



UNIVERSIDAD DE LA RIOJA

TESIS DOCTORAL

Título
El derecho fundamental al secreto de las comunicaciones ante nuevos escenarios tecnológicos
Autor/es
Juan Ocón García
Director/es
María Amelia Pascual Medrano y Ricardo Luis Chueca Rodríguez
Facultad
Facultad de Ciencias Jurídicas y Sociales
Titulación
Departamento
Derecho
Curso Académico



El derecho fundamental al secreto de las comunicaciones ante nuevos escenarios tecnológicos, tesis doctoral de Juan Ocón García, dirigida por María Amelia Pascual Medrano y Ricardo Luis Chueca Rodríguez (publicada por la Universidad de La Rioja), se difunde bajo una Licencia Creative Commons Reconocimiento-NoComercial-SinObraDerivada 3.0 Unported.

Permisos que vayan más allá de lo cubierto por esta licencia pueden solicitarse a los titulares del copyright.



**UNIVERSIDAD
DE LA RIOJA**

**EL DERECHO FUNDAMENTAL AL SECRETO
DE LAS COMUNICACIONES ANTE NUEVOS
ESCENARIOS TECNOLÓGICOS**

Juan Ocón García

Tesis Doctoral dirigida por:

Dra. Amelia Pascual Medrano – Dr. Ricardo Chueca Rodríguez

PROGRAMA DE DOCTORADO EN DERECHO Y CAMBIO SOCIAL

2020

ÍNDICE

INTRODUCCIÓN.....	7
-------------------	---

CAPÍTULO PRIMERO DELIMITACIÓN DEL DERECHO FUNDAMENTAL DEL ART. 18.3 CE

I. Introducción.....	16
II. Una ojeada histórica	18
II.1. Nacimiento y expansión del derecho	18
II.2. El derecho al secreto de las comunicaciones en la historia constitucional española	20
II.3. El proceso constituyente de 1978.....	22
III. Intimidad y secreto de las comunicaciones: dos derechos autónomos y distintos ...	25
IV. Objeto y contenido	30
IV.1. Objeto.....	30
IV.2. Contenido	38
V. Titularidad.....	40
VI. Suspensión del derecho	48
VI.1. Suspensión general (55.1 CE).....	48
VI.2. Suspensión individual (55.2 CE).....	50

CAPÍTULO SEGUNDO
LA COMUNICACIÓN PROTEGIDA EN EL ARTÍCULO 18.3 CE

I. Concepto constitucional de comunicación.....	56
I.1. Una comunicación consiste en una transmisión de expresiones de sentido	57
I.2. Entre personas <i>previamente</i> determinadas. Difusión pública y comunicación privada.....	61
A. Predeterminación de destinatarios frente a audiencias potencialmente ilimitadas	65
B. Interactividad <i>versus</i> pasividad: la conmutabilidad de roles en la relación comunicativa.....	68
C. La singularidad del destinatario en las comunicaciones privadas.....	69
I.3. Comunicación técnicamente mediada y a través de canal cerrado.....	73
A. Soporte e intermediación técnica: comunicación <i>versus</i> conversación directa	73
B. Características del medio. Las denominadas «comunicaciones abiertas»	82
II. Ámbito temporal del derecho: intervención y acceso	87
II.1. Inicio del proceso comunicativo	88
II.2. Finalización del proceso comunicativo	89
A. La protección del sistema comunicativo	90
B. La protección de la comunicación hasta el conocimiento del contenido por el destinatario	91
C. La estricta limitación de la protección a la comunicación en tránsito y la participación del tercero.....	93
III. Modalidades comunicativas protegidas.....	99
III.1. Comunicaciones postales y telegráficas.....	99
III.2. Comunicaciones bidireccionales simultaneas	103
III.3. Comunicaciones telemáticas alternativas.....	106

CAPÍTULO TERCERO
EL SECRETO CONSTITUCIONALMENTE PROTEGIDO

I. El secreto en el ordenamiento jurídico.....	112
A. Secreto como límite al conocimiento	112
B. Secreto como concepto relacional	113
C. Secreto como atribución normativa de carácter teleológico	115
D. El secreto presenta una doble dimensión imperfecta.....	118
II. Objeto del derecho: el secreto —¿y la libertad?— de las comunicaciones.....	122
II.1. El secreto de las comunicaciones	122
A. Ámbito objetivo del secreto	122
B. Dimensión temporal del secreto	124
C. Ámbito subjetivo del secreto	125
D. El deber de confidencialidad del prestador del servicio.....	132
II.2. La libertad de las comunicaciones	134
A. Libertad de las comunicaciones expresamente garantizada	135
B. Delimitación de la libertad de las comunicaciones	138
B.1. Libertad de las comunicaciones como derecho al medio o servicio de comunicaciones	139
B.2. Libertad de las comunicaciones como libertad de acción.....	140
B.3. Libertad de las comunicaciones como prohibición de alterar su curso normal	143
B.4. Libertad de las comunicaciones como libertad para compartir expresiones de sentido exclusivamente con sujetos determinados	146
III. El secreto tecnológicamente garantizado	148
III.1. El cifrado de comunicaciones	151
III.2. Incidencia del cifrado en el derecho fundamental al secreto de las comunicaciones	155
III.3. Intervención de comunicaciones cifradas.....	162
A. Interceptación del contenido comunicacional mediante ataques de suplantación	163
B. Remoción de las técnicas de cifrado con auxilio de terceros	164
C. Descifrado mediante técnicas de criptoanálisis	166
D. Registro remoto de dispositivos como técnica de intervención de comunicaciones	166

CAPÍTULO CUARTO
SECRETO DE LAS COMUNICACIONES Y DATOS DE TRÁFICO

I. Introducción.....	172
II. Datos de tráfico: concepto y regulación	174
II.1. Datos de tráfico y datos <i>afines</i>	174
II.2. El uso de datos de tráfico en la investigación penal	176
A. La conservación generalizada de datos.....	176
B. La preservación de datos almacenados	184
C. La interceptación de datos en tiempo real.....	185
III. Datos de tráfico y derechos fundamentales afectados	188
III.1. Interceptación de datos de tráfico asociados a comunicaciones en curso	190
III.2. Acceso a datos de tráfico asociados a comunicaciones consumadas	192
A. Datos en poder del prestador del servicio.....	194
B. Datos en poder de los comunicantes	199

CAPÍTULO QUINTO
EL CONTENIDO DEL DERECHO FUNDAMENTAL AL
SECRETO DE LAS COMUNICACIONES

I. La doble dimensión del derecho fundamental	206
II. Contenido subjetivo del derecho	212
II.1. La intervención constitucional de las comunicaciones ¿límite o delimitación?	212
II.2. El legislador del artículo 18.3 CE: la previsión del límite.....	218
A. La necesidad de <i>interpositio legislatoris</i>	218
B. La «calidad» de la norma limitadora	226
C. Fundamentos de la limitación	242
D. Los límites a la actividad limitadora del legislador	245
D.1. El contenido esencial como límite de los límites.....	245
D.2. La proporcionalidad del límite como parámetro de constitucionalidad de la ley.....	247
II.3. El juez del artículo 18.3 CE: la aplicación del límite	251
A. El juicio sobre la decisión de intervención	251
A.1. Presupuestos para la aplicación del límite	251
A.2. El test de proporcionalidad	257
B. La resolución judicial.....	262
C. Práctica de la intervención y control judicial	266
III. Contenido objetivo. El secreto de las comunicaciones en las relaciones entre particulares.....	270
III.1. Fundamentos constitucionales de la dimensión objetiva de los derechos fundamentales.....	270
III.2. Dimensión objetiva del derecho fundamental al secreto de las comunicaciones	272
A. El efecto irradiante de los derechos fundamentales	273
B. El deber de protección de los derechos fundamentales	273
III.3. El derecho fundamental al secreto de las comunicaciones en las relaciones entre particulares	280
 CONCLUSIONES	 287
 BIBLIOGRAFÍA	 295
JURISPRUDENCIA	321

INTRODUCCIÓN

La comunicación —poner en común— es condición de existencia de la persona, es decir, del ser humano en su interrelación con otros miembros de su especie. Por tanto, el término comunicación no alude a un modo concreto de relación: el ser humano es capaz de expresarse socialmente a través de una variada gama de lenguajes.

Pero cada modo de relación, de comunicación, posee un conjunto de códigos propio que la hacen posible. Y el concepto de civilización de nuestro modelo cultural incluye una historia del despliegue de los medios y técnicas capaces de construir comunicación, vale decir, relación entre quienes, al hacerlo, devienen personas.

Una condición de existencia de la comunicación demanda que la acción comunicativa se desarrolle entre actores que son *dominus* de ella. Se trata en definitiva de una condición de libertad. El mantenimiento de la autenticidad e invulnerabilidad de la relación comunicativa en libertad es, así visto, un logro que resulta especialmente dificultoso en relación directa a la capacidad de control de la comunicación por los propios actores. Lo que es evidente cuando la posibilidad de comunicación requiere de un soporte cuyo control es compartido con, o dependiente de, terceros.

