiene un contenido de intimidad sólo frente a terceros; si los interlocutores no divulgan su contenido, ello no será en obediencia a una obligación jurídica de silencio, sino en atención a motivos éticos o estéticos*. Esto es que, si uno de los interlocutores de la conversación mantenida grabase la misma por cualquier medio, dicho acto no conculcaría en ningún caso el derecho protegido en el art. 18.3 CE. Si bien, únicamente si se produjera una ulterior difusión del contenido por este sujeto podría verse materializada la infracción constitucional al derecho a la intimidad del art. 18.1 CE.

Caso contrario sería el tercero que aporte como fuente de prueba una comunicación electrónica en la que no haya sido partícipe, tal conducta constituiría una vulneración del derecho al secreto de las comunicaciones. En cuanto a esto, la sentencia anteriormente citada aclara que *quien graba una conversación de otros atenta, independientemente de toda otra consideración, al derecho reconocido en el art. 18.3 CE.* Por este motivo concluye que, lo que *la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia erga omnes) ajenos a la comunicación misma, […],* rechazando *la interceptación o el conocimiento antijurídicos de las comunicaciones ajenas*[243].

[240] Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas, publicada en el BOE núm. 70, de 22 de marzo de 2019, pp. 30091-30120, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4241

[241] STS 1235/2002, de 27 de junio.

[242] STC 115/2013, de 9 de mayo.

[243] STC 114/1984, de 9 de noviembre, FJ 7.

Como indica la jurisprudencia, la validez de dicho medio de prueba no está condicionada al consentimiento en la grabación *de todos los partícipes o contertulios; ni a la ausencia de toda connotación subrepticia o de engaño u ocultación por parte de quien dispone lo necesario para la fijación en un soporte de la conversación.* Por ello asevera que será suficiente con que uno de los interlocutores autorice la intervención y grabación por parte de un tercero para que pierda su efecto la cláusula de exclusión del art. 11 LOPJ. En cualquiera de los casos anteriores se tratará de un elemento probatorio susceptible de valoración por el órgano jurisdiccional, puntualizando que, *sólo la escucha o grabación por un tercero sin autorización de ninguno de los comunicantes ni de la autoridad judicial convierte en inutilizable ese medio probatorio*[244].

Al tratarse de un acto lícito y reconocido por la jurisprudencia, se ha denominado como *bugging* el hecho de *pinchar las conversaciones telefónicas mantenidas por el propio usuario y partícipe de la conversación*[245]. El ordenamiento jurídico ha permitido esta práctica, en la que se incluye la revelación, divulgación o comunicación de dichas conversaciones, en virtud del principio de autonomía de la voluntad que rige las comunicaciones privadas entre interlocutores, ostentando el derecho a decidir libremente sobre éstas.

Los interlocutores disponen de plena autonomía sobre la información integrante del acto comunicativo, de tal forma que la divulgación a terceros del contenido de una comunicación a través de las TIC ya sea por correo electrónico, mensaje instantáneo, llamada telefónica, o cualquier otro, no constituye violación alguna del derecho tratado. Y es que, como cita el Tribunal Constitucional, *en una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo*[246].

La sentencia núm. 145/2014 del Tribunal Constitucional, establece las distintas formas de conculcar dicho derecho, por ejemplo, mediante la interceptación material del soporte del mensaje o del proceso comunicativo, con el conocimiento ilícito del contenido transmitido, o con la obtención no autorizada

[244] STS 145/2023, de 2 de marzo, FJ 4.
[245] ARRABAL PLATERO, P., *La prueba…*, Op. Cit., p. 147.
[246] STC 123/2002, de 20 de mayo, FJ 5.

de metadatos de tráfico telefónico los cuales contienen elementos identificativos de la comunicación[247].

En este mismo sentido se pronuncia la FGE en la Circular citada anteriormente, precisando que el ámbito de protección del derecho fundamental tratado comprende *determinados datos externos que se producen como consecuencia de una comunicación.* Es decir, los mencionados metadatos de tráfico telefónico como son *la identidad subjetiva de los interlocutores y el listado de llamadas o la propia existencia de la comunicación, su momento, duración y destino,* ya sea en redes de comunicación públicas o privadas, independientemente del medio de trasmisión[248].

MARCHENA GÓMEZ considera que, en relación con la intervención de las comunicaciones por correo electrónico, debe interpretarse que su protección constitucional se ciñe exclusivamente al ámbito del artículo 18.3 CE[249]. Sin embargo, esta concepción resulta jurídicamente incompleta, pues la doctrina establece que *la protección del derecho al secreto de las comunicaciones alcanza solo el proceso de la comunicación,* pero una vez concluido el acto comunicativo la protección de los contenidos transmitidos queda supeditada al ámbito de protección del derecho a la intimidad personal u otros derechos fundamentales[250]. En consecuencia, la tutela de este derecho se extiende a las interferencias producidas exclusivamente en el ámbito de un acto comunicativo.

Por tanto, la calificación de la vulneración de derechos fundamentales citada dependerá del momento procesal en que se produzca la interceptación. Por un lado, la intromisión durante el proceso comunicativo activo afectaría al derecho al secreto de las comunicaciones del art. 18.3 CE, como por ejemplo la información interceptada durante el tránsito. Mientras que el acceso a mensajes ya remitidos y almacenados por el destinatario podría constituir una vulneración del derecho a la intimidad del art. 18.1 CE, como podrían ser los que ya han sido objeto de lectura por éste, lo cual aclara JIMÉNEZ CAMPO estableciendo que *esta protección no estaría ya al servicio de la comunicación misma, sino de sus*

[247] STC 145/2014, de 22 de septiembre.

[248] Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado.

[249] MARCHENA GÓMEZ, M., *Dimensión jurídico-penal del correo electrónico*, Diario La Ley, núm. 6475, Sección Doctrina, 4 de mayo de 2006, pp. 23-27.

