FACULTAD DE DERECHO

EL DERECHO AL SECRETO DE LAS COMUNICACIONES Y SU INCIDENCIA EN EL PROCESO PENAL

Autor: Gabriela Corchado Albisu

4º E-1 JGP

Derecho Procesal

Madrid

Marzo, 2025

RESUMEN

Este trabajo analiza el derecho fundamental al secreto de las comunicaciones y su incidencia en el proceso penal, tratando su evolución normativa y jurisprudencial. Se estudia su regulación en el artículo 18.3 CE y las garantías establecidas por la LO 13/2015 para la intervención de comunicaciones. Se examinan tanto los requisitos de proporcionalidad y necesidad, como las diferencias en la regulación de medios como llamadas telefónicas y otros medios de comunicación digital, además, las comunicaciones telefónicas se analizan de manera particular. También se analizan supuestos de vulneración del derecho y su control judicial. Finalmente, se reflexiona sobre los retos futuros que plantean las nuevas tecnologías y la supervisión digital, subrayando la importancia de balancear seguridad y privacidad en el proceso penal.

Palabras clave: secreto de las comunicaciones, proceso penal, intervención de comunicaciones, proporcionalidad y necesidad, LO 13/2015, control judicial y protección de la privacidad.

ABSTRACT

This paper analyses the fundamental right to secrecy of communications and its impact on criminal proceedings, dealing with its regulatory and jurisprudential evolution. It studies its regulation in article 18.3 CE and the guarantees established by LO 13/2015 for the interception of communications. It examines both the requirements of proportionality and necessity, as well as the differences in the regulation of means such as telephone calls and other means of digital communication. It also analyses cases of infringement of the right and its judicial control. Finally, it reflects on the future challenges posed by new technologies and digital supervision, highlighting the importance of balancing security and privacy in criminal proceedings.

Key words: secrecy of communications, criminal proceedings, interception of communications, proportionality and necessity, LO 13/2015, judicial control and protection of privacy.

LISTADO DE ABREVIATURAS

CE: Constitución Española.

CEDH: Carta Europea de Derechos Humanos.

IA: Inteligencia Artificial.

LECrim: Ley de Enjuiciamiento Criminal.

LO: Ley Orgánica.

TC: Tribunal Constitucional.

TEDH: Tribunal Europeo de Derechos Humanos.

TJUE: Tribunal de Justicia de la Unión Europea.

TS: Tribunal Supremo.

UE: Unión Europea.

ÍNDICE

CAPITULO I: INTRODUCCIÓN

1. CUESTIÓN OBJETO DE LA INVESTIGACIÓN

Este trabajo se centra en el derecho al secreto de las comunicaciones y su incidencia en el proceso penal. He escogido este trabajo dada la importancia que considero que tienen las comunicaciones debido a la notable evolución de las nuevas tecnologías en la última década, como los teléfonos móviles o el correo electrónico. Las comunicaciones son realmente esenciales en el ámbito jurídico, así como en la vida cotidiana.

En este trabajo, al tratarse de comunicaciones privadas, he decidido centrarme en las intervenciones, violaciones y novedades, tanto tecnológicas como normativas, relativas a la confidencialidad de la información y su impacto en el proceso penal. Esto se considera relevante teniendo en cuenta los cambios importantes en la prueba y otros aspectos relevantes.

2. ANTECEDENTES

Considero relevante mencionar el contexto histórico de las comunicaciones. A lo largo de la historia han existido otros medios de relación entre personas alejadas. El más tradicional ha sido, sin duda, el correo. Las fuentes romanísticas nos ofrecen la existencia de intercambios postales e incluso noticia de la actividad que vulneraba la privacidad de esas relaciones: la 'per lustración' o indagación y lectura de los contenidos de las misivas.[1]

En cuanto a nuestras constituciones históricas, se considera relevante que la Constitución de 1869 prohíbe a las autoridades gubernativas la 'detención y apertura' de la correspondencia confiada al correo, así como la detención de los telegramas. Señala asimismo que con autorización de un juez competente podrán intervenirse ambos medios. No obstante, la Constitución de 1876 prohíbe tan solo la apertura de la correspondencia y exige que el auto judicial que la dispone sea motivado. Nuestro actual artículo 18.3 de la CE es relativamente igual a este, añadiendo los medios de comunicación generalizados en 1978.

La Constitución de 1978 introdujo, dentro de los derechos fundamentales, el derecho al secreto de las comunicaciones en su artículo 18.3, incorporando de manera abierta los medios de comunicación modernos cuando dice que ‘se garantiza el secreto de las

[1] Belda Pérez-Pedrero, E.**,** “El derecho al secreto de las comunicaciones”, *Parlamento y Constitución. Anuario*, núm. 2, 1998, p. 171.

comunicaciones (...) en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial', influenciado por épocas en las que las comunicaciones postales y telegráficas eran el medio habitual. Sin embargo, la vertiginosa evolución de las comunicaciones a partir de entonces ha hecho necesario modelar y conformar una interpretación uniforme de este derecho por parte del Tribunal Constitucional[2].

3. OBJETIVOS DEL TRABAJO

Este trabajo tiene como objetivo principal un análisis del derecho fundamental al secreto de las comunicaciones y su incidencia en el proceso penal, abordando su evolución normativa actual, sus excepciones y sus límites, así como su aplicación práctica en la investigación judicial.

Para ello, se plantean los siguientes objetivos:

1. Estudiar el fundamento, titularidad y alcance del derecho al secreto de las comunicaciones, distinguiendo su reconocimiento constitucional en el Título I y su eficacia, así como los diferentes medios de comunicación protegidos en la normativa española. Esta primera aproximación permite sentar las bases conceptuales necesarias para el posterior desarrollo del trabajo.
2. Abordar la vulneración del derecho al secreto de las comunicaciones, reconociendo las excepciones previstas por la ley y distinguiendo entre intromisión legítima e ilegítima.
3. Analizar la regulación de la intervención de las comunicaciones, sus requisitos legales, jurisprudencia relevante y garantías procesales.
4. Examinar la reforma introducida por la Ley Orgánica 13/2015 en la Ley de Enjuiciamiento Criminal, identificando sus cambios y su impacto en la obtención y valoración de la prueba.
5. Analizar especialmente las comunicaciones telefónicas y telemáticas, al considerarse dos de los medios de comunicación más relevantes de la historia.

[2] Lorca Sánchez, M. Á.**,** *El derecho al secreto de las comunicaciones: Influencia de la jurisprudencia y análisis de su aplicación en la práctica jurídica*, tesis doctoral, Universitat d'Alacant/Universidad de Alicante, 2021, p. 6 (DOI: http://hdl.handle.net/10045/118895).

6. Abordar los retos legislativos actuales y perspectivas de futuro en lo relativo a las nuevas tecnologías y la protección del secreto a las comunicaciones.

4. METODOLOGÍA Y PLAN DE TRABAJO

Para realizar este estudio, aplico la metodología basada en el análisis de la doctrina, jurisprudencia y normativa. Se han utilizado fuentes normativas, como la Constitución Española, la Ley de Enjuiciamiento Criminal y diversas reformas legislativas, como la introducida en la LO 13/2015, que he comentado. Además, se han analizado sentencias tanto del Tribunal Supremo como del Tribunal Constitucional para comprender el desarrollo interpretativo de este relevante derecho fundamental.

El trabajo se divide en partes claramente definidas para abordar diferentes aspectos del derecho al secreto de las comunicaciones y su incidencia en el proceso penal. En primer lugar, se analiza su fundamentación jurídica, abarcando los diferentes tipos de comunicaciones; en segundo lugar, se examinan las excepciones, vulneraciones, y su incidencia en el proceso penal. En tercer lugar, se dedica un apartado en especial a la regulación de las comunicaciones telefónicas y telemáticas, dada su relevancia. Finalmente, se abordan las perspectivas de futuro y retos pendientes, en lo relativo a las nuevas tecnologías.

CAPITULO II: EL DERECHO AL SECRETO DE LAS COMUNICACIONES

1. CONCEPTO Y FUNDAMENTO

El derecho al secreto de las comunicaciones está regulado en la CE de 1978, concretamente en la Sección 1ª del Capítulo II del Título Primero, en su artículo 18.3., que establece: "*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*"[3]. Por tanto, se trata de un derecho fundamental, gozando así del máximo nivel de protección.

La CE asegura el derecho fundamental al secreto de las comunicaciones, por esta razón el concepto de *comunicación* es interpretado junto al término *secreto* que le precede e

[3] Constitución Española (BOE 29 de diciembre de 1978).

inevitablemente delimita. Así, solo estarán consideradas incluidas en el objeto de este derecho las comunicaciones cuyo secreto sea susceptible de ser garantizado[4].

Asimismo, el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea, expone: "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*"[5].

Según J. Ocón, para que una actividad comunicacional pertenezca al derecho fundamental debe cumplir dos requisitos. En primer lugar, que las personas intervinientes estén identificadas y, en segundo lugar, que se realice la comunicación a través de un medio técnico. El concepto de comunicación regulado en el artículo 18.3 CE consiste en que la intención sea que el mensaje llegue a conocimiento del destinatario, excluyendo a terceros, al tratarse de un mensaje privado. Por tanto, es exigible que el número de intervinientes esté determinado al inicio de la comunicación[6].

La protección del secreto de las comunicaciones debe tener las siguientes características[7]:

1. Que se realice a través de un medio de comunicación en el que exista un emisor y un receptor para intercambiar un mensaje.
2. Que el intercambio del mensaje sea entre personas separadas físicamente, entre los que exista una distancia.
3. Que sea una comunicación privada, es decir, que se excluya al resto.

Según el TS, en la sentencia 228/2015, de 21 de abril[8], el derecho al secreto de las comunicaciones está estrechamente vinculado con el derecho a la intimidad regulado en el artículo 18.1 de la CE[9]. La sentencia destaca que este derecho fundamental protege tanto el contenido de los mensajes, como a los ciudadanos frente a las posibles intromisiones en su privacidad por parte de terceros. El TS señala en la misma sentencia: "*la intimidad y el secreto de las comunicaciones son derechos fundamentales cuya restricción solo puede producirse en virtud de una resolución judicial motivada que*

[4] Ocón García, J., "Constitución y secreto de las comunicaciones: desafíos tecnológicos para el derecho fundamental", *Nuevos Horizontes del Derecho Constitucional*, núm. 2, 2022, p. 89.
[5] Carta de los Derechos Fundamentales de la Unión Europea (Diario Oficial de la Unión Europea de 30 de marzo de 2010).
[6] Ocón García, J., op.cit., p. 90.
[7] Belda Pérez-Pedrero, E., op.cit., pp. 174-175.
[8] Sentencia del Tribunal Supremo núm. 228/2015, de 21 de abril de 2015 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2015/51662].
[9] Constitución Española (BOE 29 de diciembre de 1978).

respete el principio de proporcionalidad". Asimismo, indica que cualquier medida debe ser debidamente justificada y que se deben evitar las interpretaciones excesivas puesto que derivan en medidas invasivas, lesionando los derechos fundamentales.

Es decir, en los dos supuestos se trata de derechos fundamentales relacionados entre sí, puesto que el principal objetivo del derecho al secreto de las comunicaciones es proteger la privacidad de las personas, al no ser estas comunicaciones públicas, por tanto, ahí es donde entra en juego el derecho fundamental recogido en el artículo 18.1 de la CE.