Este escenario es el que describe nuestro artículo 18.3 CE. Un escenario comunicativo que incluye un riesgo que pretende confinar el contenido del derecho fundamental allí configurado.

Toda comunicación a distancia requiere de un medio técnico que soporte el mensaje, y a veces de un tercero ajeno.

Por ello, los Estados se deciden a prever mecanismos jurídicos dirigidos a paliar los riesgos asociados a estos elementos, esto es, impedir que la existencia o contenido de la comunicación sean desvelados por personas distintas a las que se dirige y, con ello, generar un nivel óptimo de confianza en el prestador del servicio, necesario para asegurar su utilización.

Se declara así la inviolabilidad de la correspondencia, previéndose en primer lugar en normas de régimen interno de los servicios de correos y pasando a los textos constitucionales a partir del primer tercio del siglo XIX.

Las normas dirigidas a tal fin se estructuran típicamente en dos proposiciones: prohibición general de ruptura del secreto de las comunicaciones y habilitación de su levantamiento, con observancia de determinadas garantías, en aquellos casos en que la protección de un bien constitucionalmente relevante legitime la intervención. En esto consiste nuestro artículo 18.3 CE.

El constituyente de 1978 no pudo imaginar la explosiva evolución de las entonces incipientes tecnologías de la comunicación durante las siguientes décadas.

No obstante, la textura parcialmente abierta de la norma le ha permitido acoger en su objeto comunicaciones no mencionadas expresamente. Así, la garantía de secreto se extiende hoy, además de a las tradicionales comunicaciones telefónicas y postales, a otras modalidades comunicativas de uso generalizado como el correo electrónico, los chats o mensajes soportados por telefonía celular, y una variada gama de tecnologías que incesantemente se incorporan a la práctica diaria de comunicación social de las sociedades avanzadas.

Podría decirse que la norma iusfundamental ha superado con cierta solvencia el test de elasticidad, demostrando probada su capacidad de

adaptación a cambios tecnológicos y sociales a través de la interpretación del precepto y sin necesidad, por tanto, de recurrir a su reforma. Sin embargo, como regla jurídica, la norma de derecho fundamental posee fronteras estrictas, siendo necesario distinguir con precisión los fenómenos comunicacionales protegidos, de aquellos que, so riesgo de desbordar su objeto y merma de su eficacia, deben entenderse más allá de sus fronteras.

Desde la redacción del precepto se han producido transformaciones, principalmente tecnológicas, pero también sociales y políticas, en los ámbitos de realidad que identifican los conceptos de «comunicación» y «secreto», así como en la capacidad del Estado de garantizar el espacio de autodeterminación que la Constitución proclama.

Al análisis de estos elementos he dedicado la tesis doctoral que presento*.

* * * * *

El primer capítulo da cuenta de la delimitación del derecho fundamental al secreto de las comunicaciones por parte de la doctrina científica y jurisprudencial.

Se analiza la evolución histórica del derecho, su origen y despliegue en las constituciones de referencia y en las históricas propias. Dedicamos especial atención al devenir del precepto en el proceso constituyente.

Se estudia además la relación que mantiene con otros derechos vecinos, como el de intimidad, del primer apartado del artículo 18 de la Constitución. Damos cuenta también de su asociación al concepto, tan general e impreciso, de vida privada utilizado en normas como el Convenio Europeo de Derechos Humanos.

* La tesis se ha realizado en el marco de los Proyectos DER2014-52817-P, «Crisis y cambio de los derechos fundamentales: la frontera del derecho fundamental en la constitución normativa», y PGC2018-093737-B-I00, «El nexo dato científico/tecnológico derecho fundamental: un desafío para los actuales ordenamientos constitucionales».

Finalmente se analizan los elementos clásicos del derecho fundamental, esto es, su objeto, contenido y titularidad, así como las modalidades de suspensión del ejercicio de este derecho que se prevén en el artículo 55 CE.

* * * * *

El capítulo segundo examina el significado y alcance del concepto de comunicación en el art. 18.3 CE.

El desarrollo de nuevas tecnologías de la comunicación ha tenido incidencia en todos los elementos componentes de la comunicación: emisor, receptor, mensaje, código y canal o medio.

Si tradicionalmente las relaciones comunicativas por medio técnico se mantenían entre dos personas, el desarrollo de procesos comunicativos soportados por Internet ha generalizado el uso de comunicaciones *one to many*, donde la información transita hacia varios comunicantes simultáneamente sin pretender divulgar su contenido, sino el intercambio entre sus destinatarios.

El mensaje, tradicionalmente oral o escrito, adopta en los modernos sistemas comunicacionales otras formas, compartiéndose frecuentemente imágenes, en formato foto o video, documentos o la propia localización geográfica del comunicante. Incluso el código comunicacional, típicamente alfanumérico, convive en la actualidad con la transmisión de información a través de ideogramas como los tan utilizados *emojis*.

Pero los cambios que mayor incidencia tienen para el concepto de comunicación objeto del derecho fundamental son los referidos al canal o medio soporte del proceso comunicativo.

La clásica escisión de los medios tradicionales de comunicación, en modalidad privada (correo, telégrafo o teléfono) o pública (prensa, radio, televisión), ha quedado diluida por soportes convergentes que permiten al

usuario integrar funcionalidades de comunicación privada y difusión pública en un único dispositivo o herramienta.

La dilución de esta escisión disipa consecuentemente el nexo entre medio utilizado y derecho protegido, forzando la revisión del formato de los procesos comunicacionales para entenderlos protegidos por el derecho fundamental al secreto de las comunicaciones.

La identificación y análisis de tales criterios constituye el objeto de la primera parte del segundo capítulo.

Además, se analiza la dimensión temporal del derecho fundamental, diferenciando aquellas fases del proceso comunicativo que, en atención al fundamento constitucional del derecho, deben integrar su objeto de otras cuya tutela corresponde a derechos fundamentales diversos como la intimidad o la protección de datos.

Finalmente, las consideraciones sobre la delimitación objetiva y temporal del concepto de comunicación protegido se proyectan en el estudio de las diversas modalidades comunicativas, ordenadas en comunicaciones postales y telegráficas, bidireccionales simultáneas y telemáticas alternativas.

* * * * *

El capítulo tercero se dedica al análisis del concepto de secreto del art. 18.3 CE.

Se examinan en primer lugar las características del concepto jurídico de secreto en el ordenamiento jurídico. Se procede así a una delimitación del alcance objetivo, subjetivo y temporal de la garantía de secreto, así como la posición del prestador del servicio en la relación comunicativa secreta.

Se aborda igualmente la identificación doctrinal y jurisprudencial del bien jurídico al que sirve el secreto: la libertad de comunicación.

Las transformaciones tecnológicas que con mayor profundidad han incidido en el concepto de secreto se deben a la generalización de técnicas de cifrado en las herramientas de comunicación interpersonal.

El cifrado transfigura el mensaje transmitido al convertirse en datos codificados inaccesibles a la percepción humana analógica. De tal manera que la técnica posibilita una garantía material de secreto casi absoluta, impidiendo la intervención eficaz de los poderes públicos incluso cuando la ruptura de secreto se satisfaga como como constitucionalmente legítima.

En tal sentido, se estudia la evolución de la criptografía y su relación con el derecho fundamental. Se analizan tanto las posibilidades de regulación general sobre los elementos internos de los sistemas criptográficos como los modos de intervención de comunicaciones cifradas.

* * * * *

Dedicamos un capítulo propio, el cuarto, al análisis del régimen jurídico de los datos de tráfico asociados a procesos comunicativos. La dificultad de su delimitación conceptual, así como las discrepancias doctrinales y jurisprudenciales sobre su encuadramiento iusfundamental justifican el tratamiento autónomo asignado.

La expresión *datos de tráfico* viene referida a una serie de componentes que, sin ser parte del contenido comunicado, acompañan inseparablemente a todo proceso comunicativo al exigirlo la necesaria intermediación técnica. Permiten, por ello, revelar diversas circunstancias contextuales de la relación comunicativa, como la identificación de los comunicantes, la fecha y duración de la comunicación, la ruta técnica seguida o los medios comunicativos utilizados.

La intervención legislativa en esta materia ha estado fuertemente impulsada por la Unión Europea y en un entorno de intensos debates políticos y gran conflictividad jurisprudencial.

En tal medida, el capítulo cuarto tiene por objeto tratar de clarificar el concepto de datos de tráfico y su diferenciación de otros datos afines, así como los diversos modos de su intervención por los poderes públicos.

Se analizan además los derechos fundamentales involucrados en los tratamientos de estos datos, distinguiendo entre intervención de datos asociados a comunicaciones en curso y acceso a datos de tráfico conservados por las operadoras o almacenados en registros en poder de los comunicantes.