[250] STC 70/2002, de 3 de abril, FJ 9.C.

contenidos o de su medio de documentación[251]. En último lugar, el derecho tampoco se garantiza en su fase preparatoria, por lo que no ampara las meras intenciones o preparativos previos al intercambio.

3.2.4. Derecho a la protección de datos personales

El art. 18.4 CE en relación con el derecho fundamental a la protección de datos personales, dispone explícitamente que *la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*[252]. En concreto, el Tribunal Constitucional ha calificado este derecho como libertad informática por la *libertad de controlar el uso de esos mismos datos insertos en un programa informático, lo que se conoce con el nombre de habeas data*.

Por su parte, la Carta de los Derechos Fundamentales de la Unión Europea, en concreto su art. 8 CDFUE, reconoce a toda persona el derecho a la protección de datos de carácter personal, y según cita la norma, los *datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley*[253].

Dicho *habeas data* actúa como instrumento jurídico clave que protege otros derechos fundamentales como el honor y la intimidad. Este opera como garantía negativa que impone límites al tratamiento informático de datos para preservar el honor e intimidad, así como el libre ejercicio de los derechos individuales, pero a su vez se erige como un derecho fundamental en sí mismo. La doctrina lo conceptualiza como *el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos*, esto es, como garantía positiva de la intimidad *en forma de derecho de control sobre los datos relativos a la propia persona*[254].

En esta misma línea, FUENTES SORIANO añade que el derecho a la protección de datos, contrario a lo que sucede con el derecho a la intimidad, *atribuye al titular una serie de facultades que consiste, en la mayor parte, en el*

---

[251] JIMÉNEZ CAMPO, J., *La garantía constitucional…*, Op. Cit., p. 43.

[252] Artículo 18, apartado cuarto, de la Constitución Española.

[253] Carta de los Derechos Fundamentales de la Unión Europea, publicado en el DOUE núm. 303, de 14 de diciembre de 2007, pp. 1-16, recuperado de https://boe.es/buscar/doc.php?id=DOUE-Z-2007-70004

[254] SSTC 254/1993, de 20 de julio, FJ 5, 6 y 7; 11/1998, de 13 de enero, FJ 4; y 202/1999, de 8 de noviembre, FJ 2.

poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos[255]. Es decir, se configura como un derecho de control activo sobre la propia información personal del sujeto, el cual tendrá capacidad de exigir ciertas obligaciones de hacer o no hacer a terceros.

El Tribunal Constitucional, en su sentencia 292/2000, describe estas facultades como parte del contenido esencial del derecho fundamental, en referencia a la disposición y control sobre los datos personales. Éstas se concretan jurídicamente en la potestad de permitir *la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular*. Asimismo, a ello debe añadirse el *saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos*[256].

Esta garantía de control y disposición de toda persona física sobre sus datos personales tanto frente a terceros como a los poderes públicos es conocido como el derecho a la autodeterminación informativa [257]. El diccionario panhispánico del español jurídico lo define como el *derecho a conocer, acceder, rectificar y cancelar los datos personales contenidos en ficheros o archivos informáticos,* así como *a impedir agresiones a la dignidad y a la libertad fruto del uso ilegítimo y mecanizado de datos*[258].

Dentro del ámbito particular de la intimidad, un contenido exclusivamente negativo no cumpliría con los requisitos de protección establecidos por el derecho a la libertad informática, y especialmente en un contexto donde las herramientas de recopilación de datos personales se han extendido de manera generalizada, las cuales no solo son accesibles para las entidades estatales sino también para actores privados. Por todo esto han cobrado relevancia conceptos como el Big Data, definidos como *conjunto de tecnologías, prácticas y conceptos que permiten la recolección, almacenamiento, procesamiento y análisis de*

[255] FUENTES SORIANO, O., *La prueba prohibida*…, Op. Cit., p. 723.

[256] STC 292/2000, de 30 de noviembre, FJ 7.

[257] GUERRERO PICÓ, M. C., *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*, Thomson Civitas, Cizur Menor, 2006, p. 187.

[258] Definición de "derecho a la autodeterminación informativa" obtenida del Diccionario panhispánico del español jurídico de la RAE, recuperado el 11 de mayo de 2025 de https://dpej.rae.es/lema/derecho-a-la-autodeterminaci%C3%B3n-informativa

grandes volúmenes de datos que son demasiado complejos o extensos para ser gestionados con las herramientas tradicionales de gestión de datos[259].

Dicha información se produce de forma constante, pudiendo clasificarse sus principales fuentes de generación de datos masivos en cinco tipos[260], según establece la multinacional de tecnología informática y consultoría IBM.

En primer lugar, reseña los datos de grandes transacciones, denominados *Big Transaction Data*, que comprenden registros de facturación y comunicaciones telefónicas, entre otros, incluyendo información empresarial derivada de sistemas de datos de clientes, inventarios de ventas o transacciones. En segundo término, los datos procedentes de redes sociales y páginas web, abarcando tanto interacciones en plataformas como LinkedIn, Facebook o Twitter, como transacciones digitales. La tercera categoría, los datos biométricos, tales como escaneos de retina, huellas dactilares, reconocimiento facial o genético. La siguiente, los datos generados por seres humanos mediante comunicaciones en *call centers*, correos electrónicos, documentos digitales, transacciones con tarjetas bancarias o notas de voz. Y, por último, los datos máquina a máquina, llamados *M2M*, generados mediante dispositivos interconectados que funcionan como sensores o medidores, como los sistemas inteligentes de medición de consumo de agua, gas o electricidad de servicios públicos, produciendo volúmenes masivos de información destinada a monitorizar variables como frecuencia o voltaje.