Según expone E. Belda, la posibilidad de mantener una comunicación privada ha sido relacionada estrechamente con el derecho a la intimidad regulado en el art. 18.1 CE. Es relevante destacar la notable relación entre el primer y el tercer apartado del art. 18 CE, dado que se comparte un objetivo común de garantía de las relaciones personales, no obstante, difieren en objeto[10].

2. TITULARIDAD

Según J. Ocón, la comunicación es condición de existencia de la persona, en otras palabras, los seres humanos se comunican entre sí, y su ejercicio en libertad hace que la comunicación tenga lugar entre personas que son *dominus* de ella. Por lo tanto, mantener la autenticidad e invulnerabilidad de la relación comunicativa en libertad es una meta que es particularmente complicada en relación directa con la habilidad de los actores para controlar la comunicación[11].

Un relevante problema que suele tener el análisis de un derecho fundamental es a quién se le reconoce, es decir su titularidad. En el caso de este derecho fundamental, la titularidad es de toda persona, al estar directamente relacionado con la dignidad humana, es decir, no debe haber ningún tipo de excepción específica por nacionalidad, sexo, raza…[12]

Debemos plantearnos así la titularidad de las personas jurídicas. Es cierto que su condición de derecho de la persona puede poner en duda esta característica, no obstante,

[10] Belda Pérez-Pedrero, E., op.cit., p. 170.
[11] Ocón García, J., op.cit., p. 88.
[12] Díaz Revorio, F. J., "El derecho fundamental al secreto de las comunicaciones", *Derecho PUCP*, núm. 59, 2006, p. 161.

la Audiencia Provincial de Guadalajara en la sentencia n.º 214/2017 del 8 de junio[13], expone:

"*Es cierto que el Tribunal Constitucional ha reconocido la titularidad de las personas jurídicas con respecto a algunos derechos fundamentales en concreto: la tutela judicial efectiva, incluso en lo concerniente al ejercicio de la acción popular; la inviolabilidad del domicilio; el derecho al secreto de las comunicaciones, implícitamente al menos; y el derecho al honor*".

Por tanto y según el TS en la sentencia 841/2016, de 8 de noviembre[14], se le reconoce la titularidad del derecho al secreto de las comunicaciones tanto a las personas físicas, como a las personas jurídicas.

3. EFICACIA

Como señala el TS en la sentencia 964/2021 del 10 de diciembre[15], la norma constitucional pretende claramente garantizar que no pueda ser penetrada por terceros (públicos o privados, el derecho posee eficacia *erga omnes*) ajenos a la comunicación misma, de modo que no exista "secreto" de la persona a la que se dirige la comunicación ni implica contravención del artículo 18.3 de la CE para preservar por todos los medios el contenido del mensaje.

En otras palabras, el derecho al secreto de las comunicaciones tiene como objetivo principal garantizar que un tercero ajeno a la comunicación nunca pueda tener acceso al contenido de la misma, es decir, es impenetrable. Esta protección, como bien afirma el TS, tiene carácter *erga omnes*, es decir, que obliga a todos por igual.

4. COMUNICACIONES REGULADAS

4.1 Postales

Las comunicaciones postales están reguladas en el artículo 7 del Real Decreto 437/2024, de 30 de abril, por el que se aprueba el Reglamento de los servicios postales, en desarrollo

[13] Sentencia de la Audiencia Provincial de Guadalajara núm. 214/2017, de 8 de junio de 2017 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2017/157723].
[14] Sentencia del Tribunal Supremo núm. 841/2016, de 8 de noviembre de 2016 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2016/202623].
[15] Sentencia del Tribunal Supremo núm. 964/2021, de 10 de diciembre de 2021 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2021/777954].

de lo establecido por la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal. Dicho artículo expone que los operadores postales, conforme al artículo 18 de la CE, están obligados a asegurar que se cumpla el secreto de las comunicaciones postales, la inviolabilidad de los envíos postales y la protección de datos de carácter personal. El artículo 18.3 de la CE señala que "*se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*". Esto evidencia la importancia que el Constituyente le otorga al derecho a las comunicaciones postales, situándolo junto al derecho al honor, a la intimidad personal y familiar, y a la inviolabilidad del domicilio. Además este artículo manifiesta que dicho derecho establece una prohibición absoluta para los operadores postales de desvelar datos confidenciales en relación con las comunicaciones postales, salvo autorización del destinatario o remitente[16].

Como se ha mencionado anteriormente, el artículo 18.3 de la CE señala que "*se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*". Estos derechos son derivados de la dignidad humana y están dirigidos a proteger el patrimonio moral de las personas.

Asimismo, según la sentencia del TC 281/2006, de 9 de octubre[17], "*la existencia de la comunicación, la identidad de los corresponsales, el momento en el que se produce, los lugares de remisión y destino, son todos ellos datos que, una vez iniciado el proceso de comunicación, son secretos para cualquier persona ajena a la comunicación. El conocimiento de esta información por quien presta el servicio postal solo puede ser utilizado a los efectos de la prestación del servicio*".

Esta regulación muestra cómo, a pesar del gran avance tecnológico que se ha producido a lo largo de los años, la comunicación postal no ha perdido relevancia, pese a ser una comunicación tradicional. El hecho de que la CE mencione las comunicaciones postales, refleja cómo es un tipo de comunicación que sigue en auge, manteniendo la confidencialidad entre los ciudadanos.

[16] Real Decreto 437/2024, de 30 de abril**,** por el que se aprueba el Reglamento de los servicios postales (BOE 18 de mayo de 2024).
[17] Sentencia del Tribunal Constitucional núm. 281/2006, de 9 de octubre de 2006 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2006/273570].

4.2 Telegráficas

El telégrafo se utiliza en España desde el año 1850 aproximadamente. El uso de dicha herramienta implica, además de los interlocutores, la intervención de al menos dos personas más –(los encargados de transmitir y recibir el mensaje)- que, debido a su rol en el proceso, tienen acceso al contenido del mensaje. Estos intervinientes deben, legalmente, guardar el secreto comunicativo[18].

Pese a que el telégrafo está considerado como un medio tradicional, la jurisprudencia más actual los incluye en el ámbito de la garantía constitucional.

4.2 Telefónicas

La reforma de la LO 13/2015, de 5 de octubre, se expande a las comunicaciones telefónicas y telemáticas. La gran diferencia entre ambos tipos de comunicación se encuentra en el medio utilizado en cada caso: telefónica, cuando se utilice un teléfono para generar el mensaje que se comunica; y telemática, cuando se utilice un sistema informático[19].

Está claro que las comunicaciones telefónicas han experimentado una increíble evolución tecnológica con el surgimiento de las plataformas de comunicación digitales como las aplicaciones como: *Zoom*, *WhatsApp*, etc. Por esta razón, es por la que las comunicaciones telefónicas son las más utilizadas hoy en día en el siglo XXI.

CAPITULO III: VULNERACIÓN DEL SECRETO DE LAS COMUNICACIONES

1. RÉGIMEN JURÍDICO

Cuando se cumplen los presupuestos del artículo 18.3 de la CE que regula el derecho al secreto de las comunicaciones, ya es posible que se aprecie una vulneración de dicho derecho.

[18] Díaz Revorio, F. J., op. cit, p. 163.
[19] Martínez Polo, P. O., y Sandoval Pérez, K. D. P., "La intervención del Ministerio Público en los requerimientos del levantamiento del secreto de las comunicaciones telefónicas y su vulneración a los derechos fundamentales", *Tesis de Grado*, p. 36 (DOI: https://hdl.handle.net/20.500.12692/97119).

Para que se pueda estimar que existe una vulneración, son necesarios dos requisitos esenciales[20]:

1. Que concurran uno o varios terceros ajenos al proceso comunicador sin conocimiento de uno o de todos los comunicantes. En caso de que los intervinientes desvelen el mensaje, sería posible que se deriven consecuencias según afecte al derecho de la intimidad, o al secreto profesional.
2. Que exista una intención clara de intervenir en el proceso comunicativo y no sea fruto de una casualidad. Es importante mencionar que cuando, sin intención, un tercero tenga acceso a una comunicación personal de otros, es una situación jurídicamente irrelevante.

Por tanto, como señala el TS en su sentencia 864/2015 de 10 de diciembre[21], el derecho se vulnera a través de la interceptación en sentido estricto, es decir, cuando se aprehende físicamente el mensaje, se captura el proceso de comunicación o se accede al contenido, y, en segundo lugar, con el conocimiento antijurídico de la comunicación es decir, el hecho de acceder sin autorización a comunicaciones ya emitidas, como por ejemplo abrir correspondencia ajena, leer correos electrónicos o consultar mensajes de telefonía móvil sin consentimiento. El secreto protege tanto el contenido, como los datos externos de la comunicación, como puede ser la identidad de los interlocutores.

2. CASOS EXCEPCIONALES

A pesar de ser el derecho al secreto de las comunicaciones un derecho constitucional, según la Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas, existen varios supuestos en los que no se considera vulnerado dicho derecho[22].

[20] Belda Pérez-Pedrero, E., op.cit., pp. 175-176.
[21] Sentencia del Tribunal Supremo núm. 864/2015, de 10 de diciembre [versión electrónica – base de datos Lefebvre. Ref. EDJ 2015/269989].
[22] Circular 2/2019, de 6 de marzo, sobre interceptación de comunicaciones telefónicas y telemáticas (BOE 22 de marzo de 2019).

2.1 Las conversaciones grabadas o difundidas por uno de los interlocutores

Según el TS en la sentencia 964/2021, de 10 de diciembre[23], "*el artículo 18.3 de la Constitución no es aplicable entre los interlocutores de una comunicación, pues no existe secreto de las comunicaciones entre quienes mantienen o son destinatarios de una comunicación electrónica o epistolar*". Entre los interlocutores participantes en la conversación no existe secreto, es decir, el acceso al conocimiento de la información por el interlocutor es totalmente lícito, ya que cuenta con el poder de poseer esta información.

La ilegalidad podría originarse en un momento posterior; cuando se haga uso de esta información almacenada de forma privada. El TS concluye que quien graba una conversación de terceros vulnera el derecho reconocido en el artículo 18.3. CE, no obstante, quien graba una conversación en el que él actúa como interlocutor o destinatario, no incurre por este solo hecho en conducta contraria a la CE.

La protección del derecho fundamental referido, no tiene por objeto proteger al interlocutor, emisor o destinatario frente a otros intervinientes en la comunicación. En esta línea, la jurisprudencia ha subrayado reiteradamente que el derecho al secreto de las comunicaciones no puede extenderse a los participantes de la conversación puesto que, como se ha mencionado anteriormente, no existe secreto entre ellos.

2.2. Las comunicaciones por radio

El TS, en la sentencia 695/2013 del 22 de julio[24], expone que "*las captaciones de conversaciones radiotelegráficas, en frecuencia de uso público, no precisan autorización judicial, porque precisamente por ser de uso público y siendo esto conocido por los usuarios, ello implica una implícita aceptación de la posibilidad de captación*".

Es decir, el TS manifiesta que al tratarse de conversaciones radiotelegráficas sin estar limitadas y de uso abierto, los usuarios intervinientes aceptan implícitamente los riesgos de que sus conversaciones pueden ser captadas por terceros, al tratarse de un uso público.