* * * * *

El quinto y último capítulo afronta el estudio del contenido del derecho fundamental al secreto de las comunicaciones.

La primera parte aborda el contenido jurídico subjetivo del derecho, partiendo del análisis de la naturaleza jurídica de la intervención de comunicaciones constitucionalmente prevista.

Se analizan de modo sucesivo las características, fundamento y límites a que el legislador se ve sometido en la regulación del levantamiento del secreto, así como las garantías de la autorización judicial de intervención.

La segunda parte del capítulo da cuenta de la incidencia de la dimensión objetiva del derecho fundamental al secreto de las comunicaciones. Se examinan y clasifican las normas dirigidas a dar cumplimiento al deber de protección de los poderes públicos con el derecho analizado y la eficacia que la norma iusfundamental despliega en las relaciones entre particulares.

La Memoria de Tesis Doctoral se cierra con las pertinentes Conclusiones y los oportunos Anexos.

CAPÍTULO PRIMERO

DELIMITACIÓN DEL DERECHO FUNDAMENTAL DEL ART. 18.3 CE

I. INTRODUCCIÓN

II. UNA OJEADA HISTÓRICA

II.1. Nacimiento y expansión del derecho

II.2. El derecho al secreto de las comunicaciones en la historia constitucional española

II.3. El proceso constituyente de 1978

III. INTIMIDAD Y SECRETO DE LAS COMUNICACIONES: DOS DERECHOS AUTÓNOMOS Y DISTINTOS

IV. OBJETO Y CONTENIDO

IV.1. Objeto

IV.2. Contenido

V. TITULARIDAD

VI. SUSPENSIÓN DEL DERECHO

VI.1. Suspensión general (55.1 CE)

VI.2. Suspensión individual (55.2 CE)

I. INTRODUCCIÓN

El artículo 18.3 de la Constitución Española garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

Mediante el establecimiento de la garantía formal de secreto, que solo puede ser salvada por intervención judicial, se protege el derecho a comunicarse en libertad, sin intromisiones ajenas, en aquellos procesos comunicativos que se llevan a cabo a través de determinados medios técnicos.

Así, el constituyente decidió dotar este derecho, de larga tradición constitucional, con las más estrictas garantías previstas en la norma fundamental.

Disfruta, en su condición de derecho fundamental, de las garantías generales de vinculatoriedad y resistencia de su contenido esencial frente a la acción del legislador. Pero, además, forma parte del grupo de derechos que se benefician de otras garantías reforzadas (desarrollo por ley orgánica, acceso al amparo constitucional y reforma agravada).

Pese a ello, el legislador no se ha decidido hasta el momento a desarrollar este derecho más allá de determinadas normas procesales reguladoras —frecuentemente insuficientes— de las condiciones para levantar el secreto; lo que ha obligado a que su construcción se llevase a cabo, en su mayor parte, por la doctrina científica y jurisprudencial.

Se pretende en este capítulo exponer los términos en los que, hasta el momento, se ha producido la delimitación del derecho al secreto de las comunicaciones para, en los sucesivos, afrontar los problemas que actualmente retan a su objeto y contenido.

II. UNA OJEADA HISTÓRICA

II.1. Nacimiento y expansión del derecho

La génesis de los hoy reconocidos como derechos fundamentales se halla, como es sabido, en las declaraciones de derechos del último tercio del siglo XVIII¹. Sin embargo, ni la declaración de derechos de Virginia de 1776, ni la francesa de 1789, contienen referencia alguna al secreto o inviolabilidad de la correspondencia².

La necesidad de establecer este derecho surge con la generalización del uso de la correspondencia y la violación de su secreto³. En Francia, fue el cardenal Richelieu quien, a partir de 1620, puso el servicio de correos a disposición de los ciudadanos con la creación de *la poste aux lettres*⁴.

Sin embargo, la instauración de este servicio vino acompañada de la práctica de acceder al contenido de las cartas. Un claro exponente de institucionalización de esta práctica nació con el *Cabinet Noir* o *Cabinet des Secrets des Postes*, un servicio especial creado para abrir y controlar la

¹ Cfr. CRUZ VILLALÓN, P., «Formación y evolución de los derechos fundamentales», *Revista Española de Derecho Constitucional*, 25, 1989, págs. 35-62.

² Se ha apuntado como razón de esta ausencia el carácter fragmentario e incompleto de estos textos, que recogen aquellos aspectos de las libertades ciudadanas que más preocupaban a sus redactores en el contexto sociopolítico del momento. Vid. RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones y su interceptación legal*, Sepín, Madrid, 2016, pág. 20. En similar sentido, respecto del caso francés, para CRUZ VILLALÓN la constitucionalización de los derechos se va a producir en forma de un «intento fracasado», no agotando los derechos franceses su presencia en la Declaración. Cfr. CRUZ VILLALÓN, P., «Formación y evolución de los derechos fundamentales», *op.cit.*, pág. 49. El secreto de la correspondencia se incluyó, no obstante, en algunos trabajos preliminares de la declaración de derechos francesa, siendo finalmente suprimido por considerarse ya protegido en el derecho a comunicar libremente pensamientos y opiniones; vid. ZUIDERVEEN BORGESIUUS, F.J., y STEENBRUGGEN, W., «The right to communications confidentiality in Europe: protecting privacy, freedom of expression, and trust», *Theoretical Inquiries in Law*, Vol. 20, 1, 2019, págs. 295.

³ Es aquí oportuna la cita de MONTESQUIEU: «Las conspiraciones en el estado se han vuelto difíciles, porque desde la invención del correo, todos los secretos particulares están en poder del Estado». Vid. *Considérations sur les causes de la grandeur des Romains et de leur décadence*, 1734, pág. 134.

⁴ RICARD, J.D., *Droit et jurisprudence en matière de postes, télégraphes, téléphones*, Recueil Sirey, París, 1931, pág. 2.

correspondencia orientada a los intereses políticos o a la mera satisfacción de la curiosidad personal del monarca⁵.

Los abusos de este *Cabinet Noir* alentaron, sin duda, el desarrollo de las ideas liberales revolucionarias y el nacimiento del principio de inviolabilidad de la correspondencia⁶.

En el contexto del nacimiento del movimiento constitucional, la Asamblea Nacional francesa proclamó, en un decreto de 10 de agosto de 1790, el secreto e inviolabilidad de las cartas, disponiendo que «bajo ningún pretexto podrá ser infringido ni por los individuos ni por los cuerpos administrativos»⁷. Multiplicándose, a partir de este momento, las declaraciones encaminadas a conjurar las amenazas provenientes tanto del poder central como de los municipios⁸.

La Constitución belga de 1831 será la primera que reconozca entre su catálogo de derechos, y en términos absolutos, el de la inviolabilidad de la correspondencia, disponiendo en su artículo 29 que «[e]l secreto de las cartas es inviolable. La ley determina qué agentes son responsables de la violación del secreto de cartas confiadas a la oficina de correos».

Tras las revoluciones de 1848 la presencia de este derecho en las constituciones se generaliza⁹. En la Constitución del Imperio Alemán de 28 de

⁵ MARTÍN MORALES, R., *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid, 1995, págs. 21 y ss. Con anterioridad, ya una ordenanza de 1464 prescribía que los funcionarios reales abrieran las cartas transportadas por los correos, para descubrir si había algo que perjudicara el servicio del rey y contraviniera sus órdenes. RICARD, J.D., *Droit et jurisprudence en matière...*, *op.cit.*, pág. 111.

⁶ RICARD, J.D., *Droit et jurisprudence en matière...*, *op.cit.*, pág. 112.

⁷ Un nuevo decreto de 26 de agosto de ese mismo año establece la obligación de los empleados de correos de prestar juramento de respetar el secreto de las cartas y, el Código penal de 1791 castiga a quienes violasen el secreto postal, imponiendo penas más graves en caso de que tal conducta fuese cometida «por una orden del poder ejecutivo o por un oficial del servicio postal». RICARD, J.D., *Droit et jurisprudence en matière...*, *op.cit.*, pág. 115.

⁸ FERNÁNDEZ GARCÍA, J.J., «Inviolabilidad y secreto de la correspondencia», *Revista Española de Derecho Administrativo*, 39, 1983, pág. 559.

⁹ Art. 29 de la Constitución del Reino de las Dos Sicilias de 29 de enero de 1848; Constitución de Suiza de 1848; art. 9 de la Constitución de la República Romana de 1849. *Vid.*

marzo de 1849 se establece por primera vez la posibilidad de su limitación, al prever en su art. 141 la facultad de intervenir la correspondencia «en virtud de orden judicial motivada».

Las constituciones elaboradas tras la II Guerra Mundial no circunscriben este derecho únicamente al secreto de la correspondencia y extienden ya su ámbito de protección a otros medios de comunicación¹⁰.

Por su parte, los textos internacionales surgidos desde ese momento comparten la técnica de reconocer en un mismo precepto este derecho junto al respeto de la vida privada y familiar y la inviolabilidad del domicilio: así sucede en el art. 12 de la Declaración Universal de los Derechos Humanos de 1948, el art. 8 del Convenio Europeo de Derechos Humanos y el art. 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966¹¹.