En la sentencia núm. 143/1994 del Tribunal Constitucional se cuestiona la legitimidad constitucional de una disposición normativa que, mediante un mecanismo de recolección de datos, podría facilitar un uso indebido de los mismos, derivando en una vulneración efectiva de la privacidad de los ciudadanos afectados. Respecto a este particular, el incremento de nuevas tecnologías de tratamiento de datos puede provocar dicha consecuencia, lo que exige ampliar la protección del derecho a la intimidad para impedir intromisiones en la esfera privada realizadas por cualquier medio, incluso las de carácter

[259] REDONDO MARTÍN, J. A., *Qué es Big Data: funcionamiento, aplicaciones y salidas profesionales*, CEU, 14 de septiembre de 2024, recuperado el 11 de mayo de 2025 de https://www.ceu.es/blog/2024/que-es-big-data-funcionamiento-aplicaciones-y-salidas-profesionales/

[260] IEP, *5 tipos de datos en el Big Data*, Instituto Europeo de Postgrado, 8 de mayo de 2019, recuperado el 11 de mayo de 2025 de https://iep.edu.es/5-tipos-de-datos-en-el-big-data/

indirecto. Además de todo esto, el Tribunal Constitucional ha establecido la conveniencia de *incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho*[261].

El Alto Tribunal también ha afirmado carecer de relevancia *la trascendencia e importancia objetiva de los datos personales y familiares*. Esto se debe a que no resulta admisible establecer distinciones a efectos de protección entre *datos o elementos "objetivamente" relevantes para la intimidad,* aparentemente susceptibles de protección penal, y *datos "inocuos"*, cuya supuesta irrelevancia los excluiría del ámbito de la intimidad amparada por el derecho penal. Pero, finaliza especificando que *sí debe exigirse que los datos o información pertenezcan al ámbito privado y personal o familiar del sujeto*[262].

Por tanto, tal derecho no queda limitado exclusivamente a salvaguardar la información íntima o privada, sino que, como indica SOLER MARTÍNEZ, abarca *cualquier tipo de dato personal, sea o no íntimo*[263], cuyo uso indebido por terceros pueda afectar los derechos del titular, con independencia de su naturaleza jurídica. Así que, su objetivo transciende la mera protección de la intimidad, ya garantizada en el art. 18.1 CE, para extenderse a todo tipo de información personal. Esto es, como refiere el autor recientemente citado, comprende la *esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal*, incluyendo el derecho al honor citado en el mismo art. 18.4 CE.

En este sentido, la sentencia núm. 292/2000 del Tribunal Constitucional, reseñada más arriba, amplía los datos amparados por este derecho entre los que incluye *todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole,* o que, en situaciones concretas, puedan derivar en un perjuicio para el individuo afectado[264].

[261] STC 143/1994, de 9 de mayo, FJ 7.
[262] STS 374/2020, de 8 de julio, FD 5.
[263] SOLER MARTÍNEZ, J. A., *Protección constitucional de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías*, Anuario de Derecho Canónico, núm. 11, 2022, p. 115.
[264] STC 292/2000, de 30 de noviembre, FJ 6.

3.2.5. Derecho a la protección del entorno digital

Más de una década ha pasado desde que el Tribunal Constitucional afirmara que existe el *derecho al propio entorno virtual*, concretamente en su sentencia del 17 de abril de 2013. Este ámbito comprende *toda la información en formato electrónico* que el usuario genera mediante el empleo de las tecnologías digitales, ya sea de manera consciente o inconsciente, voluntaria o involuntaria, hasta constituir una huella digital accesible para los poderes públicos. Esta realidad plantea la necesidad de establecer una protección jurídica efectiva frente a las posibles intromisiones del Estado en dicho espacio digital, motivadas por las *tareas de investigación y castigo de los delitos*[265].

Según ARRABAL PLATERO, el rasgo distintivo de este derecho consiste en la tutela integral que confiere a los datos alojados en dispositivos tecnológicos, los cuales reflejan el perfil personal del sujeto investigado. Se configura, así como *un derecho constitucional de nueva generación que ampara de forma unitaria la información que venía protegiéndose de forma separada y con un régimen de protección diferenciado*[266].

Dicho entorno virtual personal será configurado por un dispositivo electrónico y que, probablemente contendrá un cúmulo de información sobre datos personales. Estos pueden incluir una pluralidad de archivos sobre su vida privada y profesional como contactos, documentos, fotografías o videos, así como registros de actividad como páginas web visitadas, participación en foros de conversación, operaciones de comercio electrónico, o lectura de noticias.

Como refieren GONZÁLEZ-CUÉLLAR SERRANO y MARCHENA GÓMEZ estos *formatos digitalizados han traído consigo la generación de datos que, bajo su aparente neutralidad técnica, encierran una información muy valiosa*[267]. Y en este sentido, el Tribunal Constitucional añade que *puede afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc*[268].

---

[265] STS 342/2013, de 17 de abril, FD 8.

[266] ARRABAL PLATERO, P., *La prueba*…, Op. Cit., p. 168.

[267] GONZÁLEZ-CUÉLLAR SERRANO, N., y MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal de 2015*, Castillo de Luna, p. 286.

[268] STC 173/2011, de 7 de noviembre, FJ 3.

Además, el Tribunal Constitucional continúa detallando que los datos contenidos en un dispositivo electrónico podrían considerarse intranscendentes si se examinan aisladamente. Sin embargo, LÓPEZ-BARAJAS PEREA especifica que, *analizados en su conjunto permiten configurar un perfil altamente descriptivo de la personalidad del titular*[269]*.* Por este motivo afirma que será esencial su protección *frente a la intromisión de terceros o de poderes públicos*.

Asimismo, con elevada probabilidad cualquier dispositivo electrónico con capacidad de configurar un entorno virtual personal, también dispondrá de la funcionalidad de establecer comunicaciones con terceras personas como instrumento útil para la emisión o recepción de mensajes. Es por ello que cualquier tipo de intromisión en dichos dispositivos podría vulnerar tanto al derecho al secreto de las comunicaciones del art. 18.3 CE, como al derecho a la intimidad personal del art. 18.1 CE, e incluso al derecho a la protección de datos del art. 18.4 CE si, por ejemplo, contuviera datos de geolocalización de archivos. Por otra parte, *el art. 18.1 CE reconoce al titular del derecho el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido*[270].