[23] Sentencia del Tribunal Supremo núm. 964/2021, de 10 de diciembre de 2021 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2021/777954].
[24] Sentencia del Tribunal Supremo núm. 695/2013, de 22 de julio de 2013 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2013/174352].

2.3. Acceso a la memoria o contactos de un teléfono móvil

El acceso a los datos contenidos en la agenda de contactos de un teléfono móvil por parte de las autoridades policiales no vulnera el derecho al secreto de las comunicaciones.

El TS en la sentencia 87/2020 del 3 de marzo[25] estima, haciendo referencia a la sentencia del TC 115/2013, que con el acceso a la agenda de contactos del teléfono móvil los agentes de policía no obtienen datos sobre un proceso de comunicación, sino solamente un listado de números de teléfono introducidos voluntariamente por el usuario del dispositivo, equiparable a una agenda en papel. El TC considera que esta actuación no afecta al derecho al secreto de las comunicaciones, sino únicamente al derecho a la intimidad recogido en el art. 18.1. CE.

La intervención de las comunicaciones requiere siempre de autorización judicial, pero el derecho a la intimidad no prevé esta misma garantía, por lo que se admite que la policía realice determinadas prácticas que vulneren ligeramente el derecho a la intimidad de las personas sin previa autorización judicial, siempre que: (1) exista la suficiente habilitación legal, (2) la misma resulte justificada con arreglo a los criterios de urgencia y necesidad y (3) se cumpla el requisito de proporcionalidad al ponderar los intereses en juego en el caso concreto[26].

La diferencia será, en caso de que las autoridades policiales acceden a cualquier otra función del móvil, cómo puede ser el acceso al registro de llamadas salientes y entrantes.

Es relevante destacar que el apartado hace referencia al acceso policial a dispositivos propiedad de personas detenidas. En el supuesto en el que una persona física acceda al contenido de un teléfono móvil de otro particular sin su consentimiento, constituiría un delito contra la intimidad previsto en el art. 197.1 del Código Penal[27].

2.4. Visionado directo de un número de teléfono entrante

[25] Sentencia del Tribunal Supremo núm. 87/2020, de 3 de marzo de 2020 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2020/515843].
[26] El Derecho, "¿Pueden acceder los agentes de policía al registro de llamadas del teléfono móvil del detenido?", *El Derecho*, 27 de abril de 2020 (DOI: https://elderecho.com/pueden-acceder-los-agentes-policia-al-registro-llamadas-del-telefono-movil-del-detenido).
[27] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (BOE 24 de noviembre de 1995).

El TS en la sentencia 264/2018 del 31 de mayo[28] expone que los datos obtenidos en el volcado del teléfono, tanto la agenda telefónica como el contenido de los mensajes, no afectan al secreto de las comunicaciones, sino al derecho a la intimidad, sin que fuera preciso, en tales supuestos y en todo caso, la previa autorización judicial.

No obstante, el tribunal destaca que sí que existiría intromisión en caso de que las autoridades policiales accedieran a una carta abierta que el detenido llevaba consigo en el momento de la detención.

2.5. La conversación escuchada por agentes policiales a través del modo "manos libres" de uno de los interlocutores que accede a ello

El TS en la sentencia 681/2017 del 18 de octubre[29], declara que la conversación entre los interlocutores y escuchada por las autoridades policiales, siempre y cuando sea a través del manos libres o un amplificador, no supone una vulneración del derecho, puesto que los intervinientes han consentido la difusión de la conversación en ese entorno.

Es destacable que la jurisprudencia señala que el derecho al secreto de las comunicaciones protege el canal de transmisión, no protege la información una vez ha sido recibida por uno de los particulares.

CAPITULO IV: INTERVENCIÓN DE LAS COMUNICACIONES EN EL PROCESO PENAL

1. RÉGIMEN JURÍDICO Y REFORMA INTRODUCIDA POR LA LO 13/2015, DE 5 DE OCTUBRE

La LO 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'[30], pone fin a las deficiencias y lagunas jurídicas que inundaba

[28] Sentencia del Tribunal Supremo núm. 264/2018, de 31 de mayo de 2018 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2018/511347].
[29] Sentencia del Tribunal Supremo núm. 681/2017, de 18 de octubre de 2017 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2017/218369].
[30] 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. (BOE 6 de octubre de 2015).

nuestra legislación que regulaba el derecho al secreto de las comunicaciones, según J.L. González-Montes, profesor titular de Derecho Procesal[31].

El TEDH, a lo largo de los años, venía reclamando una reforma legislativa, lo que hizo que el TC y el TS establecieran una serie de criterios para resolver esas lagunas existentes en el ordenamiento. Por esta razón tuvo lugar la reforma de la LECrim de la LO 13/2015, de 5 de octubre; esta reforma consigue completar la regulación de dicho derecho y fortalece las garantías procesales[32]. Asimismo, esta reforma promueve una mayor seguridad jurídica y poder luchar eficazmente contra la delincuencia.

El legislador español ha tratado de presentar un marco normativo más completo y sólido para la interceptación de las comunicaciones. La ley proporciona más controles judiciales y procesales, con el objetivo de que la intervención en el secreto de las comunicaciones se haga debidamente y justificadamente, al tratarse de un derecho fundamental muy relevante.

Asimismo, la adaptación normativa se llevó a cabo asegurando la conformidad con los estándares constitucionales y europeos, a través de la trasposición de dos Directivas; la Directiva 2013/48/UE sobre asistencia letrada y la Directiva 2014/42/UE sobre embargo y decomiso de los instrumentos y del producto del delito en la UE.

Por tanto, dado que la situación de desarrollo de las nuevas tecnologías ha supuesto un antes y un después, se puso de manifiesto la necesidad de afrontar ciertas cuestiones que no podían esperar a la promulgación de un nuevo texto normativo que sustituyera a la LECrim; (1) la necesidad de establecer disposiciones eficaces de agilización de la justicia penal que eviten dilaciones indebidas, (2) el fortalecimiento de los derechos procesales de conformidad con las exigencias del Derecho de la UE, (3) la regulación de las medidas de investigación tecnológica, (4) la previsión de un procedimiento de decomiso

[31] González-Montes Sánchez, J. L., "Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", *Revista Electrónica de Ciencia Penal y Criminología*, núm. 17, 2015, p. 5 (DOI: http://criminet.ugr.es/recpc).

[32] Elso Montanary, Í., *Reflejo de la doctrina jurisprudencial en la regulación de la intervención de las comunicaciones en la Ley Orgánica 13/2015, de 5 de octubre*, Trabajo de Fin de Grado, Universidad de Valladolid, 2019 (DOI: http://uvadoc.uva.es/handle/10324/38396).

autónomo, (5) la instauración de la segunda instancia y (6) la reforma de la revisión penal[33].

La reforma de la LO 13/2015 era tanto urgente como necesaria, sobretodo en un contexto de constante evolución como son las comunicaciones. Esta reforma ha proporcionado una regulación más concreta y detallada, mientras que la normativa previa a esta reforma estaba anclada en el pasado. Es cierto que esta reforma precisa de cambios, no obstante, es un buen primer paso hacia un futuro en el que las comunicaciones estén mejor reguladas.

2. PROCEDIMIENTO Y GARANTÍAS PROCESALES

El capítulo IV de la LECrim trata sobre las disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas como una medida de investigación tecnológica que afecta de manera directa al derecho fundamental del secreto de las comunicaciones. Al tratarse de una intromisión en un derecho fundamental, su aplicación está sujeta a requisitos procesales y controles judiciales[34].

El Juez de instrucción es el competente para autorizar la medida para la intervención, asegurando la supervisión judicial del proceso penal. No obstante, es relevante destacar que el juez de guardia también puede llevarla a cabo en situaciones de urgencia, debiendo ser ratificada posteriormente[35].

El artículo 588 bis.a LECrim[36] manifiesta que "*durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo, siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida*".

[33] Rayón Ballesteros, M. C., "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", *Anuario Jurídico y Económico Escurialense*, núm. 52, 2019, pp. 181-182.
[34] Gascón Inchausti, F., *Derecho procesal penal: Materiales para el estudio*, 6ª edición, Universidad Complutense de Madrid, 2024, pp. 170-171.
[35] Lorca Sánchez, M. Á., op. cit, p. 198.
[36] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (BOE 17 de septiembre de 1882).

Las medidas de investigación tecnológica para la interceptación de las comunicaciones, según el artículo 588 bis.b LECrim, se acordarán por el Juez, o a instancia de la policía judicial o del Ministerio Fiscal.

El contenido del oficio de solicitud es importante, ya que la posterior resolución judicial se fundamentará en las razones y argumentos expuestos en la solicitud inicial. La jurisprudencia ha establecido que la autorización de la intervención debe contar con una justificación. En esta línea, el TS en la sentencia 634/2019 de 19 de diciembre, reafirma que el control judicial es la principal garantía del sistema procesal, también obliga a cumplir los principios de necesidad y proporcionalidad.

El apartado tercero del artículo 588 bis.c LECrim dispone que la petición del Ministerio Fiscal o la Policía Judicial deberá contener los siguientes extremos: (1) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida, (2) la identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido, (3) la extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a, (4) a unidad investigadora de Policía Judicial que se hará cargo de la intervención, (5) la duración de la medida, (6) la forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida, (7) la finalidad perseguida con la medida, (8) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

Este procedimiento es esencial para asegurar un equilibrio entre la eficacia de la investigación penal y el respeto a los derechos fundamentales. La interceptación de las comunicaciones, como se ha reflejado, es un recurso muy invasivo, por lo cual las garantías como por ejemplo el control judicial, son estrictamente necesarias para garantizar la legitimidad de dicha medida, evitando así un uso abusivo.

Por otro lado, la colaboración de las operadoras de telecomunicaciones es esencial en la ejecución de la medida de intervención. Estas instituciones deben asegurar la interceptación de manera legal y con todas las salvaguardias necesarias. Sin embargo, su

actuación debe ajustarse al principio de proporcionalidad y estar limitada a los casos autorizados judicialmente[37].

En conclusión, la interceptación de las comunicaciones es una medida excepcional en el proceso penal y debe ser aplicada con las máximas garantías posibles para tratar de no vulnerar el derecho fundamental al secreto de las comunicaciones.

3. REQUISITOS DE LA INTERVENCIÓN: PROPORCIONALIDAD, NECESIDAD Y CONTROL JUDICIAL

El derecho al secreto de las comunicaciones debe respetarse, aunque la información transmitida no se integre en el ámbito de la privacidad. Este derecho no es de carácter absoluto, pues en toda sociedad democrática existen determinados valores que pueden justificar con las debidas garantías su limitación[38].

Existen tres principios esenciales; proporcionalidad, necesidad y control judicial.

En primer lugar, el principio de proporcionalidad regula la relación de la lesión del derecho fundamental con el fin perseguido. El artículo 588 bis.a.5. de la LO 13/2015 indica que "las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

Según L. Bachmaier, el principio de proporcionalidad es la relación que existe entre el fin perseguido (la persecución del delito), frente a la lesión del derecho fundamental. El legislador de la reforma de la LO 13/2015 indica los elementos en los que debe basarse

[37] Lorca Sánchez, M. Á., op. cit, p. 159.
[38] Mitran, G. D., *La intervención de las comunicaciones telefónicas y telemáticas*, Trabajo de Fin de Grado, Universidad de Almería, 2021, p. 11 (DOI: http://hdl.handle.net/10835/13187).

el juez para ponderar los intereses a la hora de decidir sobre una medida de investigación telemática[39].