II.2. El derecho al secreto de las comunicaciones en la historia constitucional española

En el caso de España, no será hasta mediados del siglo XVIII cuando el correo adquiera una eficaz organización como servicio público, culminando su implantación casi definitiva con la aparición del sello o timbre postal en 1850¹².

Sin embargo, el reconocimiento del derecho al secreto de la correspondencia en un texto constitucional tardará más en llegar. Hasta entonces sólo encontraremos cierta protección jurídica de las comunicaciones

RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho al secreto de las comunicaciones: dimensión constitucional e histórica», *Diario La Ley*, 7647, 2011, pág. 8.

¹⁰ Vid. v.gr. art. 15 de la Constitución de la República Italiana de 1947 y art. 10 de la Ley Fundamental de Bonn de 1949.

¹¹ RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, op.cit., pág. 25.

¹² BAHAMONDE, A., *Las comunicaciones del siglo XIX al XX. Correo, telégrafo y teléfono*, Santillana, Madrid, 1996, págs. 9 y ss.

en normas que imponen el deber de confidencialidad de los prestadores de servicios postales¹³.

La Constitución de 1869 es la primera en la historia constitucional española en prohibir la detención y apertura de la correspondencia en su artículo 7:

«En ningún caso podrá detenerse ni abrirse por la Autoridad gubernativa la correspondencia confiada al correo, ni tampoco detenerse la telegráfica. Pero en virtud de auto de juez competente podrán detenerse una y otra correspondencia, y también abrirse en presencia del procesado la que se le dirija por correo».

El constituyente español variará así la técnica de garantía respecto de sus antecedentes europeos. No declara la inviolabilidad de la correspondencia, sino que «se la examina desde su punto de vista negativo: la prohibición que tienen los poderes públicos a su acceso»¹⁴.

Además de prever expresamente, en su artículo 8, la motivación de la resolución que ordenare la detención de la correspondencia, el «celo garantizador» del constituyente de 1869 incluía «una indemnización proporcionada al daño causado» en los casos en que se incumpliere aquel requisito o los motivos alegados se declarasen «ilegítimos o notoriamente insuficientes»¹⁵.

Esta regulación fue reproducida casi literalmente, excepción hecha de la cláusula indemnizatoria, en el art. 7 de la Constitución de 1876¹⁶. Y, al coincidir

¹³ RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho...», *op.cit.*, págs. 7 y ss.

¹⁴ RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho...», *op.cit.*, pág. 12.

¹⁵ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *Revista Española de Derecho Constitucional*, 20, 1987, pág. 37.

¹⁶ «No podrá detenerse ni abrirse por la autoridad gubernativa la correspondencia confiada al correo», pero sí por la autoridad judicial, ya que el artículo 8 disponía que «[t]odo auto [...] de detención de la correspondencia, será motivado».

su promulgación con el momento álgido del proceso codificador español, el desarrollo procesal de este derecho se plasmó además en diversas normas¹⁷.

Por su parte, el art. 32 de la Constitución de 1931 proclamó este derecho en términos positivos y con una redacción abierta en cuanto al objeto protegido: «Queda garantizada la inviolabilidad de la correspondencia en todas sus formas, a no ser que se dicte auto judicial en contrario»¹⁸.

En resumen, y como se ha señalado, la regulación de este derecho en todas las constituciones españolas anteriores contenía ya las dos proposiciones que se mantienen en nuestro actual art. 18.3 CE: la garantía del secreto y la previsión de su levantamiento judicial¹⁹.

II.3. El proceso constituyente de 1978

La Constitución española de 1978 recoge un amplio catálogo de derechos fundamentales, entre los que se incluye el derecho fundamental al secreto de las comunicaciones.

El Anteproyecto de Constitución propuso, en su art. 18.3, declarar el derecho en los siguientes términos: «Se garantiza el secreto de las comunicaciones postales, telegráficas y telefónicas, salvo mandato judicial»²⁰.

¹⁷ Artículos 579 a 588 de la Ley de Enjuiciamiento Criminal de 1882, 517 a 523 del Código de Justicia Militar de 1890 y 230 a 237 de la Ley de Enjuiciamiento Militar de la Marina de 1894. Vid. FERNÁNDEZ GARCÍA, J.J., «Inviolabilidad y secreto de la correspondencia», *op.cit.*, pág. 559.

¹⁸ RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho...», *op.cit.*, pág. 12.

¹⁹ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 36.

²⁰ BOCG, Congreso de los Diputados, núm. 44, de 5 de enero de 1978.

Las cuatro enmiendas presentadas en el Congreso perseguían el objetivo común de introducir expresamente la necesidad de que el mandato judicial que permitía levantar el secreto fuera motivado²¹.

Además, la enmienda número 339, presentada por el Grupo Socialista del Congreso, propuso una redacción abierta de las comunicaciones protegidas, separando el *genus* —«comunicaciones»— de la *species* —«postales, telegráficas y telefónicas»— mediante la introducción de la cláusula «en especial». No se hace, sin embargo, referencia a tan trascendental extremo en la justificación de la enmienda²².

El Informe de la Ponencia incluyó parcialmente esta enmienda, ampliando así el ámbito de protección a todas las comunicaciones. La redacción surgida de la Ponencia será, en esencia, la finalmente plasmada en el texto constitucional²³.

En el debate en Comisión de Asuntos Constitucionales y Libertades Públicas se acordó sustituir el término «mandamiento judicial» por el de «resolución judicial», alcanzando de esta manera una solución intermedia entre el texto propuesto en las enmiendas —«resolución judicial motivada»— y la redacción del anteproyecto. La oposición por parte del Grupo

²¹ Enmiendas número 116 (Grupo Parlamentario de la Minoría Catalana), 339 (Grupo Socialista del Congreso), 470 (Grupo Parlamentario Mixto) y 695 (Grupo Parlamentario Comunista).

²² El texto propuesto fue el siguiente: «Se garantiza el secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial motivada». Por su parte, la enmienda núm. 470, del Grupo Parlamentario Mixto, también propuso ampliar la protección a «otros medios de comunicación», además de garantizar expresamente no solo el secreto, sino también la libertad de las comunicaciones. No obstante, esta redacción se encontraba presente en el Borrador de Proyecto de Constitución publicado, junto con las actas de la Ponencia constitucional, en 1984. *Vid.* «Las actas de la Ponencia constitucional», *Revista de las Cortes Generales*, 2, 1984, pág. 384.

²³ «Se garantiza el secreto de las comunicaciones y en especial de las postales, telegráficas y telefónicas, salvo mandamiento judicial» (BOCG, Congreso de los Diputados, núm. 82, de 17 de abril de 1978). Algún autor ha atribuido, quizá erróneamente, esta redacción abierta de las comunicaciones protegidas a una enmienda presentada en el Senado, pero lo cierto es que la misma, desde su admisión por la Ponencia, se mantendrá ya en el texto hasta su aprobación definitiva. *Vid.* RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, pág. 30.

Parlamentario de Unión de Centro Democrático a las enmiendas presentadas se justificó en dos razones: el carácter recurrible de la «resolución judicial motivada» y la necesidad, en caso de asumir tal redacción, de dar audiencia a las partes antes de dictarla, lo que haría perder el sentido a gran parte de las intervenciones adoptadas²⁴.

La redacción finalmente aprobada por el Congreso fue, por tanto, la hoy vigente: «Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial»²⁵.

Dos enmiendas fueron presentadas en el Senado. Retirada una de ellas en el debate en Comisión, la otra fue aprobada y recogida en el Dictamen de la Comisión de Constitución del Senado²⁶, aprobado después por el Pleno²⁷: «Se garantiza la libertad y el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

Finalmente, en las deliberaciones de la Comisión Mixta, de carácter secreto, se eliminó la previsión expresa de la garantía de la libertad de las comunicaciones, introducida en el Senado, resultando como texto aprobado del artículo 18.3, en el Dictamen de la Comisión Mixta²⁸, aquel que finalmente sería el recogido en la Constitución:

«Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

²⁴ Diario de Sesiones del Congreso de los Diputados, núm. 70, del 19 de mayo de 1978, págs. 2520 y ss.

²⁵ BOCG, Congreso de los Diputados, núm. 135, de 24 de julio de 1978.

²⁶ BOCG, Senado, núm. 157, de 6 de octubre de 1978.

²⁷ BOCG, Senado, núm. 161, de 13 de octubre de 1978.

²⁸ BOCG núm. 170, de 28 de octubre de 1978.

III. INTIMIDAD Y SECRETO DE LAS COMUNICACIONES: DOS DERECHOS AUTÓNOMOS Y DISTINTOS

El artículo 18 de la Constitución española acoge diferentes derechos dotados para proteger, aun reflejamente, determinados aspectos de la vida privada, que no es, o no queremos que sea, de general conocimiento: tal es el caso del derecho a la intimidad (art. 18.1), la inviolabilidad del domicilio (18.2), el secreto de las comunicaciones (18.3), la protección de los datos de carácter personal (18.4) y, en cierto modo, el derecho a la propia imagen (18.1)²⁹.