Dos son las características propias de la información digital según LÓPEZ-BARAJAS PEREA, siendo estas su deslocalización y su volatilidad. Respecto a la primera, expone que los datos pueden almacenarse tanto en soportes físicos como en dispositivos en la nube. Los conocidos como nube o *cloud computing* serán alojados en servidores remotos*,* permitiendo el uso de servicios de almacenamiento o compartición de documentos, *todo ello sin necesidad de que el usuario disponga de servidores o de software propios*[271]. Esto último no significa que expresamente *la información esté localizada en dicho lugar*[272].

Una particularidad del derecho tratado en el presente apartado, así como el derecho a la intimidad, es su posibilidad de *ampliación o reducción por el propio titular.* Esto se debe a que ante una presunta vulneración del derecho a la

[269] DÍAZ MARTÍNEZ, M., LÓPEZ-BARAJAS PEREA, I., BUENO DE MATA, F., *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas* (1ª edición), Tirant lo Blanch, 2018, p. 137.
[270] STC 196/2004, de 15 de noviembre, FJ 2.
[271] DÍAZ MARTÍNEZ, M., LÓPEZ-BARAJAS PEREA, I., & BUENO DE MATA, F., *La nueva reforma…*, Op. Cit., p. 146.
[272] ORTIZ PRADILLO, J. C., *Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica*, en *El proceso penal en la sociedad de la información*, La Ley, 2012, pp. 305-310.

intimidad en casos de uso compartido de dispositivos electrónicos no se podrá obviar el hecho de *hacer uso común de una contraseña de acceso*. Es decir, quien incorpora fotografías o documentos digitales a un dispositivo de almacenamiento masivo de uso compartido asume conscientemente que la delimitación entre lo estrictamente privado y lo potencialmente accesible a terceros, *se difumina de forma inevitable*[273].

Biblioteca
UNIVERSITAS Miguel Hernández

[273] STS 287/2017, de 19 de abril, FD 2.

4. Conclusiones

PRIMERA. Ante la inexistencia de regulación expresa por parte del Legislador de una definición específica de las pruebas tecnológicas, considero de urgente necesidad que este último establezca una definición normativa que sirva de base para su adecuada reglamentación procesal y garantice la seguridad jurídica.

SEGUNDA. Se ha podido constatar que las pruebas tecnológicas presentan una dualidad característica. Por un lado, ofrecen ventajas determinantes como su capacidad para proporcionar información objetiva, completa y técnicamente verificable debido a su facultad de conservar metadatos y huellas digitales únicas que permiten la reconstrucción de hechos con precisión científica. Pero por otro, se ven contrarrestadas por los riesgos derivados de su volatilidad, fácil alterabilidad y potencial afectación a derechos fundamentales durante su obtención y consiguiente ilicitud probatoria.

TERCERA. El tratamiento de las pruebas ilícitas revela profundas contradicciones en la práctica judicial, donde se ha podido examinar que coexisten criterios diferentes en cuanto a la exclusión probatoria basada en las diferentes teorías tratadas en el presente TFG. Esta disparidad evidencia la imposibilidad de establecer una regla general absoluta y la necesidad de articular un sistema probatorio flexible pero coherente, que combine el respeto a los estándares constitucionales con una adecuada adaptación a las peculiaridades de la prueba digital en la era tecnológica.

CUARTA. El proceso penal enfrenta el reto de compatibilizar la obtención de pruebas tecnológicas con la protección irrenunciable de los derechos fundamentales recogidos en el art. 18 CE ante la potencial afectación de éstos, tal como se ha referido en la conclusión SEGUNDA. Si bien, estos derechos suponen un límite casi infranqueable tanto para el Estado como particulares, motivo por el que la jurisprudencia y la doctrina concluyen que la verdad procesal nunca puede justificar su vulneración. En este sentido es imprescindible delimitar cada uno de estos derechos con el fin de establecer la frontera entre lo lícito y lo ilícito. Por ello, se debe determinar qué elementos conforman el núcleo esencial

del derecho a la intimidad personal y bajo qué parámetros se configura, ya sea desde la autopercepción individual o mediante criterios jurídicos objetivos; precisar el concepto de morada, y los espacios que abarca su inviolabilidad, así como su posible vinculación con requisitos temporales; definir el alcance material del secreto de las comunicaciones, es decir, si solo protege el contenido de la comunicación o también el proceso comunicativo en sí, incluyendo la identidad de los interlocutores y los medios tecnológicos utilizados, y cuál es el límite que una vez sobrepasado vulneraría el derecho a la intimidad; esclarecer los contornos del derecho a la protección de datos, en el que se garantiza el control individual sobre cualquier dato personal, sea íntimo o no, imponiendo límites a su tratamiento automatizado y exigiendo transparencia en su uso; y, finalmente, establecer qué componentes del entorno virtual, incluyendo metadatos y huellas digitales de actividad, merecen protección por configurar un perfil identificativo del individuo, con independencia de su aparente neutralidad.

QUINTA. Como afirmó Heráclito de Efeso, *lo único constante es el cambio*. Este principio adquiere especial transcendencia en el ámbito de las pruebas tecnológicas, donde la acelerada evolución digital genera continuamente nuevos medios de prueba. Ante esta realidad cambiante, resulta inevitable que tanto la jurisprudencia como el legislador mantengan una actualización constante, permitiendo anticiparse a escenarios futuros y así garantizar un proceso penal equilibrado, donde la búsqueda de la verdad no socave las garantías fundamentales en ningún contexto tecnológico.

5. Bibliografía

ABEL LLUCH, X., *Régimen jurídico de la prueba electrónica*. Colección de Formación Continua Facultad de Derecho ESADE, J.M. Bosch Editor, Barcelona, 2011.

ABEL LLUCH, X., PICÓ I JUNOY, J., *La prueba electrónica*, Colección de Formación Continua Facultad de Derecho ESADE, Serie estudios prácticos sobre los medios de prueba, J. M. Bosch editor, 2011.