En segundo lugar, el principio de necesidad está regulado en el artículo 588 bis.a.4 LECrim. Dicho artículo señala que "en aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida".

Según F. Gascón, la necesidad significa que no exista al alcance de la autoridad, del Estado, otro instrumento menos lesivo para alcanzar el mismo fin con un grado análogo de eficacia[40].

La intervención de las comunicaciones debe ser una medida de última instancia, empleándose en caso de que no exista otra alternativa viable. Solo se recurrirá a la misma en ausencia de opciones menos lesivas.

Además, resulta necesario que esta diligencia sea indispensable para la investigación del hecho punible y la determinación de su autor, sin que se puedan determinar tales extremos a través de otro medio probatorio[41].

En tercer lugar, esta medida solo podrá acordarse previa autorización judicial, a petición de la Fiscalía o de la Policía Judicial. La solicitud de autorización, deberá contener[42]:

- La identificación del número de abonado, del terminal o de la etiqueta técnica
- La identificación de la conexión objeto de la intervención o

[39] Bachmaier Winter, L., "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *Boletín del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes*, núm. 2195, 2017, p. 16 (DOI: https://revistas.mjusticia.gob.es/index.php/BMJ/article/view/2827).
[40] Gascón Inchausti, F., op. cit., p. 163.
[41] López-Barajas Perea, I., "Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la Ley", *Revista de Derecho Político*, núm. 98, 2017, p. 107 (DOI: https://doi.org/10.5944/rdp.98.2017.18652).
[42] Lorca Sánchez, M. Á., op. cit., p. 100.

- Los datos necesarios para identificar el medio de telecomunicación de que se trate.

Este control se mantiene sostenido en el tiempo. Según el artículo 588 ter.g LECrim, la duración máxima inicial de la intervención, que se computará desde la fecha de autorización judicial, será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses, lo cual impide duración de la intervención invasiva *sine die* en su dimensión temporal[43].

Según la Sala de lo Penal del TS en la sentencia 153/2015, de 18 de marzo[44], el requisito del control judicial es esencial en la adopción de la medida. El fallo de la sentencia señala que la intervención de las comunicaciones necesita un control judicial efectivo, lo que significa un análisis razonado por parte del juez sobre el principio de necesidad y de proporcionalidad de la medida. La ausencia de dicho análisis puede conducir a la nulidad de la prueba obtenida, como pasó en esta sentencia, que implica un análisis razonado y motivado por parte del juez sobre la proporcionalidad y necesidad de la medida. La falta de este análisis puede llevar a la nulidad de la prueba obtenida, como ocurrió en este caso.

4. IMPLICACIONES PRÁCTICAS EN LA OBTENCIÓN Y VALORACIÓN DE LA PRUEBA

La obtención y valoración de la prueba en el proceso penal, presenta numerosas dificultades, sobre todo con respecto a los derechos fundamentales, como es, en este caso, la intervención de las comunicaciones. La jurisprudencia ha desarrollado varios criterios para determinar la licitud de las pruebas obtenidas mediante este tipo de medidas, imponiendo los limites necesarios. En esta línea, es necesario analizar casos reales en los que se plantearon este tipo de problemas.

El TC en la sentencia 61/2021 de 15 de marzo[45], abarcó un caso en el que tanto el juzgado de lo Social, como la como la Sala de lo Social del Tribunal Superior de Justicia de Madrid, aceptaron la exclusión probatoria de una prueba documental al tratarse de una prueba en la que la empresa monitorizó todo lo que la trabajadora hacía en su ordenador

[43] Gascón Inchausti, F., op. cit., p. 175.
[44] Sentencia del Tribunal Supremo núm. 153/2015, de 18 de marzo de 2015 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2015/36426].
[45] Sentencia del Tribunal Constitucional núm. 61/2021, de 15 de marzo de 2021 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2021/515845].

de trabajo; captaron todo lo que tenía en su ordenador y utilizaron esta información para su despido. Por tanto, el TC concluyó que dicha prueba había sido obtenida con vulneración del derecho a la intimidad y al secreto de las comunicaciones, por lo que la prueba fue anulada.

Este caso refleja una gran dificultad que existe en la obtención y valoración de la prueba cuando se relaciona con vulnerar un derecho fundamental.

En contraste, en el ámbito contencioso-administrativo, los tribunales han determinado que la valoración de la prueba de una intervención en las comunicaciones no siempre implica una vulneración de garantías procesales, sobre todo cuando existe una autorización judicial firme.

De este modo, el TS en la sentencia 135/2025 del 7 de febrero[46], abordó un caso en el que enjuiciaron la admisión de la prueba que se obtuvo por la Administración Tributaria, debido a que posiblemente vulneraba el derecho a la inviolabilidad del domicilio regulado en el artículo 18.2 CE. El Tribunal concluyo que la admisión y valoración de la prueba no vulneraban las garantías del procedimiento, puesto que la única conexión jurídica entre la lesión del derecho fundamental y la obtención de la prueba es la valoración sobre la autorización judicial firme. En este sentido, el fallo destaca que la jurisprudencia ha establecido criterios más estrictos para validar las pruebas obtenidas en este ámbito.

Según el artículo 11.1 de la Ley Orgánica del Poder Judicial[47]: "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". La regla de exclusión establecida en este artículo no implica la anulación sistemática de toda prueba obtenida irregularmente; en esta línea la doctrina establece que la nulidad puede darse con pruebas indirectamente ilícitas, cuando deriven de una vulneración previa. Este concepto es conocido como "fruto del árbol envenenado[48]".

[46] Sentencia del Tribunal Supremo núm. 135/2025, de 7 de febrero de 2025 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2025/508319].
[47] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).
[48] Casas Baamonde, M. E., "¿Una "tercera" doctrina judicial sobre la prueba ilícita por vulneración de derechos fundamentales y sus efectos en la calificación del despido?", *Revista de Jurisprudencia Laboral*, núm. 3, 2023, p. 10 (DOI: https://doi.org/10.55104/RJL_00430).

Desde un punto de vista jurisprudencial, la prueba ilícita ha sido un concepto de amplio debate en el derecho procesal penal. En este sentido, las resoluciones del TC han desarrollado los efectos de la ilicitud probatoria.

En particular, el principio de exclusión probatoria impide utilizar pruebas que se han obtenido lesionando derechos fundamentales, dado que atenta contra los mismos, no obstante, esta regla no es absoluta, sino que cuenta con excepciones; como la doctrina del "descubrimiento inevitable" o la ruptura del nexo causal, las cuales permiten la obtención de pruebas que, aunque derivadas de fuentes ilícitas, han sido obtenidas independiente y legítimamente[49].

Otra cuestión relevante es el alcance del control judicial en la revisión de las pruebas obtenidas. El TS en la sentencia 54/2024, de 18 de enero[50], ha reafirmado que el control judicial sobre la valoración probatoria en casación debe respetar los principios de inmediación y contradicción. En esta misma línea, el artículo 849.2 de la LECrim exige que el error en la apreciación probatoria "*ha de fundarse en una verdadera prueba documental*" y que esta "*ha de evidenciar el error de algún dato o elemento fáctico o material de la sentencia de instancia, por su propio y literosuficiente poder demostrativo directo, es decir, sin precisar de la adición de ninguna otra prueba ni tener que recurrir a conjeturas o complejas argumentaciones".* Asimismo, se establece que *"el dato que el documento acredite no se encuentre en contradicción con otros elementos de prueba, pues en esos casos no se trata de un problema de error sino de valoración, la cual corresponde al Tribunal, art. 741 LECrim*". En esta sentencia el TS sostiene que la casación no autoriza una nueva valoración de la prueba, sino la corrección del relato de hechos demostrados cuando su existencia o inexistencia resultan incuestionables basándose en un documento especifico.

Por último, en este contexto, se plantea el debate entre la exclusión de la prueba y el derecho a la defensa, puesto que eliminar una prueba puede suponer la imposibilidad de utilizar una prueba que puede considerarse clave para el proceso. La exclusión de la prueba puede llegar afectar al derecho del acusado a presentar todos los medios de prueba

[49] Bohigues Esparza, M. D., "La ilicitud de la prueba con vulneración de derechos fundamentales. A propósito de la sentencia del Tribunal Constitucional núm. 61/2021 de 15 de marzo", *IUSLabor. Revista d'anàlisi de Dret del Treball*, núm. 2, 2021, p. 271 (DOI: https://doi.org/10.31009/IUSLabor.2021.i02.9).
[50] Sentencia del Tribunal Supremo núm. 54/2024, de 18 de enero de 2024 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2024/501917].

pertinentes para su defensa, por lo que se presenta el conflicto entre la protección de los derechos fundamentales y la tutela judicial efectiva, regulada en el artículo 24.2 CE. El TC ha señalado que aunque existen criterios y requisitos claros para la aplicación de excepciones a la regla de exclusión, sigue habiendo un margen de discrecionalidad judicial que exige un análisis caso por caso[51].

Este problema relativo a la obtención y valoración de la prueba quedó regulado en la LO 13/2015, la cual aumentó las garantías para evitar la lesión a los derechos fundamentales. Sin embargo, la aplicación práctica sigue generando disputas como se ha reflejado a lo largo de este apartado.

CAPITULO V: INTERVENCIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS EN ESPECIAL

Como se menciona durante todo el trabajo, el derecho al secreto de las comunicaciones consagrado en el artículo 18.3 CE es un derecho muy amplio. En la actualidad, existen numerosas formas de comunicación, no obstante, las comunicaciones telefónicas han adquirido una posición considerablemente relevante dentro del proceso penal. A pesar de las nuevas tecnologías, las telefónicas siguen siendo claves en este ámbito.

1. EVOLUCIÓN NORMATIVA

Antes de la entrada en vigor de la reforma de la LO 13/2015, la jurisprudencia y la doctrina llevaban años reclamando una puesta al día de las herramientas de investigación de nuestro proceso penal. La sentencia 850/2014 de 26 de noviembre del TS[52] es un claro ejemplo de dicha petición de reforma; el Tribunal se pronunciaba así: "*La intervención de las comunicaciones telemáticas carece de regulación legal expresa en nuestro ordenamiento procesal penal, laguna que es preciso subsanar con la máxima urgencia, dada la relevancia de los derechos fundamentales e intereses generales en conflicto. La doctrina jurisprudencial ha realizado un considerable esfuerzo para subsanar este*

[51] Sanchís Marín, Á. J., *La prueba ilícita en el proceso penal: La regla de exclusión*, Trabajo de Fin de Grado, Universidad Pontificia Comillas (ICADE), 2023, p. 2 (DOI: http://hdl.handle.net/11531/72147).
[52] Sentencia del Tribunal Supremo núm. 850/2014, de 26 de noviembre de 2014 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2014/222781].

déficit, que afecta a la calidad democrática de nuestro sistema de investigación penal, por la vía de la asimilación de las comunicaciones telemáticas al régimen de las intervenciones telefónicas, lo que implica, con carácter general, la exigencia de autorización judicial sujeta a los principios de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad de la medida".