Ahora bien, su aptitud común para proteger la vida privada no borra las fronteras entre los mismos: sus diferentes objetos y contenidos estrictamente definidos³⁰.

No obstante, alguna doctrina y, en ocasiones, el Tribunal Constitucional han conectado los derechos a la intimidad y al secreto de las comunicaciones, quizá incluso sugiriendo una desigual posición iusfundamental, recurriendo al bien jurídico cuya protección comparten. Se llegará a afirmar que «toda aproximación al secreto de las comunicaciones y a la necesidad de su protección como derecho debe tener como punto de partida la relación que lo une a la noción de intimidad»³¹.

Y hay incluso posiciones que llegan a considerar el secreto de las comunicaciones como un derecho vicario del de intimidad, al entender que aquel «constituye una garantía del derecho a la vida privada y, en especial, a

²⁹ ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, Aranzadi, Cizur Menor, 2015, pág. 97.

³⁰ En similares términos, sobre la amplitud e indefinición del concepto de privacidad, *vid.* JOVE VILLARES, D., «*Quo vadis, intimidad?*», AA.VV., *Setenta años de Constitución Italiana y cuarenta años de Constitución Española*, Vol. II, Boletín Oficial del Estado – Centro de Estudios Políticos y Constitucionales, Madrid, 2020, págs. 151-165.

³¹ RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones: tecnología e intimidad*, McGraw-Hill, Madrid, 1998, pág. XVII. En similar sentido, se ha dicho que «[e]l estudio del derecho al secreto de las comunicaciones tiene como referente principal el derecho a la intimidad y, al igual que éste, desemboca, como toda la Constitución en bloque, en el valor superior de libertad». MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 23.

la intimidad personal que constituye su núcleo esencial»³². Involucran así el bien jurídico en cuya protección coinciden con el objeto jurídico de ambos derechos fundamentales. Un deslizamiento en el que es fácil incurrir, pero que no debería producirse.

También el Tribunal Constitucional se ha pronunciado en similar dirección, al afirmar que «la observación de las telecomunicaciones supone una grave injerencia en la esfera de la intimidad personal»³³. Y el Tribunal Supremo, cuando dice que «este secreto de las comunicaciones, que en sede constitucional se trata de garantizar, no es sino una manifestación, y muy cualificada, del derecho a la intimidad personal y familiar»³⁴. Con frecuencia, según se ve, el fervor argumental lo es en menoscabo del rigor jurídico.

La mayoría de la doctrina, sin embargo, ha mantenido una postura equilibrada, defendiendo una vinculación entre ambos derechos en los términos antes descritos, pero desde su autonomía. El derecho fundamental

³² MONTAÑÉS PARDO, M.A., *La intervención de las comunicaciones. Doctrina jurisprudencial*, Aranzadi, Pamplona, 1999, pág. 22. También se expresa en este sentido FRÍGOLS BRINES cuando afirma que «estos derechos fundamentales sirven, en última instancia, a la protección de la intimidad como elemento fundamental, entendida ésta de un modo amplio, como barrera jurídica a la intromisión de terceros, tanto del Estado como de particulares, siendo los derechos a la inviolabilidad del domicilio y al secreto de las comunicaciones manifestaciones concretas de este derecho fundamental de libertad, desgajadas del mismo a los meros efectos de una mejor protección de esas parcelas de la realidad». FRÍGOLS BRINES, E., «La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías», en BOIX REIG, J. (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, pág. 43.

³³ ATC 344/1990, de 1 de octubre. También, respecto el 18.2 CE: «[...] la protección constitucional del domicilio es una protección de carácter instrumental, que defiende los ámbitos en que se desarrolla la vida privada de la persona. Por ello, existe un nexo de unión indisoluble entre la norma que prohíbe la entrada y el registro en un domicilio (art. 18.2 de la Constitución) y la que impone la defensa y garantía del ámbito de privacidad (artículo 18.1 de la Constitución)»; STC 22/1984, de 17 de febrero (FJ. 2).

³⁴ STS, Sala de lo Penal, de 20 de diciembre de 1996 (FJ. 5). Como se ha dicho, también esta opinión ha calado en ocasiones en el legislador, poniendo como ejemplo la Exposición de motivos de la Ley Orgánica 7/1984, de 7 de octubre sobre tipificación penal de escuchas telefónicas, que dispone: «Establecido en nuestra Constitución el secreto de las comunicaciones telefónicas como uno de los principios de la protección que nuestra máxima Ley dispensa al honor y a la intimidad personales, se hace necesario tipificar penalmente los comportamientos que atenten contra dicho bien jurídico». JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 40.

al secreto de las comunicaciones —como la inviolabilidad del domicilio— tendría como objetivo garantizar autónomamente un ámbito concreto de la intimidad formalizado en los respectivos objetos de los derechos³⁵.

Este parece ser el sentido de la STC 110/1984, de 26 de noviembre (FJ. 3), cuando considera la necesidad de proteger el domicilio «como espacio físico en que normalmente se desenvuelve la intimidad» y la correspondencia en tanto «que es o puede ser medio de conocimiento de aspectos de la vida privada».

Comunicaciones y domicilio se entienden, pues, como áreas «reservadas al disfrute de la intimidad». En ellas tal disfrute simplemente se presume y, por tanto, su protección jurídica se adelanta en forma de garantía formal³⁶.

Consideramos, sin embargo, más acertadas las opiniones que mantienen una nítida diferenciación entre ambos derechos, entendiendo que «el derecho constitucional al secreto de las comunicaciones se configura como una situación jurídica en sí misma, para cuya interpretación no es necesario —y sí perturbador— acudir a los criterios que puedan entenderse presentes en el enunciado de otros derechos fundamentales»³⁷. Aun cuando converjan en muchas ocasiones en la finalidad que persigan, contienen

³⁵ Vid. MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, págs. 23 y ss., RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, págs. 14 y ss., REBOLLO DELGADO, L., «El secreto de las comunicaciones: problemas actuales», *Revista de Derecho Político*, 48-49, 2000, págs. 360 y ss. y DÍAZ REVORIO, F.J., «El derecho fundamental al secreto de las comunicaciones», *Derecho PUCP. Revista de la Facultad de Derecho*, 59, 2006, pág. 160.

³⁶ RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, págs. 16-17. También CARRILLO: «Ciertamente, el ámbito espacial o territorial del derecho a la intimidad queda protegido, *prima facie*, por el derecho a la inviolabilidad del domicilio (art. 18.2 CE) y, en su caso, también, por el derecho a la inviolabilidad de las comunicaciones (art. 18.3 CE)». Cfr. CARRILLO, M., «Los ámbitos del derecho a la intimidad en la sociedad de la comunicación», AA.VV., *El derecho a la privacidad en un nuevo entorno tecnológico*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pág. 28.

³⁷ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 39.

objetos, contenidos e instrumentación garantista distintos. Son cabalmente, derechos fundamentales distintos.

El art. 18.3 protege la comunicación en sí y, en todo caso, mediante el instituto jurídico del secreto³⁸, con independencia del carácter íntimo de su contenido. Frente al concepto de intimidad, el secreto de las comunicaciones es pues rigurosamente formal³⁹. «Toda comunicación es, para la norma fundamental, secreta, aunque sólo algunas, como es obvio, serán íntimas»⁴⁰.

Pero esa separación se proyecta también sobre el régimen de protección constitucional de ambos derechos: «si ex art. 18.3 CE la intervención de las comunicaciones requiere siempre resolución judicial, no existe en la Constitución reserva absoluta de previa resolución judicial respecto del derecho a la intimidad personal»⁴¹.

La especialidad de las comunicaciones protegidas en el art. 18.3 reside en la participación de un tercero que, por sí o mediante diversas técnicas, hace posible la comunicación. Tal intervención origina la necesaria protección constitucional del secreto de las comunicaciones⁴².

En este sentido, el Tribunal Constitucional ha señalado que «[...] el fundamento del carácter autónomo y separado del reconocimiento de este

³⁸ «If only private communication were protected, it would be necessary to access the communication to determine whether or not it deserves protection. Then, the content of communication would already be disclosed, thereby infringing privacy and confidentiality». Cfr. ZUIDERVEEN BORGESIU, F.J., y STEENBRUGGEN, W., «The right to communications confidentiality...», *op.cit.*, pág. 315.

³⁹ «[...] el concepto de "secreto" en el art. 18.3 tiene un carácter "formal", en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado». STC 114/1984, de 29 de noviembre (FJ. 7).