ABEL LLUCH, X., RICHARD GONZÁLEZ, M., *Estudios sobre prueba penal*, Wolters Kluwer, Madrid, 2013.

AGUSTINOY GUILAYN, A., MONCLÚS RUIZ, J., *Aspectos legales de las redes sociales*, Editorial Bosch, Barcelona, 2016.

ARAGÓN REYES, M., *La inviolabilidad del domicilio*, Revista Española de Derecho Constitucional, 1998, recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=2001827

ARMENTA DEU, T., *La verdad en el filo de la navaja (nuevas tendencias en materia de prueba ilícita)*, Revista Ius et Praxi, núm. 2, 2013, pp. 345 a 377, recuperado de http://dx.doi.org/10.4067/S0718-00122007000200014

ARRABAL PLATERO, P., *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, 2020.

ASENCIO MELLADO, J. M., *Derecho procesal penal* (7ª edición), Tirant lo Blanch, 2015.

ASENCIO MELLADO, J. M., FUENTES SORIANO, O., *Derecho procesal penal* (3ª edición), Tirant lo Blanch, 2024.

ASENCIO MELLADO, J. M., FUENTES SORIANO, O., *El procedimiento probatorio y valoración de la prueba en el marco del proceso penal. Introducción al derecho procesal*, Tirant lo Blanch, 2019, pp. 260-269.

BANACLOCHE PALAO, J., *La prueba en el proceso penal*, Aspectos fundamentales del Derecho Procesal Penal, editorial La Ley (2ª edición), Madrid, 2011.

BENDER, A., *El correo electrónico como prueba en la jurisprudencia*, Thomson Reuters, 2013.

BUENO DE MATA, F., BUJOSA VADELL, L.-M. *Prueba Electrónica y Proceso 2.0.* Tirant lo Blanch, 2014.

BUJOSA VADELL, L.M., et al., *La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia*, Revista Brasileira de Direito Processual Penal, 7(2), 2021, pp. 1347-1384.

CABEZUDO BAJO, M.J., *La inviolabilidad del domicilio y el proceso penal* (1ª edicición), Iustel
Publicaciones, 2004.

CAMPANER MUÑOZ, J., *La confesión precedida de la obtención inconstitucional de fuentes de prueba*, Tesis Doctoral, Universidad Complutense de Madrid, Facultad de Derecho, 2015.

CARRILLO DEL TESO, A. E., *La prueba prohibida aportada por particulares al proceso penal: la evolución en el TS, Proceso y prueba prohibida* (1ª edición), editado por ROCA MARTÍNEZ, J. M. y NIETO MORALES, C., Dykinson, 2022.

CASEY, E., Digital evidence and computer crime (3ª edición), Elsevier, 2011, recuperado de https://dl.acm.org/doi/pdf/10.5555/2021194

CASTELLS OLIVÁN, M., *La era de la información. Economía, sociedad y cultura* (Vol. 3), Alianza Editorial, 2001.

COSTA TORNÉ, M. C., *La prueba ilícita por violación de Derechos Fundamentales y sus excepciones*, Revista de Derecho UNED, Nº11, 2012, recuperado de https://revistas.uned.es/index.php/RDUNED/article/view/11128/10656

CUADRADO SALINAS, C., *Fundamento y efectos de la exclusión de la prueba obtenida con vulneración de derechos fundamentales*, Valencia, Tirant lo Blanch, 2021.

CUADRADO SALINAS, C., *Registro informático y prueba digital: estudio y análisis comparado de la ciberinvestigación criminal en Europa,* La Ley Penal, nº 107, 2014.

DELGADO DEL RINCÓN, L. E., *La regla de exclusión de la prueba ilícita, excepciones y eficacia*, Dialnet, 2013.

DELGADO MARTÍN, J., *La prueba del Whatsapp*, Diario La Ley, nº 8605, Sección Tribuna, 2015.

DELGADO MARTÍN, J., *La prueba digital. Concepto, clases, aportación al proceso y valoración*, Diario La Ley, nº 6, Sección Ciberderecho, Wolters Kluwer, 2017.

DE URBANO CASTRILLO, E., Los delitos informáticos tras la reforma del CP de 2010, en Delincuencia informática: tiempos de cautela y amparo, Thomson Reuters, Madrid, 2012.

DEVIS ECHANDÍA, H., *Teoría general de la prueba judicial* (5º edición), Tomo I, Buenos Aires, 1981.

DÍAZ MARTÍNEZ, M., LÓPEZ-BARAJAS PEREA, I., & BUENO DE MATA, F., *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas* (1a edición), Tirant lo Blanch, 2018, pp. 135-168.

DÍAZ REVORIO, F. J., *El derecho fundamental al secreto de las comunicaciones*, Derecho PUCP, Revista de la Facultad de Derecho, núm. 59, 2006, pp. 159-175, recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=5085108

DÍEZ-PICAZO, L. M., *Sistema de derechos fundamentales* (5ª edición), Tirant lo Blanch, 2021.

ESPÍN TEMPLADO, E., *Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio*, Revista del Centro de Estudios Constitucionales, núm. 8, 1991, pp. 39-53, recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=1050860

FERNÁNDEZ ENTRALGO, J., *Las reglas del juego. Prohibición de hacer trampas: la prueba ilegítimamente obtenida*, Cuadernos de Derecho Judicial, C.G.P.J., Madrid, 1996.

FUENTES SORIANO, O., *El valor probatorio de los correos electrónicos*. Capítulo del libro: Justicia Penal y Nuevas formas de delincuencia, (Dir. ASENCIO MELLADO, Coord. Fernández López), Ed. Tirant lo Blanch, Valencia 2017, pp. 149-183.

FUENTES SORIANO, O., *La intervención de las comunicaciones tecnológicas tras la Reforma de 2015*, en El nuevo proceso penal tras las reformas de 2015 (ALONSO CUEVILLAS I SAYROL, Dir), Atelier, 2016.