Debido a esta regulación tan pobre, el Tribunal Europeo de Derechos Humanos en el año 2003 declaró vulnerado el artículo 8 del Convenio de Roma (Derechos y Libertades Públicas) en su sentencia de 18 de febrero de 2003. España fue condenada por el TEDH con el objetivo de que el legislador impulsara una reforma de la LECrim. Como se comenta más adelante, dicha reforma fue llevada a cabo doce años después de la condena[53].

En el año 2012 se intentó llevar a cabo una reforma de la LECrim a través del Código Procesal Penal, no obstante, no se consiguió. Por lo que en el año 2015 se modernizó la LECrim con la LO 13/2015, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, y con la Ley 41/2015, de modificación de la LECrim para la agilización de la justicia penal y el fortalecimiento de las garantías procesales.

Fracasado ese intento, se trató de modernizar la LECrim a través de dos leyes: la LO 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 y la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales[54].

2. PARTICULARIDADES DE LA INTERVENCIÓN TELEFÓNICA FRENTE A OTROS MEDIOS DE COMUNICACIÓN

El correo electrónico está considerado como uno de los principales medios, junto con las telefónicas, permitiendo el traspaso de información instantáneo. Existe una gran

[53] Velasco Perdigones, J. C., *Las intervenciones telefónicas y el secreto de las comunicaciones. Estado de la cuestión en la jurisprudencia,* s.f, p.2.
[54] Sanchis Crespo, C., "Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas", *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, núm. 125, 2017, p. 3.

diferencia entre las comunicaciones telefónicas y los correos electrónicos; las telefónicas se interceptan con inmediatez y tienen naturaleza efímera, mientras que los correos crean un registro escrito, almacenando todos los mensajes enviados, por lo que puede consultarse en cualquier momento. Este medio de comunicación ha dado lugar a un debate, puesto que las telefónicas cuentan con una regulación más consolidada que los correos, lo cual cuenta con más vacíos legales.

J.C. Velasco destaca las diferencias existentes entre la intervención telefónica y la del correo electrónico en el proceso penal español.

En primer lugar, en lo relativo a los requisitos legales, los medios telefónicos solo tendrán la condición de legítimos cuando cumplan el artículo 588 bis a) LECrim; la autorización judicial, el principio de legalidad, principio de especialidad, principio de idoneidad, principios de excepcionalidad y necesidad y principio de proporcionalidad, denominados como los principios rectores[55].

No obstante, la intervención de correos electrónicos presenta una ambigüedad real, puesto que mediante la afirmación "cesión de datos electrónicos", pueden obtenerse datos sin un límite claro, lo cual supone un riesgo para la inviolabilidad de las comunicaciones.

La intervención telefónica permite alcanzar las conversaciones en tiempo real, es decir en el tiempo en el que dure la llamada, autorizando así la escucha y la grabación en curso. No obstante, la diferencia con la intervención de correos electrónicos es que estos permiten el acceso al almacenamiento de correos almacenados, en cualquier momento, lo que genera dudas sobre cuestiones de privacidad y protección de datos[56].

Asimismo, existen notables diferencias en lo relativo a la regulación legal de ambos medios. Las llamadas telefónicas requieren, como se ha hecho referencia anteriormente, autorización judicial motivada y que los principios rectores del artículo 588 bis.a) LECrim estén bien definidos. Sin embargo, la legislación de los correos electrónicos es más ambigua en este sentido, por lo cual ofrece menos límites para actuar y deja un mayor margen de interpretación[57].

[55] Velasco Perdigones, J. C, op. cit. p. 5.
[56] Pérez Gil, J., "Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución", en *Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli*, Aracne, 2018, p. 6.
[57] Gimeno Sendra, J.V., *Manual de Derecho Procesal Penal*, Editorial Tirant lo Blanch, 2020, p. 414.

En resumen, las intervenciones telefónicas tienen una doble naturaleza en el proceso penal; pueden servir tanto como fuente de investigación de delitos, como prueba, por tanto, se requiere una exigencia imprescindible que cumplan la regulación correspondiente, mientras que la regulación del correo electrónico ofrece un margen más amplio.

Por otro lado, el medio *WhatsApp* está llegando ser un recurso fundamental y novedoso en la comunicación, con validez y eficacia en el proceso penal; su extensión global y uso generalizado en la sociedad muestra la importancia que está obteniendo en la actualidad[58].

Como se ha reflejado anteriormente, las comunicaciones telefónicas han sido consideradas el principal medio de comunicación en la historia, por lo que su regulación ha evolucionado a lo largo de los años. No obstante, debido al uso masivo y global del medio de comunicación *WhatsApp*, es relevante destacar que este medio de comunicación permite, tanto el envío de mensajes escritos de manera instantánea, como la realización de llamadas y video llamadas.

Estas vías de comunicación –llamadas de voz por un lado y texto por otro- poseen muchas diferencias frente a las comunicaciones telefónicas. Por tanto, ante la importancia del medio *WhatsApp*, resulta relevante analizar su valor probatorio.

Según A. Martínez, las llamadas telefónicas son captadas en tiempo real, lo que hace imposible su manipulación. Mientras que, por otro lado, las pruebas obtenidas a través de *WhatsApp* solo pueden alcanzarse mediante los dispositivos de los usuarios, lo que provoca una baja autenticidad y una posible manipulación, puesto que las personas pueden eliminar o alterar los mensajes[59].

Según el TS en la sentencia 300/2015 de 19 de mayo[60] establece que el medio preferido por la jurisprudencia para acreditar la autenticidad del contenido del mensaje obtenido, es la práctica de una prueba pericial informática. Por lo que será estrictamente necesaria dicha prueba para autenticar dichos mensajes.

[58] Martínez Guerrero, A., "Incorporación de los WhatsApp y otras aplicaciones semejantes de mensajería electrónica al proceso penal en la fase de instrucción", *Revista Acta Judicial*, núm. 10, 2022, p. 21.
[59] Martínez Guerrero, A., "A vueltas con el whatsapp y semejantes como fuente de prueba en la fase instructora del proceso penal", *Revista Claves Jurídicas,* pp. 2-21 (DOI: https://www.clavesjuridicas.com/index.php/raj/article/view/117).
[60] Sentencia del Tribunal Supremo núm. 300/2015, de 19 de mayo de 2015 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2015/77775].

En esta misma línea, J.F. Soto expresa que la fácil manipulación de los mensajes y llamadas de los usuarios en *WhatsApp,* la convierten en la aplicación que más problemas ocasiona como medio de prueba en ilícitos penales[61]. El principal inconveniente de *WhatsApp* es su volatilidad, intangibilidad, lo que hace que sean manipulables provocando que la parte contraria impugne la autenticidad de la prueba[62]. Javier Rubio, perito informático del Colegio de Ingenieros en Informática de Madrid, indica: "*la manipulación de los mensajes recibidos de WhatsApp es sencilla y no deja rastro, pues «altera directamente la base de datos de la aplicación en el terminal del usuario*".

Por tanto, la posible y probable manipulación del contenido de las comunicaciones de *WhatsApp* plantea dudas sobre su fiabilidad probatoria, lo que la diferencia de las comunicaciones telefónicas, un medio mejor regulado y seguro.

3. LÍMITES Y CONTROL JURISPRUDENCIAL EN LA INTERVENCIÓN DE COMUNICACIONES TELEFÓNICAS

A pesar de que el derecho al secreto de las comunicaciones esté garantizado en el artículo 18.3 CE y esté considerado como derecho fundamental al estar regulado por el Título Primero, puede ser restringido en casos excepcionales. Por ello, existen varios límites y principios establecidos por la jurisprudencia para evitar el abuso y asegurar el respeto al derecho fundamental.

El primer límite del derecho es la reserva judicial y la autorización motivada. La LECrim establece que el Juez de Instrucción será quien autorice o deniegue la medida de intervención, a través de auto motivado y oído el Ministerio Fiscal[63]. Este requisito es el más importante puesto que, en caso de que no lo autorice el juez competente, el derecho al secreto de las comunicaciones se considerará vulnerado.

En esta línea, el TS en la sentencia 634/2019 de 19 de diciembre[64], reafirma que la intervención del juez de instrucción constituye la principal garantía que arbitra nuestro sistema jurídico. Esta garantía está sujeta a unas exigencias inexcusables: (a) motivación,

[61] Soto Campillo, J. F., *WhatsApp: como medio de prueba en el procedimiento penal*, Trabajo de Fin de Grado, Universidad Miguel Hernández, 2017, p. 57 (DOI: http://hdl.handle.net/11000/7100).
[62] Soto Campillo, J. F., op. cit., p. 59.
[63] Estévez Díaz, S., La intervención telefónica en el proceso penal español como diligencia de intervención y medio de prueba, Trabajo de Fin de Grado, Universidad de la Laguna, p.16.
[64] Sentencia del Tribunal Supremo núm. 634/2019, de 19 de diciembre de 2019 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2019/785654].

(b) competencia del juez, (c) resolución judicial dictada en un proceso jurisdiccional, (d) resolución adoptada para la averiguación de un delito con sujeción a los principios de excepcionalidad, temporalidad y proporcionalidad y (e) sujeción de la medida a un estricto control judicial en su ejecución.

El segundo límite del derecho son los principios de proporcionalidad y necesidad. La intervención de las comunicaciones debe estar debidamente justificada. El principio de proporcionalidad se ha introducido a través de la reforma de la LO 13/2015, estableciendo el artículo 588 bis.a) LECrim los principios que deben cumplirse, y en el artículo 588 bis.c) LECrim la obligación de designar la finalidad perseguida con la medida.

El principio de proporcionalidad establece que la investigación debe enfocarse en descubrir y eliminar delitos que justifican una injerencia en derechos fundamentales, cuya definición debe efectuarse no solo en función de la sanción establecida para el delito, sino también en reproche social que puede llegar a generar[65].

De acuerdo con J. Ocón, la decisión judicial de intervención de comunicaciones telefónicas deberá tener en cuenta la superación del juicio de proporcionalidad[66]. Esta idea está relacionada con el principio de necesidad puesto que la medida de intervención solo se considera proporcional si es realmente necesaria para conseguir el objetivo perseguido y si es el único método para alcanzarlo.

El TC reafirma la idea del principio de proporcionalidad, desarrollándolo como un límite fundamental y basándose tanto en su jurisprudencia como en la del TEDH. Para comprobar si la medida de intervención supera el juicio de proporcionalidad, se deberá constatar si cumple los tres siguientes requerimientos: (1) si a través de tal medida es posible de alcanzar el objetivo propuesto, (2) si era estrictamente necesaria, es decir, que no existía otra medida menos lesiva y con la que se obtuviera el mismo resultado, (3) y si la medida implicaba un equilibrio entre el interés general y los posibles daños que pudiera causar a los derechos[67].

Asimismo, el TC ha ratificado la relevancia de identificar de manera precisa a los sujetos investigados y el alcance de la intervención como parte del principio de proporcionalidad

[65] Lorca Sánchez, M. Á., op. cit., p. 50.
[66] Ocón García, J., op. cit., p. 104.
[67] Blanco, A. E., "La jurisprudencia del Tribunal Constitucional español sobre el principio de proporcionalidad en el proceso penal", *Anuario de Derecho Penal y Ciencias Penales*, núm. 1, 2021, p. 720 (DOI: http://hdl.handle.net/11000/7100).

en la sentencia 25/2011 de 14 de marzo[68]. En esta misma línea, la sentencia ha manifestado que la resolución judicial debe exteriorizar los datos objetivos que justifiquen la existencia del delito y la conexión del investigado con el mismo.