⁴⁰ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 41. Para defender, pese a ello, una vinculación entre ambos derechos se ha dicho que «[...] al margen del carácter del contenido del mensaje que se comunica (íntimo o no) puede afirmarse que el emisor presenta respecto a ese mensaje una auténtica expectativa de intimidad pues conoce el secreto del mismo al usar como soporte un canal cerrado». Cfr. FERNÁNDEZ RODRÍGUEZ, J. J., *Secreto e intervención de las comunicaciones en internet*, Civitas, Madrid, 2004, pág. 89.

⁴¹ STC 123/2002, de 20 de mayo (FJ. 5).

⁴² RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho...», *op.cit.*, pág. 3.

derecho fundamental y de su específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación»⁴³.

Pero añade a continuación que tal reconocimiento autónomo «no impide naturalmente que pueda contribuir a la salvaguarda de otros derechos, libertades o bienes constitucionalmente protegidos, como el secreto del sufragio activo, la libertad de opinión, ideológica y de pensamiento, de la libertad de empresa, la confidencialidad de la asistencia letrada o, naturalmente también, el derecho a la intimidad personal y familiar»⁴⁴.

No obstante, consideramos que afirmaciones de este tipo no deben llevar a caer en el error de confundir la capacidad del derecho de salvaguardar, potencialmente y de forma refleja, otros bienes jurídicos, con su objeto específico de protección, que debe ser estrictamente delimitado.

⁴³ SSTC 123/2002, de 20 de mayo (FJ. 5) y 281/2006, de 9 de octubre de 2006 (FJ. 3).

⁴⁴ En el mismo sentido MARTÍN MORALES atribuye al derecho fundamental al secreto de las comunicaciones «[...] la función de garantía de una variedad de derechos y libertades: contribuye a asegurar la libertad ideológica y política, garantiza la libertad de empresa, el secreto profesional, etc.». MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 43.

IV. OBJETO Y CONTENIDO

IV.1. Objeto

El objeto de un derecho fundamental se identifica con el ámbito jurídicamente tipificado de la realidad que la norma iusfundamental garantiza, es decir, con el «espacio de autodeterminación constitucionalmente configurado»⁴⁵. Al delimitar el objeto de un derecho fundamental estamos, por tanto, aludiendo a aquello que protege.

Para tal fin la norma define en ocasiones positivamente la esfera de libertad individual que garantiza mediante un permiso. Lo que se protege en estos casos —por ejemplo, la libertad ideológica o la libertad de expresión— es un *agere licere* constitucionalmente formalizado «con plena inmunidad de coacción del Estado y de cualesquiera grupos sociales»⁴⁶.

En otras ocasiones, como es nuestro caso, la configuración de ese espacio de autodeterminación se produce indirectamente, mediante una prohibición constitucional que, como reflejo, define el ámbito de libertad garantizado⁴⁷.

El art. 18.3 CE, pues, prohíbe la intervención de las comunicaciones mediante la imposición expresa de su secreto y, a su través, garantiza la libertad para llevarlas a cabo: «el secreto es aquí condición de libertad»⁴⁸.

⁴⁵ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 38 y BASTIDA FREIJEDO, F., VILLAVERDE MENÉNDEZ, I., REQUEJO RODRÍGUEZ, P., PRESNO LINERA, M.A., ALÁEZ CORRAL, B., FERNÁNDEZ SARASOLA, I., *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, 2004, pág. 103.

⁴⁶ STC 24/1982, de 13 de mayo (FJ. 1). *Vid.* BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 103 y VILLAVERDE MENÉNDEZ, I., «Concepto, contenido, objeto y límites de los derechos fundamentales», AA.VV., *La democracia constitucional. Estudios en homenaje al Profesor Francisco Rubio Llorente*, Congreso de los Diputados, Madrid, 2002, pág. 333.

⁴⁷ VILLAVERDE MENÉNDEZ, I., «Concepto, contenido, objeto y límites...», *op.cit.*, pág. 333.

⁴⁸ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 51.

Así lo ha manifestado el Tribunal Constitucional al afirmar que «[r]ectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas»⁴⁹.

En consecuencia, el objeto del derecho fundamental descrito en el art. 18.3 CE vendrá determinado por el significado que otorguemos a los conceptos de *secreto* y de *comunicaciones*.

Al análisis de cada uno de estos elementos dedicaremos los capítulos sucesivos del presente trabajo. Pero conviene adelantar ahora el entendimiento por la jurisprudencia constitucional de algunos aspectos.

Tal y como ya hemos dejado dicho, el secreto garantizado en el artículo 18.3 CE es de carácter formal, «en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado»⁵⁰.

El proceso comunicacional se protege con independencia del contenido —incluso aunque tal contenido no exista— como única posibilidad de asegurar su libertad. Y por tanto no es preciso acudir a presunción alguna de la naturaleza del contenido⁵¹.

La garantía formal prevista se impone a los terceros ajenos a la comunicación, pero no a quienes participan en ella. Por tanto, no existe un deber de secreto para los interlocutores derivado del 18.3 CE, sino, en su

⁴⁹ STC 114/1984, de 29 de noviembre (FJ. 7).

⁵⁰ STC 114/1984, de 29 de noviembre (FJ. 7).

⁵¹ En la resolución que venimos citando, el Tribunal Constitucional quiso ver en el carácter formal de secreto la existencia de una «presunción iuris et de iure de que lo comunicado es “secreto”, en un sentido sustancial»; STC 114/1984, de 29 de noviembre (FJ. 7). En este sentido, se ha afirmado que no son «las comunicaciones privadas las que determinan el núcleo de la garantía, sino la privacidad de la comunicación»; cfr. RIDAURA MARTÍNEZ, M.J., «El legislador ausente del artículo 18.3 de la Constitución (la construcción pretoriana del derecho al secreto de las comunicaciones)», *Revista de Derecho Político*, 100, 2017, pág. 357.

caso, y en función del contenido de la comunicación, un «deber de reserva» impuesto por el derecho a la intimidad del 18.1 CE y ajeno por tanto al derecho que nos ocupa⁵².

No hay pues vulneración del derecho al secreto de las comunicaciones cuando uno de los interlocutores autoriza el acceso o conocimiento⁵³.

Por su parte, el ámbito objetivo del secreto no alcanza solo al contenido de la comunicación, «sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales»⁵⁴.

Para el caso de las comunicaciones telefónicas, el Tribunal Constitucional ha mantenido que el secreto comprende «la existencia de la comunicación misma y el contenido de lo comunicado, así como la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino»⁵⁵.

Por ello, el Tribunal Constitucional ha entendido incluido en el ámbito de protección del art. 18.3 CE tanto la entrega por parte de la compañía suministradora del servicio de telefonía de listados de llamadas telefónicas a la policía (STC 123/2002, de 20 de mayo), como el acceso directo por parte de los agentes al registro de llamadas en el teléfono móvil incautado a un detenido (STC 230/2007, de 5 de noviembre).

⁵² STC 114/1984, de 29 de noviembre (FJ. 7). En contra de esta opinión, que consideramos la más acertada, se ha defendido, con base en el entendimiento de que el secreto de las comunicaciones se dirige a proteger la intimidad de la persona, que «el objeto es, sin duda, la reserva del contenido de la carta» y, por tanto, atentaría contra este derecho, «la publicación no autorizada de la carta» y «la divulgación, aun sin publicación, del contenido de la misma». Cfr. FERNÁNDEZ GARCÍA, J.J., «Inviolabilidad y secreto de la correspondencia», *op.cit.*, pág. 561.

⁵³ Tal es el caso de permitir a los agentes de la Guardia Civil el acceso al registro de sus conversaciones telefónicas. STC 56/2003, de 24 de marzo (FJ. 3).

⁵⁴ STC 114/1984, de 29 de noviembre (FJ. 7).

⁵⁵ STC 123/2002, de 20 de mayo (FJ. 5).

Por otro lado, el concepto de comunicación que se contiene en el art. 18.3 CE «no se extiende a todos los fenómenos de comunicación entre personas, ni alcanza a cualesquiera materiales con ella relacionados presentes, pasados o futuros»⁵⁶.

La norma no ofrece, sin embargo, una definición de qué deba entenderse por *comunicación*, limitándose a hacer expresa referencia a las «postales, telegráficas y telefónicas».

La cláusula —«en especial»— que precede a esta enumeración no debe ser interpretada en el sentido de que esas tres modalidades requieran o merezcan una especial protección, sino que se trata simplemente de los sistemas comunicativos de uso generalizado en el momento de elaborarse nuestra Constitución⁵⁷.

En consecuencia, prácticamente la unanimidad de la doctrina ha entendido que aquella enumeración no constituye un *numerus clausus* de comunicaciones y es posible, por tanto, su ampliación a otras modalidades comunicativas, «cualquiera que sea el sistema empleado para realizarlas»⁵⁸.

Esta extensión queda sujeta, no obstante, a ciertas cautelas, «de modo que la noción constitucional de comunicación ha de incorporar los elementos o características comunes a toda clase de comunicación»⁵⁹, que vendrán, a su vez, determinadas —añadimos— por el fundamento de la protección de este derecho, que, como dijimos, se halla en la «evidente vulnerabilidad de las

⁵⁶ STC 170/2013, de 7 de octubre (FJ. 4).