FUENTES SORIANO, O., *La prueba prohibida. Viejos problemas procesales de las nuevas tecnologías*. Capítulo de libro. En PRIORI POSADA. G. (Coord.), Justicia y proceso en el S. XXI. Desafíos y tareas pendientes, Ed. Palestra, Perú, 2019.

FUENTES SORIANO, O., *La prueba prohibida aportada por particulares a la luz de las nuevas tecnologías*. Derecho probatorio y otros estudios procesales. Liber

amicorum Vicente Gimeno Sendra, ASENCIO MELLADO (Dir.), Castillo de Luna. Ediciones jurídicas, Madrid, 2020, pp. 715 a 745.

FUENTES SORIANO, O., "*Las comunicaciones telemáticas: aportación y valoración de la prueba*", en El proceso penal. Cuestiones fundamentales (Coord. FUENTES SORIANO), Tirant Lo Blanch, Valencia, 2017, pp. 277-301.

GIL NOGUERAS, L.A., *La valoración de la prueba electrónica en el proceso civil*, práctica de Tribunales, núm. 130, Wolters Kluwer, 2018.

GIMENO SENDRA, V., *Derecho procesal penal* (2ª edición), Editorial Aranzadi, 2015.

GIMENO SENDRA, V., *Fundamentos del derecho procesal*, Civitas, 1981.

GINER ALEGRÍA, C. A., *Prueba prohibida y prueba ilícita*. Anales de derecho. Universidad de Murcia, número 26, 2008.

GONZÁLEZ-CUÉLLAR SERRANO, N., y MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal de 2015*, Castillo de Luna.

GONZÁLEZ I JIMÉNEZ, A., *Las diligencias policiales y su valor probatorio*, BOSCH, 2014.

GONZÁLEZ MONTES, J. L., *La prueba ilícita*, Revista Persona y Derecho, núm. 54, 2006, pp. 363-383, recuperado de https://dadun.unav.edu/entities/publication/c3ed8db9-b784-43cf-92ba-d93f2f608754

GONZÁLEZ MONTES, J. L., *La prueba obtenida ilícitamente con violación* de los derechos fundamentales (el derecho constitucional a la prueba y sus límites), Revista de Derecho Procesal, 1990.

GUERRERO PICÓ, M. C., *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*, Thomson Civitas, Cizur Menor, 2006.

HERNÁNDEZ GIMÉNEZ, M. *Inteligencia artificial y derecho penal*. Actualidad jurídica iberoamericana, 2019, recuperado de https://revista-aji.com/wp-content/uploads/2019/06/792-843.pdf

JIMÉNEZ CAMPO, J., *La garantía constitucional del secreto de las comunicaciones*, Revista Española de Derecho Constitucional, núm. 20, 1987, recuperado de https://www.cepc.gob.es/sites/default/files/2021-12/24847redc020035.pdf

LÁZARO HERRERO, C., *Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad: Un proyecto europeo*, vol.5, Nº 2, 2008, pp.139-152, recuperado de https://ve.scielo.org/scielo.php?pid=S1690-75152008000200009&script=sci_abstract

LEFEBVRE, F., *Derecho de las Nuevas Tecnologías*, Memento Práctico, Écija, 2017-2018, p. 337.

MARCHENA GÓMEZ, M., *Dimensión jurídico-penal del correo electrónico*, Diario La Ley, núm. 6475, Sección Doctrina, 4 de mayo de 2006, pp. 23-27.

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

MARTÍNEZ OTERO, J. M., *Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento*, Revista Española de Derecho Constitucional, núm. 106, 2016, pp. 119-148, recuperado de https://doi.org/10.18042/cepc/redc.106.03

MATÍA PORTILLA, F. J., *El derecho fundamental a la inviolabilidad del domicilio*, McGraw-Hill Interamericana de España, Madrid, 1997, recuperado de https://dialnet.unirioja.es/servlet/libro?codigo=232397

MEDINA MARTÍN, E., La inteligencia artificial y su encuadre como medio de prueba, *El Criminalista Digital. Papeles De Criminología*, (12), 2024, pp. 33–51, recuperado de https://revistaseug.ugr.es/index.php/cridi/article/view/31430

MENESES PACHECO, C., *Fuentes de prueba y medios de prueba en el proceso civil*, Revista Ius et Praxis, vol. 14, nº 2, 2008.

MIRANDA ESTRAMPES, M., *La prueba ilícita: la regla de exclusión probatoria y sus excepciones*, Revista Catalana de Securetat Pública, mayo 2010, recuperado de https://raco.cat/index.php/RCSP/article/view/194215

MIRANDA ESTRAMPES, M., SERRA DOMINGUEZ, M., *El concepto de prueba ilícita y su tratamiento en el proceso penal* (2ª edición), Bosch Editor, 2004.

MIRÓ-LLINARES, F., *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, 2012, recuperado de https://www.infoem.org.mx/doc/biblioteca/accesoytrans/ciberdelitos/el-cibercrimen.pdf

MIRKOUSKI, D. O., *Prueba electrónica: nociones generales*, Revista Pensamiento Penal, (480), 2023, recuperado de https://www.pensamientopenal.com.ar/system/files/diego_0.pdf

MONTERO AROCA, J., *La prueba en el proceso civil*, Thomson – Civitas (4ª edición), Navarra, 2005, pp. 133-137.

MONTÓN REDONDO, A., *Los nuevos medios de prueba y la posibilidad de su uso en el proceso*, Salamanca, Departamento de Derecho Procesal de la Universidad, 1977.

MUÑOZ RODRÍGUEZ, A.B., *El impacto de la Inteligencia Artificial en el Proceso Penal*, Universidad de Extremadura, 36, 2020, pp. 695-728, recuperado de https://revista-afd.unex.es/index.php/AFD/article/view/489/572

NEFTALÍ NICOLÁS GARCÍA, J., *Las nuevas tecnologías y la prueba electrónica en el proceso judicial*, Proceso civil y nuevas tecnologías, 2021.