En este sentido, el TC en la sentencia 26/2010 de 27 de abril[69], declara que las intervenciones telefónicas no pueden ser un recurso de investigación prospectiva puesto que el derecho al secreto de las comunicaciones estaría vulnerado. Las escuchas no pueden ser utilizadas para confirmar sospechas, puesto que en ese caso la garantía constitucional desaparecería.

El tercer límite del derecho es la duración de la medida. Según el artículo 588 bis e) LECrim la duración será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses. Este límite temporal se ajusta a la exigencia de garantizar la proporcionalidad de la intervención en el derecho al secreto de las comunicaciones, previniendo intervenciones indefinidas o excesivamente extendidas sin una justificación adecuada.

A nivel internacional, la protección del derecho al secreto de las comunicaciones y sus garantías han sido asimismo abordadas por el TEDH. Cuya jurisprudencia ha establecido los límites que deben cumplir los estados en lo relativo a la intervención de las comunicaciones.

El TEDH ha condenado en diversas ocasiones a Estados miembros, incluyendo a España, en caso de vulnerar el artículo 8 del Convenio Europeo de Derechos Humanos[70], que establece: "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*".

Uno de los casos más relevantes es el de Prado Bugallo vs. España (2003). El caso comenzó con una embarcación en la que el sospechoso transportó cocaína de Colombia a España. Es relevante mencionar, que, a lo largo de la investigación, las autoridades

[68] Sentencia del Tribunal Constitucional núm. 25/2011, de 14 de marzo de 2011 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2011/28557].
[69] Sentencia del Tribunal Constitucional núm. 26/2010, de 27 de abril de 2010 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2010/61524].
[70] Convenio Europeo de Derechos Humanos (BOE 4 de noviembre de 1950).

intervinieron sus comunicaciones telefónicas sin que se asegurara un control judicial efectivo[71].

El TEDH condenó a España por vulnerar el artículo 8 del Carta Europea de Derechos Humanos debido a las intervenciones telefónicas realizadas. Basaron el fallo en que las intervenciones telefónicas realizadas a lo largo de la investigación no cumplieron con los requisitos del artículo 588 bis a) LECrim y con las garantías legales correspondientes. Asimismo, el Tribunal criticó la legislación española del momento puesto que no regulaba suficiente la intervención de las comunicaciones y que debían precisar de un control judicial más efectivo[72].

Esta sentencia se consideró un punto de inflexión puesto que influyó considerablemente en la posterior reforma de la LO 13/2015 de la LECrim.

Por otro lado, el caso Roman Zakharov vs. Rusia (2015) fue muy relevante en la jurisprudencia del TEDH, abordando la interceptación masiva de comunicaciones sin control judicial efectivo. El Tribunal constató que el control judicial en la interceptación secreta de las telecomunicaciones solo actuaba en la fase de autorización, dejando el resto en manos del poder ejecutivo, vulnerando así el artículo 8 del CEDH[73].

Este fallo, semejante al caso Prado Bugallo vs. España (2003), mostró los defectos en los sistemas de supervisión de algunas naciones y fortaleció el control judicial en la intervención de las comunicaciones.

CAPITULO VI: PERSPECTIVAS DE FUTURO Y RETOS PENDIENTES

1. EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS

El avance tecnológico de los últimos tiempos ha generado un gran cambio en la manera en la que las personas se comunican, aumentando la utilidad y dependencia de los dispositivos electrónicos. No obstante, este avance plantea retos en la protección del

[71] Roxin, I., "La provocación del delito contraria al Estado de Derecho y sus consecuencias jurídicas", *Cuadernos de Derecho Penal*, núm. 23, 2020, p. 69 (DOI: https://doi.org/10.22518/jour.cdp/202023ID2578).
[72] Matia Portilla, F. J., "Examen de las sentencias del Tribunal de Estrasburgo que afectan al Reino de España", *Teoría y Realidad Constitucional*, núm. 42, 2018, p. 307 (DOI: 10.5944/trc.42.2018.23653).
[73] González Monje, A., "Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto", *Revista Europea de Derechos Fundamentales*, núm. 29, 2017, pp. 289-290 (DOI: http://hdl.handle.net/10366/157196).

derecho al secreto de las comunicaciones. La evolución de las nuevas tecnologías supera en ocasiones la capacidad reguladora del derecho, produciendo vacíos normativos que deben ser sucedidos por la jurisprudencia[74]. Es crucial analizar cómo garantizar la privacidad en este nuevo entorno digital sin comprometer la eficacia del proceso penal.

En la actualidad, cada vez se desarrollan más sistemas de Inteligencia Artificial, aptos para analizar grandes cantidades de datos, este sistema puede ser una gran ayuda a los tribunales para tomar decisiones más precisas. Algunos ejemplos de estos sistemas son "*PredPol*", el cual genera predicción de delincuencia en tiempo real o "*HunchLab*", que incorpora factores ambientales como el clima u horarios para generar la evaluación de riesgos[75].

No obstante, aunque estas herramientas pueden contribuir a una mayor eficiencia para prevenir la actividad delictiva, no están exentas de controversia. La capacidad de la IA para procesar grandes volúmenes de datos y anticipar delitos plantea serias preguntas en lo relativo a sus límites de uso y el impacto en los derechos fundamentales, como el derecho al secreto de las comunicaciones.

Los algoritmos predictivos se consideran parte del ámbito de la seguridad con el objetivo de antelar actividades delictivas, no obstante, existe un riesgo de lesión de derechos fundamentales en lo relativo a la privacidad de los ciudadanos puesto que estos sistemas analizan datos masivos sin control judicial suficiente[76]. En esta línea, el uso de la IA en la vigilancia digital no cuenta con regulación específica suficiente, lo que podría originar un uso arbitrario de estos recursos, afectando así a la privacidad de los usuarios.

El derecho al secreto de las comunicaciones ha sido siempre protegido ante su intervención, no obstante, las recientes estrategias de vigilancia, han puesto énfasis en los metadatos, que facilitan la creación de perfiles sin tener acceso a los mensajes. Cuando una persona hace uso de algún servicio de telecomunicaciones, se transmiten tanto la

[74] Lorca Sánchez, M. Á., op. cit., p. 152.
[75] García Falconí, R. J., y Barona Pazmiño, K. F., "Inteligencia artificial y proceso penal", *Revista San Gregorio*, núm. 58, vol. 1, 2024, p 104 (DOI: https://doi.org/10.36097/rsan.v1i58.2808).
[76] Muñoz Rodríguez, A. B., "El impacto de la inteligencia artificial en el proceso penal", *Anuario de la Facultad de Derecho Universidad de Extremadura*, núm. 36, 2020, pp. 103-104 (DOI: https://doi.org/10.17398/2695-7728.36.695).

información del mensaje, como quien es el remitente y destinatario, la fecha, la ubicación y la hora del mismo[77].

Un ejemplo para ilustrar dicho concepto es el caso *Digital Rights Ireland* (C-293/12 y C-594/12). El Tribunal de Justicia de la UE invalidó la Directiva de Retención de Datos 2006/24/CE por considerar que constituía una intromisión desproporcionada en la privacidad y en la protección de los datos personales, puesto que dicha normativa permitía la retención de datos de tráfico y localización de todas las personas sin limitación, lo que se consideró una vulneración del artículo 7 y 8 de la Carta de Derechos Fundamentales de la UE[78]. Además, la Directiva no establecía límites del acceso a dichos datos por parte de las autoridades, ni tampoco garantías frente a los abusos.

Sin embargo, la recopilación de metadatos no es la única amonestación al secreto de las comunicaciones. Recientemente, el uso del *software* espía ha facilitado a los gobiernos la interceptación de la información de manera aún más invasiva, introduciéndose directamente en los dispositivos sin conocimiento de los usuarios.

Actualmente existen plataformas como *Spyera*, que permite por ejemplo activar la cámara, el micrófono y acceder a la ubicación de un dispositivo sin su consentimiento. Esta intromisión invasiva ha sido discutida por organizaciones de derechos humanos, como la Fundación Karisma, la cual ha denunciado la contratación de *Hacking Team*, otra empresa como *Spyera*[79]. Por tanto, la regulación de estos programas es crucial para evitar su uso invasivo, garantizando las medidas de proporcionalidad y necesidad del derecho al secreto de las comunicaciones.

2. RETOS LEGISLATIVOS EN UN CONTEXTO DE CIBERSEGURIDAD Y VIGILANCIA MASIVA

[77] Canales, M. P., & Viollier, P., "La compatibilidad de la retención general de metadatos y el respeto a los derechos fundamentales: El caso del decreto espía", *Anuario de Derecho Público de la Universidad Diego Portales*, 2018, pp. 157-158.
[78] Galli, F., "Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions", *Maastricht Journal of European and Comparative Law*, vol. 23, núm. 3, 2016, p. 462 (DOI: https://doi.org/10.1177/1023263X1602300305).
[79] Cobo Jiménez, C., "La utilización de software como herramienta de interceptación de comunicaciones", *Cuadernos de Derecho Penal*, núm. 26, 2021, pp. 101-104 (DOI: https://doi.org/10.22518/jour.cdp/202126ID2777).

La evolución de las nuevas tecnologías ha dado lugar a nuevas formas de vigilancia que pueden entrar en conflicto con los derechos fundamentales, en este caso el secreto de las comunicaciones. La urgencia de fortalecer la ciberseguridad y luchar contra la delincuencia, ha impulsado a las naciones a incrementar sus habilidades de supervisión.

La falta de un marco normativo uniforme permite que varias naciones desarrollen programas clandestinos de interceptación, como *PRISM* y *Xkeyscore.* Según el Tribunal de Justicia de la Unión Europea, estos programas acceden a datos personales, sin la supervisión adecuada, arriesgando así su privacidad[80].

Para ilustrarlo, el caso *Big Brother Watch vs. Reino Unido* analiza la legalidad de la vigilancia masiva ejercida por el gobierno del Reino Unido. Las organizaciones de derechos humanos y periodistas presentaron la demanda, después de las revelaciones de *Edward Snowden*, consultor tecnológico estadounidense, acerca de la interceptación indiscriminada de comunicaciones a través de la *Regulation of Investigatory Powers Act 2000 (RIPA).* El TJUE sostuvo que la falta de claridad en los criterios para la elección de comunicaciones interceptadas y la falta de sistemas de control efectivo aumentaban la posibilidad de abusos. Esta sentencia reafirmó la importancia de asegurar el balance entre la seguridad nacional y los derechos fundamentales, imponiendo protecciones más rigurosas para la supervisión digital[81].

En resumen, el reto legislativo más grande radica en equilibrar la normativa de la vigilancia digital para asegurar que las acciones de seguridad no lesionen el derecho al secreto de las comunicaciones. La falta de una regulación precisa sobre la utilización de instrumentos de vigilancia digital y la ausencia de mecanismos de control efectivos continúan siendo lagunas jurídicas que necesitan una reforma legislativa inmediata.