⁵⁷ Entre otros, MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 45 y RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. 67.

⁵⁸ STC 70/2002, de 3 de abril (FJ. 9). En el mismo sentido, además de los citados en la nota anterior, ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, Iustel, Madrid, 2007, pág. 16 y RIDAURA MARTÍNEZ, M.J., «El legislador ausente del artículo 18.3...», *op.cit.*, pág. 370.

⁵⁹ STC 281/2006, de 9 de octubre (FJ. 3).

comunicaciones realizadas en canal cerrado a través de la intermediación técnica de un tercero»⁶⁰.

Así, en primer lugar, se ha entendido que «la comunicación es a efectos constitucionales el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos», no sólo en soporte escrito, sino también «en otros soportes que los incorporan —cintas de cassette o de vídeo, CD's o DVD's, etc.—»⁶¹.

En segundo lugar, el derecho fundamental sólo garantiza el secreto de las comunicaciones «que se realizan a través de determinados medios o canales cerrados»⁶².

No forman parte del objeto de este derecho las comunicaciones legalmente configuradas como *comunicación abierta*; lo que tiene lugar «cuando es legalmente obligatoria una declaración externa de contenido, o cuando bien su franqueo o cualquier otro signo o etiquetado externo evidencia que [...] no pueden contener correspondencia, pueden ser abiertos de oficio o sometidos a cualquier otro tipo de control para determinar su contenido»⁶³.

Pero también cuando «se realizan en un canal del que no puede predicarse su confidencialidad», por ejemplo, por hallarse sometido al poder de fiscalización empresarial⁶⁴.

⁶⁰ STC 170/2013, de 7 de octubre (FJ. 4).

⁶¹ STC 281/2006, de 9 de octubre (FJ. 3).

⁶² STC 170/2013, de 7 de octubre (FJ. 4). Este elemento está presente en los tres tipos de comunicación expresamente mencionados en el art. 18.3 CE, por lo que se ha indicado que «la cláusula “especialmente” no autoriza a ampliar la cobertura del derecho a cualquier tipo de comunicación, sino que se limita a actuar como fórmula de apertura de cara al desarrollo futuro de nuevas formas de comunicación a distancia por canal cerrado». RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. 67.

⁶³ STC 281/2006, de 9 de octubre (FJ. 3).

⁶⁴ STC 170/2013, de 7 de octubre (FJ. 4). Actividad fiscalizadora que se ha considerado amparada, por ejemplo, en la prohibición de instalar programas en los ordenadores de uso común de la empresa (STC 241/2012, de 17 de diciembre) o en el hecho de tipificarse en el convenio colectivo la utilización por los trabajadores de los medios informáticos de la empresa para fines distintos de los relacionados con la prestación laboral (STC 170/2013, de 7 de octubre).

Asimismo, la comunicación debe ser también cerrada desde el punto de vista de su determinación subjetiva, debiendo entenderse excluidas las comunicaciones dirigidas a un número indeterminado de personas —como sucede en los medios de masas—, pero no aquellas que permiten una conversación entre más de dos personas como la multiconferencia o, en principio, los grupos de intercambio de mensajería instantánea (*WhatsApp*, *Telegram*, etc.)⁶⁵.

Además, es necesario que la comunicación se lleve a cabo a través de la intermediación técnica de un tercero que, mediante la puesta a disposición del canal a través del cual se produce la comunicación, la haga posible⁶⁶.

Por ello, la gran mayoría de la doctrina ha entendido que no serán objeto de protección de este derecho las conversaciones directas. Estas deberán hallar amparo, en su caso, en el derecho a la intimidad⁶⁷.

Sin embargo, la STC 145/2014, de 22 de septiembre (FJ. 7) consideró que las grabaciones por parte de la policía de las conversaciones mantenidas entre dos detenidos en los calabozos habían vulnerado el derecho fundamental al secreto de las comunicaciones, al entender que «el art. 18.3 CE no dispone una distinta protección de las conversaciones telefónicas [...] que de otras comunicaciones como las verbales, sino solo una garantía común

⁶⁵ DÍAZ REVORIO, F.J., «El derecho fundamental al secreto de las comunicaciones», *op.cit.*, págs. 162-163.

⁶⁶ STC 170/2013, de 7 de octubre (FJ. 4).

⁶⁷ «La comunicación “directa” [...] no es “secreta” en este sentido formal o, en otras palabras, su “secreto” no consiste en una atribución normativa ajena al contenido y a las circunstancias en que la misma se desarrolle. JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 49. También en este sentido ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, *op.cit.*, pág. 16. Para MARTÍN MORALES «la Constitución ha querido distinguir entre los casos de interceptación de una comunicación y los casos en que la acción humana creadora de intimidad sea objeto de captación, aunque sea a través de artificios o técnicas de sonido o imagen. Cuando hablamos de la exigencia de un soporte técnico nos referimos al de la comunicación y no al de la interferencia». , MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 52.

y genérica frente a la impenetrabilidad por terceros ajenos a la comunicación misma»⁶⁸.

Algunos autores han entendido también necesario que los comunicantes se encuentren físicamente separados, mediando entre ellos una distancia «entendida racionalmente como la imposibilidad de hablar en persona»⁶⁹.

Consideramos, sin embargo, que tal imposibilidad no es determinante. Si la comunicación se produce a través de un medio técnico cerrado deberá entenderse protegida por el 18.3 CE, aunque no exista distancia física entre los sujetos que participan ni impedimento alguno para mantener una conversación directa. Tal sería, por ejemplo, el caso de un envío de correo electrónico entre compañeros de trabajo que se encuentran en la misma dependencia; o el envío de un SMS a una persona que se halla en la misma habitación. Ambos casos deberán entenderse amparados por el derecho fundamental al secreto de las comunicaciones.

Por tanto, siempre que se cumplan con los requisitos expuestos, será posible ampliar la protección dispensada por el art. 18.3 CE a otras modalidades comunicativas no expresamente mencionadas.

El Tribunal Constitucional ha reconocido que «los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a

⁶⁸ El Tribunal justifica la estimación del amparo en la inexistencia de habilitación legal suficiente para practicar las grabaciones, al no considerar de aplicación para este caso, entendemos que acertadamente, el art. 579 LECrim y la jurisprudencia que había desarrollado los requisitos a observar en la intervención de comunicaciones telefónicas. Sin embargo, ni siquiera se plantea el Tribunal, pese a sus anteriores pronunciamientos, si la conversación grabada podría entenderse incluida en el concepto constitucional de comunicación que se deriva del art. 18.3 CE.

⁶⁹ BELDA PÉREZ-PEDRERO, E., «El derecho al secreto de las comunicaciones», *Parlamento y Constitución*, 2, 1998, pág. 174. En la misma dirección, se ha puesto como ejemplo de imposibilidad de contacto directo, pero sin que exista distancia física entre los interlocutores el caso de los locutorios en establecimientos penitenciarios. MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, págs. 51-52.

esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE»⁷⁰.

Debemos entender, pues, que forman parte del concepto constitucional de comunicación aquellas formas comunicativas derivadas de la incorporación de nuevas tecnologías, tales como correo electrónico, *chats* de mensajería instantánea, mensajes *SMS* o videoconferencias⁷¹.

Finalmente, la comunicación constituye siempre un proceso, lo que permitirá determinar «los términos temporales dentro de los que se desenvuelve la relación protegida y al margen de los cuales ésta desaparece»⁷².

En este sentido, la STC 70/2002, de 3 de abril (FJ. 9) ha precisado que «[l]a protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos»⁷³.

Teniendo en cuenta las consideraciones anteriores, podemos afirmar, con FERNÁNDEZ RODRÍGUEZ, que «[p]or comunicación en este supuesto hay que entender todo proceso de transmisión de mensajes a través de un soporte que se presente como un canal cerrado, lo que hará que el emisor

⁷⁰ STC 70/2002, de 3 de abril (FJ. 9).

⁷¹ Vid. ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 36.

⁷² JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 43.

⁷³ Esta delimitación temporal se encuentra ya en los primeros reconocimientos constitucionales del derecho, ya que, al proclamarse la inviolabilidad de la correspondencia «confiada al correo» se protege «en aquel momento en el que se muestra más vulnerable: mientras se encuentra en tránsito y bajo la custodia de un servicio postal generalmente dependiente del poder público». RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho...», *op.cit.*, pág. 9.

tenga razonables expectativas de que se garantiza su libertad de comunicación»⁷⁴.

IV.2. Contenido

Si el objeto del derecho hace referencia al ámbito de libertad garantizado, su contenido lo integran las facultades jurídicas que su titular posee para defenderlo⁷⁵.

Definir el contenido de este derecho fundamental consistirá, pues, en averiguar cómo se protege el espacio de autodeterminación que garantiza.