OLIVA LEÓN, R., *La prueba electrónica, validez y eficacia procesal*, Editorial Juristas con futuro, 2016, recuperado de https://dialnet.unirioja.es/servlet/libro?codigo=658404

ORTIZ PRADILLO, J. C., *Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica*, en *El proceso penal en la sociedad de la información*, La Ley, 2012.

PÉREZ PALACÍ, J. E., *La prueba electrónica: consideraciones*, Universitat Oberta de Catalunya, 2014, recuperado de http://hdl.handle.net/10609/39084

PICÓ JUNOY, J., *El derecho a la prueba en el proceso civil*, J. Mª Bosch Editor, Barcelona, 1996.

PINTO PALACIOS, F., PUJOL CAPILLA, P., *La prueba en la era digital*, Wolters Kluwer, 2017, recuperado de https://pdfcoffee.com/la-prueba-en-la-era-digital-2017-pinto-palacios-4-pdf-free.html

RICHARD GONZÁLEZ, M., *Valor como prueba de los mensajes y comunicaciones electrónicas en los procesos de familia*, Problemática actual de los procesos de familia, Especial atención a la prueba, J.M. Bosch Editor, 2018, pp. 199-250.

RIVES SEVA, A. O., *La intervención de las Comunicaciones en la jurisprudencia penal*, Editorial Aranzadi, Pamplona, 2000.

ROCA MARTÍNEZ, J. M., NIETO MORALES, C., *Procesos y Prueba Prohibida* (1ª edición), Dykinson, 2022, recuperado de https://doi.org/10.2307/j.ctv2zp4v9b

ROMÁN PUERTA, L., *La prueba en el proceso penal*, Revista Aldaba, núm. 24, 1995, recuperado de https://doi.org/10.5944/aldaba.24.1995.20334

SÁNCHEZ RUBIO, A., RODRÍGUEZ ÁLVAREZ, A., VALIÑO CES, A., ALONSO SALGADO, C., OTERO CRESPO, M., RAMOS HERNÁNDEZ, P. *La prueba tecnológica obtenida por particulares. Retos jurídicos de actualidad,* Dykinson, *2021,* pp. 41-45, recuperado de https://doi.org/10.2307/j.ctv282jgcd.9

SIGÜENZA LÓPEZ, J., *Proceso civil y nuevas tecnologías*, Thomson Reuters Aranzadi, Pamplona, 2021.

SILVA MELERO, V., *La prueba procesal*, Tomo I, Editorial Revista de Derecho Privado, Madrid, 1963.

SOLER MARTÍNEZ, J. A., *Protección constitucional de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías*, Anuario de Derecho Canónico, núm. 11, 2022, pp. 93-126, recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=8661053

VALLE MUÑOZ, F. A., *Las redes sociales como medio de prueba en el proceso laboral*, Revista de Estudios Jurídico Laborales y de Seguridad Social, núm. 6, 2023, recuperado de https://revistas.uma.es/index.php/REJLSS/article/view/16217/16780

VELASCO NÚÑEZ, E., *Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica*, Diario La Ley, Nº 8183, Sección Doctrina, 4 de noviembre de 2013, recuperado de https://diariolaley.laleynext.es/content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiMDU0MzC7Wy1KLizPw827DM9NS8kIS1xKTi_JzSktTQokzbkKLSVAA18--zMQAAAA==WKE

WARREN, S. D., y BRANDEIS, L. D., *The Right to Privacy*, Harvard Law Review, Vol. IV, núm. 5, 15 de diciembre de 1890, recuperado de https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, Cizur Menor, Navarra, 2015.

6. Jurisprudencia

STS 300/2015, de 19 de mayo, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/571257698

STS 559/2017, de 13 de julio, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/690747833

STS 236/2008, de 9 de mayo, recuperado de https://vlex.es/vid/pornografia-i-39004682

STS 330/2023, de 9 de mayo, Sala Cuarta, de lo Social, recuperado de https://www.iberley.es/jurisprudencia/sentencia-social-tribunal-supremo-9-5-23-48508047

STS 706/2020, de 23 de julio, Sala Cuarta, de lo Social, recuperado https://vlex.es/vid/849700130

ATS, de 21 de marzo de 2013, Sala Primera, de lo Civil, recuperado de https://vlex.es/vid/430195510

STS 850/2014, de 26 de noviembre, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/551912818

SAP Zaragoza 450/2019, de 31 de mayo, Sección 5ª, recuperado de https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1CjUwMDAzMTA1NDBRK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1RKTivNzSktSQ4sybUOKSlMB-rrbWkUAAAA=WKE

STC 114/1984, de 29 de noviembre, Sala Segunda, recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-1984-27955

STS 298/2013, de 13 de marzo, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/436380566

STS 325/2022, de 6 de abril, Sala Cuarta, de lo Social, recuperado de https://vlex.es/vid/902773680

STS 285/2016, de 6 de abril, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/632689961

STC 128/1990, de 5 de Julio, Sala Primera, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1990-18322

STS 299/2006, de 17 de marzo, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/grabaciones-videograficas-sobree-escenas-20549472

STS 649/2019, de 20 de diciembre, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/839267466

STS 315/2016, de 14 de abril, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/637465525

STS 167/2020, de 19 de mayo, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/844800413

STS 754/2015, de 27 de noviembre, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/591346098

STS 547/2022, de 2 de junio, Sala Segunda, de lo Penal, recuperado de https://www.icava.org/public/Attachment/2022/6/sts_547_2022.pdf

STS 115/2015, de 5 de marzo, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/563109814

STC 81/1998, de 2 de abril, publicado en el BOE núm. 108, de 6 de mayo de 1998, recuperado de https://hj.tribunalconstitucional.es/ru/Resolucion/Show/3583

STC 85/1994, de 14 de marzo, publicada en BOE núm. 89, de 14 de abril de 1994, pp. 42-48, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1994-8334

STS 113/2014, de 17 de febrero, recuperado de https://vlex.es/vid/496770538

STS 301/2013, de 18 de abril, recuperado de https://vlex.es/vid/436378942

STC 97/2019, de 16 de julio, publicada en BOE núm. 192, de 12 de agosto de 2019, pp. 89739-89762, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-11909

STS 116/2017, de 23 de febrero, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/667933841

ATS 3773/1992, de 18 de junio, Sala Segunda, de lo Penal.