3. PROPUESTAS PARA INTENTAR EQUILIBRAR LOS DERECHOS FUNDAMENTALES Y LAS NECESIDADES DEL PROCESO PENAL

Uno de los mayores retos jurídicos es el balance entre la protección y el respeto a los derechos fundamentales en el campo de la vigilancia digital. Conforme las tecnologías

[80] Peralta Gutiérrez, A., "La necesaria regulación de la vigilancia masiva: Casos Quadrature du Net y Big Brother Watch", *Diario La Ley*, núm. 9973, 2021, p. 1.
[81] Loreti, D., "Derecho a la privacidad. Intercepción de comunicaciones. TEDH, Case of Big Brother Watch and others v. The United Kingdom, 13 de septiembre de 2018 y TEDH, Case of Catt v. The United Kingdom, 24 de enero de 2019", *Revista Debates sobre Derechos Humanos*, núm. 3, 2019, p. 250 (DOI: https://publicaciones.unpaz.edu.ar/OJS/index.php/debatesddhh/article/view/652).

de interceptación se han perfeccionado, los países han potenciado sus habilidades de supervisión con el fin de asegurar la seguridad ciudadana y la eficiencia del proceso penal, por lo que resulta esencial crear mecanismos de regulación más efectivos para que las garantías ni la privacidad de los usuarios se vean comprometidas[82].

El reglamento *ePrivacy* está considerado como un recurso esencial en el marco regulatorio de la UE para, de esta manera, asegurar la privacidad en el contexto de las comunicaciones digitales, expandiendo las estipulaciones del Reglamento General de Protección de Datos[83]. Una de sus innovaciones más destacadas su implementación global, lo que implica que afecta a cualquier proveedor de servicios de comunicaciones que brinde sus servicios en la UE.

El uso cada vez mayor del cifrado extremo a extremo en las comunicaciones digitales ha presentado un reto considerable para las autoridades responsables de la investigación penal, dado que obstaculiza el acceso directo a los mensajes sin infringir los derechos fundamentales. La implementación del mismo en programas de mensajería ha fortalecido la privacidad de las comunicaciones, evitando así acceder sin autorización a mensajes privados; no obstante, esto puede considerarse un problema a la hora de obtener pruebas en una investigación. En esta línea, varios gobiernos han sugerido incorporar "puertas traseras" en los sistemas de cifrado para simplificar ese acceso a los datos[84].

En este contexto, es relevante analizar modelos internacionales, puesto que existen algunos países que han implementado controles más estrictos sobre la vigilancia digital, lo que sin duda puede llegar a ser una referencia para el modelo de nuestra nación.

En primer lugar, el TC alemán ha establecido límites estrictos a la retención de datos, implantando que una recopilación masiva sin justificación, lesiona derechos fundamentales. En el año 2023, eliminó leyes que decretaban un análisis automático de

[82] González Monje, A., op. cit., p. 293.
[83] Gascón Macén, A., "El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea", *Cuadernos de Derecho Transnacional*, vol. 13, núm. 2, 2021, p. 209 (DOI: https://doi.org/10.20318/cdt.2021.6256).
[84] García de Mesa, M., La intervención de las comunicaciones en el panorama tecnológico actual. Trabajo de Fin de Grado. Universidad Pontificia de Comillas (ICADE), p. 25 (DOI: http://hdl.handle.net/11531/29255).

la información con fines policiales, dado que estas debían cumplir con una serie de criterios; proporcionalidad y control judicial efectivo[85].

Esta postura sigue la misma línea que su previa jurisprudencia: el TC ha manifestado que la retención indiscriminada de datos sin supervisión está considerada como un riesgo para la autonomía personal y la democracia[86]. Esta postura ha convertido a Alemania en un referente para toda Europa, en materia de la protección al derecho de las comunicaciones.

Por otro lado, según M.C. Arruga, Francia ha fortalecido el control judicial en las comunicaciones a través de varias reformas legislativas para asegurar el principio de proporcionalidad. Asimismo, ha creado normativa en materia de ciberseguridad y retención de datos que exige a las autoridades a justificar la necesidad de cualquier intervención. La Ley de Inteligencia del año 2015 junto a sus recientes cambios han instaurado protocolos más rigurosos para el acceso a información personal, fortaleciendo la supervisión judicial en la vigilancia digital[87]. Estas reformas han consolidado a Francia como uno de los países europeos con un sistema más garantista en la regulación de la privacidad frente a la seguridad estatal.

La evolución de las tecnologías hoy en día ha cambiado completamente la percepción que se tenía que de las comunicaciones hace tiempo, generando así tanto desafíos como oportunidades en la protección del derecho al secreto de las comunicaciones.

CAPITULO VII: CONCLUSIONES

Este trabajo sobre el derecho al secreto de las comunicaciones y su incidencia en el proceso penal ha demostrado la gran relevancia de este derecho en la obtención y valoración de pruebas en el procedimiento judicial y, sobretodo, cómo y en qué medida afecta a la privacidad de los usuarios.

---

[85] Cotino Hueso, L., "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial: Los altos estándares que exigen el Tribunal Constitucional Alemán y otros Tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, núm. 64, 2023, p. 2.

[86] Wendel, M., "El Tribunal Constitucional Federal Alemán entre protección jurídica y exceso competencial: Sobre la eficacia de los controles constitucionales nacionales en tiempos de crisis europea", *Teoría y Realidad Constitucional*, núm. 39, 2017, p. 140 (DOI: 10.5944/trc.39.2017.19158).

[87] Arruga Segura, M. C., "Las implicaciones del derecho a la desconexión digital en la prestación de trabajo y en el teletrabajo regular", *Revista Derecho Social y Empresa*, núm. 15, 2021, p. 58 (DOI: https://doi.org/10.18172/redsye.6225).

Durante el trabajo, se han alcanzado los objetivos propuestos, analizando sus bases constitucionales y su evolución normativa a lo largo de los años, así como los retos presentes derivados de las nuevas tecnologías. A continuación, se realiza una valoración de los objetivos propuestos al inicio del trabajo, para demostrar su cumplimiento y extraer conclusiones.

En primer lugar, se propuso como objetivo estudiar el fundamento, titularidad y alcance del derecho al secreto de las comunicaciones, identificando su reconocimiento constitucional, así como su calificación como derecho fundamental. Este objetivo se logró mediante el análisis del artículo 18.3 CE y su interpretación por parte del TC. Asimismo, se ha demostrado que es un derecho erga omnes, aplicable a personas físicas y jurídicas y cuya titularidad proviene de la dignidad humana.

En segundo lugar, se planteó como objetivo abordar la vulneración del derecho al secreto de las comunicaciones, reconociendo las excepciones previstas por la ley y distinguiendo entre intromisión legítima e ilegítima. Igualmente se ha logrado este objetivo, reconociendo distintos supuestos que separan la vulneración y la intervención ilícita, así como las conversaciones grabadas por uno de los interlocutores, comunicaciones por radio o el acceso a la memoria de un teléfono móvil. Se ha destacado que este derecho, a pesar de ser un derecho fundamental, puede ser limitado y que, estas limitaciones, deben estar sujetas a los principios de necesidad, proporcionalidad y control judicial, para evitar acciones arbitrarias que pongan en riesgo el derecho.

En tercer lugar, se propuso analizar el régimen jurídico de la intervención de las comunicaciones en el proceso penal, enfocándose en los requisitos normativos para asegurar su legalidad. Este objetivo asimismo se ha cumplido mediante el estudio de la reforma introducida por la LO 13/2015, en especial de los artículos 588 bis y siguientes de la LECrim. Se han examinado también la relevante intervención del juez instructor y el control judicial, como garantía esencial, y los requisitos formales y materiales.

En cuarto lugar, se planteó estudiar intensivamente la reforma de la LO 13/2015 y cómo influyó en la obtención y la valoración de la prueba. Este objetivo también se ha cumplido, llegando a la conclusión de que dicha reforma se consideró un "antes y un después" en la regulación de las comunicaciones, al conllevar un gran avance en las garantías y en la seguridad jurídica, a pesar de que aún existan opiniones doctrinales que requieren una reforma más profunda, para enfrentarse a los desafíos actuales y futuros. Asimismo, se

destaca que el incumplimiento de las garantías puede conllevar a la nulidad de la prueba, de acuerdo con la jurisprudencia del TS y del TC.

En quinto lugar, se propuso dedicar una parte del trabajo a analizar en concreto las comunicaciones telefónicas y telemáticas, al ser dos de los medios de comunicación más relevantes hoy en día. Para demostrar el cumplimiento del quinto objetivo, se han comparado varios medios de comunicación con el teléfono, como *WhatsApp*, destacando sus diferentes regulaciones, validez como prueba y fiabilidad. En el caso de la aplicación WhatsApp, la jurisprudencia ha requerido pruebas periciales para probar la validez del contenido de los mensajes o llamadas, debido a que no cuentan con una regulación tan clara como las comunicaciones telefónicas o telemáticas.

En sexto lugar, se planteó como último objetivo del trabajo abordar los retos legislativos actuales y perspectiva de futuro en lo relativo a las nuevas tecnologías. Este objetivo se cumplió a través del estudio de la influencia de la IA, la vigilancia masiva, la recopilación de metadatos y el uso del software espía, herramientas que impactan en la protección del derecho al secreto de las comunicaciones. La necesidad de nuevas regulaciones para hacer frente a los desafíos actuales se ha reflejado en la necesidad de establecer un equilibrio entre la eficacia procesal y el respeto al derecho.

En conclusión, con el presente trabajo se ha demostrado que el derecho al secreto de las comunicaciones es esencial en el sistema jurídico, no obstante, su regulación debe estar en constante evolución debido a que el emergente crecimiento de las nuevas tecnologías afecta de manera directa a este derecho, es más, lo expande. La intervención de las comunicaciones en el proceso penal es un medio de prueba excelente y un recurso muy útil, sin embargo, debe hacerse uso de ella con sumo cuidado, puesto que la intervención se encuentra rozando el límite con el derecho a la intimidad regulado en el artículo 18.1 CE, respetando siempre los principios de necesidad, proporcionalidad y control judicial.

Con vistas al futuro, las nuevas tecnologías presentan nuevos retos y, tan solo mediante normativa sólida y detallada, será posible asegurar que la intervención de las comunicaciones no sea un recurso abusivo o intrusivo, sino un instrumento legítimo que honre el debido proceso y las garantías constitucionales.

BIBLIOGRAFÍA

1. LEGISLACIÓN

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (BOE 17 de septiembre de 1882).

Convenio Europeo de Derechos Humanos (BOE 4 de noviembre de 1950).

Constitución Española (BOE 29 de diciembre de 1978).

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (BOE 24 de noviembre de 1995).

Carta de los Derechos Fundamentales de la Unión Europea (Diario Oficial de la Unión Europea de 30 de marzo de 2010).

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. (BOE 6 de octubre de 2015).

Circular 2/2019, de 6 de marzo, sobre interceptación de comunicaciones telefónicas y telemáticas (BOE 22 de marzo de 2019).

Real Decreto 437/2024, de 30 de abril**,** por el que se aprueba el Reglamento de los servicios postales (BOE 18 de mayo de 2024).

2. JURISPRUDENCIA

Sentencia del Tribunal Constitucional núm. 281/2006, de 9 de octubre de 2006 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2006/273570].

Sentencia del Tribunal Constitucional núm. 26/2010, de 27 de abril de 2010 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2010/61524].

Sentencia del Tribunal Constitucional núm. 25/2011, de 14 de marzo de 2011 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2011/28557].

Sentencia del Tribunal Supremo núm. 695/2013, de 22 de julio de 2013 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2013/174352].