STC 49/1999, de 5 de abril, publicado en el BOE núm. 100, de 27 de abril de 1999, recuperado de https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/3791

STC 25/1981, de 14 de julio, publicado en el BOE núm. 193, de 13 de agosto de 1981, recuperado de https://hj.tribunalconstitucional.es/ru-RU/Resolucion/Show/25

STC 18/1984, de 7 de febrero, publicado en el BOE núm. 59, de 9 de marzo de 1984, pp. 12-17, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1984-6106

STC 139/2001, de 18 de junio, publicada en el BOE núm. 170, de 17 de julio de 2001, recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-2001-13794

ATC 257/1985, de 17 de abril, recuperado de https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/9320

STC 231/1988, de 2 de diciembre, publicado en el BOE núm. 307, de 23 de diciembre de 1988, pp. 44-48, recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-1988-29203

STC 115/2000, de 10 de mayo, Sala Segunda, publicado en BOE núm. 136, de 7 de junio de 2000, pp. 76-82, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-2000-10663

STC 173/2011, de 7 de noviembre, publicada en el BOE núm. 294, de 7 de diciembre de 2011, pp. 1-19, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-19231

STC 92/2023, de 11 de septiembre, Sala Segunda, publicado en el BOE núm. 244, de 12 de octubre de 2023, pp. 137042-137064, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-21154

STS 278/2021, de 10 de mayo, Sala Primera, de lo Civil, recuperado de https://vlex.es/vid/868270006

STC 94/1999, de 31 de mayo, publicado en el BOE núm. 154, de 29 de junio de 1999, pp. 33-42, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1999-14229

STC 137/1985, de 17 de octubre, recuperado de https://www.iberley.es/jurisprudencia/sentencia-constitucional-n-137-1985-tc-sala-segunda-rec-recurso-amparo-124-1985-17-10-1985-12204031

STC 10/2002, de 17 de enero, publicado en el BOE núm. 34, de 8 de febrero de 2002, pp. 56-65, recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-2002-2504

STS 538/1996, 11 de julio, recuperado de https://vlex.es/vid/flagrancia-ilegitimamente-obtenida-57621780

STS 1448/2005, de 18 de noviembre, recuperado de https://vlex.es/vid/delito-salud-as-19963861

STS 84/2001, de 29 de enero, recuperado de https://vlex.es/vid/delito-salud-va-15205869

STS 624/2002, 10 de abril, recuperado de https://vlex.es/vid/delito-salud-domicilio-u-18-2-as-15055888

STS 937/1998, 7 de julio, recuperado de https://vlex.es/vid/17715615

STS 576/2002, 3 de septiembre, recuperado de https://vlex.es/vid/falsedad-oficial-inspeccion-mandamiento-17726431

STC 189/2004, de 2 de noviembre, publicado en el BOE núm. 290, de 2 de diciembre de 2004, pp. 66-73, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-2004-20432

STC 69/1999, de 26 de abril, publicado en el BOE núm. 130, de 1 de junio de 1999, pp. 34-39, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1999-12205

STS 171/2015, de 19 de mayo, Sala Segunda, de lo Penal, recuperado de https://www.iberley.es/jurisprudencia/sentencia-penal-n-171-2015-ts-sala-penal-sec-1-rec-1491-2014-19-05-2015-47432571

STS 16/2014, de 30 de enero, recuperado de https://vlex.es/vid/secreto-comunicaciones-direcciones-494105146

STC 170/2013, de 7 de noviembre, publicado en el BOE núm. 267, de 7 de noviembre de 2013, pp. 49-67, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-11681

STS 1235/2002, de 27 de junio, Sala Segunda, de lo Penal, recuperado de https://vlex.es/vid/ia-i-15056462

STC 115/2013, de 9 de mayo, publicado en el BOE núm. 133, de 4 de junio de 2013, pp. 108-118, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-5938

STS 145/2023, de 2 de marzo, recuperado de https://www.iberley.es/jurisprudencia/sentencia-penal-ts-2-3-23-48489750

STC 123/2002, de 20 de mayo, publicada en el BOE núm. 146, de 19 de junio de 2002, pp. 61-70, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-2002-11898

STC 145/2014, de 22 de septiembre, publicado en el BOE núm. 261, de 28 de octubre de 2014, pp. 34-50, recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2014-11014

STC 70/2002, de 3 de abril, publicado en el BOE núm. 99, de 25 de abril de 2002, pp. 8-19, recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-2002-7883

STC 254/1993, de 20 de julio, publicado en el BOE núm. 197, de 18 de agosto de 1993, pp. 28-34, recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-1993-21425

STC 11/1998, de 13 de enero, publicado en el BOE núm. 37, de 12 de febrero de 1998, pp. 48-53, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1998-3143

STC 202/1999, de 8 de noviembre, publicado en el BOE núm. 300, de 16 de diciembre de 1999, pp. 19-26, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1999-23944

STC 292/2000, de 30 de noviembre, publicado en el BOE núm. 4, de 4 de enero de 2001, pp. 104-118, recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

STC 143/1994, de 9 de mayo, publicado en el BOE núm. 140, de 13 de junio de 1994, pp. 46-51, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1994-13378

STS 374/2020, de 8 de julio, recuperado de https://vlex.es/vid/849674029

STS 342/2013, de 17 de abril, recuperado de https://vlex.es/vid/438315958

STC 173/2011, de 7 de noviembre, publicado en el BOE núm. 294, de 7 de diciembre de 2011, pp. 1-19, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-19231

STC 196/2004, de 15 de noviembre, publicado en el BOE núm. 306, de 21 de diciembre de 2004, pp. 8-16, recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-T-2004-21369

STS 287/2017, de 19 de abril, recuperado de https://vlex.es/vid/678192133