Sentencia del Tribunal Supremo núm. 850/2014, de 26 de noviembre de 2014 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2014/222781].

Sentencia del Tribunal Supremo núm. 153/2015, de 18 de marzo de 2015 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2015/36426].

Sentencia del Tribunal Supremo núm. 228/2015, de 21 de abril de 2015 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2015/51662].

Sentencia del Tribunal Supremo núm. 300/2015, de 19 de mayo de 2015 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2015/77775].

Sentencia del Tribunal Supremo núm. 864/2015, de 10 de diciembre de 2015 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2015/269989].

Sentencia del Tribunal Supremo núm. 841/2016, de 8 de noviembre de 2016 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2016/202623].

Sentencia del Tribunal Supremo núm. 681/2017, de 18 de octubre de 2017 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2017/218369].

Sentencia del Tribunal Supremo núm. 264/2018, de 31 de mayo de 2018 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2018/511347].

Sentencia del Tribunal Supremo núm. 634/2019, de 19 de diciembre de 2019 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2019/785654].

Sentencia del Tribunal Supremo núm. 87/2020, de 3 de marzo de 2020 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2020/515843].

Sentencia del Tribunal Constitucional núm. 61/2021, de 15 de marzo de 2021 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2021/515845].

Sentencia del Tribunal Supremo núm. 964/2021, de 10 de diciembre de 2021 [versión electrónica – base de datos Lefebvre. Ref. EDJ 2021/777954].

Sentencia del Tribunal Supremo núm. 54/2024, de 18 de enero de 2024 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2024/501917].

Sentencia del Tribunal Supremo núm. 135/2025, de 7 de febrero de 2025 [versión electrónica- base de datos Lefebvre. Ref. EDJ 2025/508319].

OBRAS DOCTRINALES

Arruga Segura, M. C., "Las implicaciones del derecho a la desconexión digital en la prestación de trabajo y en el teletrabajo regular", *Revista Derecho Social y Empresa,* núm. 15, 2021, pp. 58-83 (DOI: https://doi.org/10.18172/redsye.6225).

Bachmaier Winter, L., "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *Boletín del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes*, núm. 2195, 2017, pp. 1-36 (DOI: https://revistas.mjusticia.gob.es/index.php/BMJ/article/view/2827).

Belda Pérez-Pedrero, E.**,** "El derecho al secreto de las comunicaciones", *Parlamento y Constitución. Anuario*, núm. 2, 1998, pp. 169-194.

Blanco, A. E., "La jurisprudencia del Tribunal Constitucional español sobre el principio de proporcionalidad en el proceso penal", *Anuario de Derecho Penal y Ciencias Penales*, núm. 1, 2021, pp. 708-734 (DOI: https://doi.org/10.53054/adpcp.v74i1.7910).

Bohigues Esparza, M. D. "La ilicitud de la prueba con vulneración de derechos fundamentales. A propósito de la sentencia del Tribunal Constitucional núm. 61/2021 de 15 de marzo", *IUSLabor. Revista d'anàlisi de Dret del Treball*, núm. 2, 2021, pp. 263-287 (DOI: https://doi.org/10.31009/IUSLabor.2021.i02.9)

Canales, M. P., & Viollier, P., "La compatibilidad de la retención general de metadatos y el respeto a los derechos fundamentales: El caso del decreto espía", *Anuario de Derecho Público de la Universidad Diego Portales*, 2018, pp. 155-171.

Casas Baamonde, M. E., "¿Una "tercera" doctrina judicial sobre la prueba ilícita por vulneración de derechos fundamentales y sus efectos en la calificación del despido?", *Revista de Jurisprudencia Laboral*, núm. 3, 2023, pp. 331-349 (DOI: https://doi.org/10.55104/RJL_00430).

Cobo Jiménez, C., "La utilización de software como herramienta de interceptación de comunicaciones", *Cuadernos de Derecho Penal*, núm. 26, 2021, pp. 93-121 (DOI: https://doi.org/10.22518/jour.cdp/202126ID2777).

Cotino Hueso, L., "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial: Los altos estándares que exigen el Tribunal Constitucional Alemán y otros Tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, núm. 64, 2023, pp. 1-22.

Díaz Revorio, F. J., "El derecho fundamental al secreto de las comunicaciones", *Derecho PUCP*, núm. 59, 2006, pp. 159-175.

Elso Montanary, Í., *Reflejo de la doctrina jurisprudencial en la regulación de la intervención de las comunicaciones en la Ley Orgánica 13/2015, de 5 de octubre*, Trabajo de Fin de Grado, Universidad de Valladolid, 2019, pp. 1-67 (DOI: http://uvadoc.uva.es/handle/10324/38396).

Estévez Díaz, S., La intervención telefónica en el proceso penal español como diligencia de intervención y medio de prueba, Trabajo de Fin de Grado, Universidad de la Laguna, pp. 1-52.

Galli, F., "Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions", *Maastricht Journal of European and Comparative Law*, vol. 23, núm. 3, 2016, pp. 460-477 (DOI: https://doi.org/10.1177/1023263X1602300305).

García de Mesa, M., La intervención de las comunicaciones en el panorama tecnológico actual. Trabajo de Fin de Grado. Universidad Pontificia de Comillas (ICADE), pp. 1-62 (DOI: http://hdl.handle.net/11531/29255).

García Falconí, R. J., y Barona Pazmiño, K. F., "Inteligencia artificial y proceso penal", *Revista San Gregorio*, núm. 58, vol. 1, 2024, pp. 87-100 (DOI: https://doi.org/10.36097/rsan.v1i58.2808).

Gascón Inchausti, F., *Derecho procesal penal: Materiales para el estudio*, 6ª edición, Universidad Complutense de Madrid, 2024.

Gascón Macén, A., "El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea", *Cuadernos de Derecho Transnacional*, vol. 13, núm. 2, 2021, pp. 209-232 (DOI: https://doi.org/10.20318/cdt.2021.6256).

Gimeno Sendra, J.V., *Manual de Derecho Procesal Penal*, Editorial Tirant lo Blanch, 2020.

González Monje, A., "Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto", *Revista Europea de Derechos Fundamentales*, núm. 29, 2017, pp. 267-294 (DOI: http://hdl.handle.net/10366/157196).

González-Montes Sánchez, J. L., "Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", *Revista Electrónica de Ciencia Penal y Criminología*, núm. 17, 2015, pp. 1-41 (DOI: http://criminet.ugr.es/recpc).
https://doi.org/10.17398/2695-7728.36.695)

López-Barajas Perea, I., "Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la Ley", *Revista de Derecho Político*, núm. 98, 2017, pp. 91-119 (DOI: https://doi.org/10.5944/rdp.98.2017.18652).

Lorca Sánchez, M. Á.**,** *El derecho al secreto de las comunicaciones: Influencia de la jurisprudencia y análisis de su aplicación en la práctica jurídica*, tesis doctoral, Universitat d'Alacant/Universidad de Alicante, 2021 (DOI: http://hdl.handle.net/10045/118895).

Loreti, D., "Derecho a la privacidad. Intercepción de comunicaciones. TEDH, Case of Big Brother Watch and others v. The United Kingdom, 13 de septiembre de 2018 y TEDH, Case of Catt v. The United Kingdom, 24 de enero de 2019", *Revista Debates sobre Derechos Humanos*, núm. 3, 2019, pp. 247-258. (DOI: https://publicaciones.unpaz.edu.ar/OJS/index.php/debatesddhh/article/view/652).

Martínez Guerrero, A., "A vueltas con el whatsapp y semejantes como fuente de prueba en la fase instructora del proceso penal", *Revista Claves Jurídicas,* pp. 2-21 (DOI: https://www.clavesjuridicas.com/index.php/raj/article/view/117).

Martínez Guerrero, A., "Incorporación de los WhatsApp y otras aplicaciones semejantes de mensajería electrónica al proceso penal en la fase de instrucción", *Revista Acta Judicial*, núm. 10, 2022, pp. 30-36.

Martínez Polo, P. O., y Sandoval Pérez, K. D. P., "La intervención del Ministerio Público en los requerimientos del levantamiento del secreto de las comunicaciones telefónicas y su vulneración a los derechos fundamentales", *Tesis de Grado*, pp. 1-102 (DOI: https://hdl.handle.net/20.500.12692/97119).

Matia Portilla, F. J., "Examen de las sentencias del Tribunal de Estrasburgo que afectan al Reino de España", *Teoría y Realidad Constitucional*, núm. 42, 2018, pp. 273-310 (DOI: 10.5944/trc.42.2018.23653).

Mitran, G. D., *La intervención de las comunicaciones telefónicas y telemáticas*, Trabajo de Fin de Grado, Universidad de Almería, 2021, pp. 1-45 (DOI: http://hdl.handle.net/10835/13187).

Muñoz Rodríguez, A. B., "El impacto de la inteligencia artificial en el proceso penal", *Anuario de la Facultad de Derecho Universidad de Extremadura*, núm. 36, 2020, pp. 695-728 (DOI:

Ocón García, J., "Constitución y secreto de las comunicaciones: desafíos tecnológicos para el derecho fundamental", *Nuevos Horizontes del Derecho Constitucional*, núm. 2, 2022, pp. 86-104.

Peralta Gutiérrez, A., "La necesaria regulación de la vigilancia masiva: Casos Quadrature du Net y Big Brother Watch", *Diario La Ley*, núm. 9973, 2021, pp. 1-30.

Pérez Gil, J., "Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución", en *Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli*, Aracne, 2018, pp. 187-198.

Rayón Ballesteros, M. C., "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", *Anuario Jurídico y Económico Escurialense*, núm. 52, 2019, pp. 179-204.

Roxin, I., "La provocación del delito contraria al Estado de Derecho y sus consecuencias jurídicas", *Cuadernos de Derecho Penal*, núm. 23, 2020, pp. 17-34 (DOI: https://doi.org/10.22518/jour.cdp/202023ID2578).

Sanchis Crespo, C., "Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas", *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, núm. 125, 2017, pp. 1-18.

Sanchis Marín, Á. J., *La prueba ilícita en el proceso penal: La regla de exclusión*, Trabajo de Fin de Grado, Universidad Pontificia Comillas (ICADE), 2023, pp. 1-55 (DOI: http://hdl.handle.net/11531/72147).

Soto Campillo, J. F., *WhatsApp: como medio de prueba en el procedimiento penal*, Trabajo de Fin de Grado, Universidad Miguel Hernández, 2017, p. 1-88 (DOI: http://hdl.handle.net/11000/7100).

Velasco Perdigones, J. C., *Las intervenciones telefónicas y el secreto de las comunicaciones. Estado de la cuestión en la jurisprudencia*, s.f, pp. 1-18.

Wendel, M., "El Tribunal Constitucional Federal Alemán entre protección jurídica y exceso competencial: Sobre la eficacia de los controles constitucionales nacionales en tiempos de crisis europea", *Teoría y Realidad Constitucional*, núm. 39, 2017, pp. 123-162 (DOI: 10.5944/trc.39.2017.19158)

3. RECURSOS DE INTERNET

El Derecho, "¿Pueden acceder los agentes de policía al registro de llamadas del teléfono móvil del detenido?", *El Derecho*, 27 de abril de 2020 (DOI: https://elderecho.com/pueden-acceder-los-agentes-policia-al-registro-llamadas-del-telefono-movil-del-detenido).