El art. 18.3 CE, como sabemos, salvaguarda la libertad de las comunicaciones a través de su secreto. Sin embargo, esa libertad no se garantiza en términos absolutos, ya que la norma permite levantar legítimamente el secreto mediante resolución judicial⁷⁶.

El contenido de este derecho consistirá, pues, «en la reivindicación por su titular de la garantía así prevista —la resolución judicial, en este caso, aunque no sólo ella— como medio de defensa frente a los atentados de que aquél pudiera ser objeto»⁷⁷.

⁷⁴ FERNÁNDEZ RODRÍGUEZ, J. J., *Secreto e intervención de las comunicaciones...*, *op.cit.*, pág. 94.

⁷⁵ BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 109.

⁷⁶ RODRÍGUEZ RUÍZ se refiere a esta cuestión abogando por una «estructura a dos niveles» del derecho fundamental, diferenciando entre *ámbito de cobertura* y *ámbito de protección*. El primero de estos conceptos, el *ámbito de cobertura*, hace referencia a todo el ámbito conceptual del derecho, integrado por todas aquellas situaciones en las que está llamado a actuar. Por su parte, el *ámbito de protección*, más reducido, vendría solamente delimitado por aquellas injerencias en el ámbito de cobertura del derecho que se hubieran producido sin observar los requisitos previstos por la Constitución y sus normas de desarrollo. Así, cualquier intervención de una comunicación supondría una injerencia en el *ámbito de cobertura* del derecho al secreto de las comunicaciones, pero sólo si la misma se ha producido sin respetar las condiciones constitucionalmente requeridas se entendería vulneradora de su *ámbito de protección*. RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, págs. 43 y ss.

⁷⁷ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 56.

El derecho que nos ocupa se configura como una prohibición —la de levantar el secreto de las comunicaciones— que puede ser excepcionada bajo determinadas circunstancias. Y su contenido, como derecho reaccional que es, se agota «en la reacción individual frente a la desobediencia de aquella prohibición» o, en su caso, en la reclamación del cumplimiento de las condiciones constitucionales previstas para excepcionarla⁷⁸.

Por tanto, la existencia de la resolución judicial previa que autorice la intervención y el cumplimiento de determinados requisitos para entenderla constitucionalmente conforme —sobre los que volveremos— «no supone negación del contenido del derecho, sino realización del mismo para la inmisión en el objeto de este modo defendido»⁷⁹.

⁷⁸ VILLAVERDE MENÉNDEZ, I., «Concepto, contenido, objeto y límites...», *op.cit.*, pág. 337 y BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 111.

⁷⁹ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 56.

V. TITULARIDAD

El artículo 18.3 CE se expresa en los términos más amplios posibles en cuanto a la titularidad del derecho que proclama.

Debe entenderse así que, mediante el uso de la fórmula impersonal «se garantiza», el derecho se extiende a todos, incluyendo extranjeros y personas jurídicas.

Para el caso de los extranjeros, como es sabido, la Constitución declara su titularidad respecto de los derechos fundamentales «en los términos que establezcan los tratados y la ley» (art. 13.1 CE).

El secreto de las comunicaciones debe entenderse incluido en el grupo de derechos que, dentro de la clasificación tripartita construida por el Tribunal Constitucional, no permiten tener en cuenta el criterio de la nacionalidad para su desarrollo legal⁸⁰, por tratarse de un derecho imprescindible «para la garantía de la dignidad humana»⁸¹.

Por su parte, la Constitución española guarda silencio respecto de la posibilidad de que las personas jurídicas sean, de forma general, titulares de derechos fundamentales, aunque tampoco lo impide expresamente.

Más allá del reconocimiento explícito de determinados derechos⁸², se ha considerado a los arts. 9.2 y 162.1.b) CE como «claros indicios de que en la norma fundamental las personas jurídicas (o, más genéricamente, los grupos)

⁸⁰ Sobre esa clasificación de los derechos de los extranjeros, *vid. v.gr.* CRUZ VILLALÓN, P., «Dos cuestiones de titularidad de derechos: los extranjeros, las personas jurídicas», *Revista Española de Derecho Constitucional*, 35, 1992, págs. 63-83.

⁸¹ STC 107/1984, de 23 de noviembre (FJ. 3). También en esta dirección JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 53.

⁸² «La Constitución, además, contiene un reconocimiento expreso y específico de derechos fundamentales para determinados tipos de organizaciones. Así, por ejemplo, la libertad de educación está reconocida a los centros docentes (art. 27 C.E.), el derecho a fundar confederaciones está reconocido a los sindicatos (art. 28.1 C.E.), la libertad religiosa se garantiza a las asociaciones de este carácter (art. 16 C.E.) o las asociaciones tienen reconocido el derecho de su propia existencia (art. 22.4 C.E.)». STC 139/1995, de 26 de septiembre (FJ. 4).

pueden ser titulares de derechos»⁸³. El primero de ellos, por cuanto equipara al «individuo» y a los «grupos» respecto de las condiciones de disfrute de su libertad e igualdad. El segundo, en tanto reconoce a la persona jurídica legitimación activa para interponer recurso de amparo cuando «invoque un interés legítimo»⁸⁴.

En cualquier caso, respecto de las personas jurídicas privadas, el Tribunal Constitucional ha entendido que pueden ser titulares de derechos fundamentales «siempre que se trate, como es obvio, de derechos que, por su naturaleza, puedan ser ejercitados por este tipo de personas»⁸⁵.

El Tribunal Constitucional no se ha pronunciado sobre la posible titularidad de personas jurídicas en el caso del derecho fundamental al secreto de las comunicaciones, pero sí con ocasión de otro derecho en cierto modo cercano como la inviolabilidad del domicilio.

Respecto al art. 18.2 CE, la titularidad de las personas jurídicas se ha entendido en sentido afirmativo desde la STC 137/1985, de 17 de octubre (FJ. 3), al considerar que tal derecho «posee una naturaleza que en modo alguno repugna la posibilidad de aplicación a estas últimas»; pero con un alcance más reducido «por faltar esa estrecha vinculación con un ámbito de intimidad en su sentido originario; esto es, el referido a la vida personal y familiar, sólo predicable de las personas físicas»⁸⁶.

⁸³ GÓMEZ MONTORO, A.J., «La titularidad de derechos fundamentales por personas jurídicas (análisis de la jurisprudencia del Tribunal Constitucional español)», *Cuestiones constitucionales*, 2, 2000, pág. 28.

⁸⁴ Aunque se trate de una norma que atribuye legitimación procesal y no titularidad de derechos, sí que se ha entendido como «un principio de “apertura” de los derechos fundamentales hacia las personas jurídicas». CRUZ VILLALÓN, P., «Dos cuestiones de titularidad de derechos...», *op.cit.*, pág. 73.

⁸⁵ SSTC 64/1988, de 12 de abril (FJ. 1), y 23/1989, de 2 de febrero (FJ. 2). Por ello se ha afirmado que «el Tribunal Constitucional español ha venido a introducir por vía jurisprudencial el contenido del artículo 19.3 de la Ley Fundamental de Bonn», el cual reza: «Los derechos fundamentales son extensivos a las personas jurídicas con sede en el país, en la medida en que por su respectiva naturaleza les sean aplicables». CRUZ VILLALÓN, P., «Dos cuestiones de titularidad de derechos...», *op.cit.*, pág. 74.

⁸⁶ STC 69/1999, de 26 de abril (FJ. 2).

La relación entre los derechos a la inviolabilidad del domicilio y a la intimidad —que no asiste a las personas jurídicas⁸⁷— ha servido de argumento a MATIA PORTILLA para criticar la jurisprudencia constitucional expuesta y afirmar que las personas jurídicas tampoco son titulares del aquél⁸⁸.

Una postura similar respecto de la vinculación entre la intimidad y los derechos de los arts. 18.2 y 3 CE es la mantenida por RODRÍGUEZ RUIZ, pero el abordaje argumental y la conclusión alcanzada son diferentes. Para esta autora, conjuga mal el hecho de que el Tribunal Constitucional reconozca que la inviolabilidad del domicilio es un aspecto de la intimidad y, sin embargo, atribuya a las personas jurídicas la titularidad del derecho a aquélla, pero no a ésta⁸⁹. El problema se halla, según el trabajo que citamos, en la interpretación restrictiva del derecho a la intimidad que ha realizado el Tribunal Constitucional, pues, de interpretarlo como el control de las zonas de retiro y secreto, nada impediría entender que las personas jurídicas son titulares del derecho a la intimidad en estos términos entendido. Y, en el mismo sentido, no habría problemas para entender su titularidad respecto del derecho al secreto de las comunicaciones⁹⁰.

Menos obstáculos se plantean para atribuir tal titularidad si se considera, como hemos defendido ya en estas páginas, el secreto de las comunicaciones como derecho plenamente autónomo. Si el secreto del artículo 18.3 es de carácter formal y se garantiza, por tanto, con independencia del contenido de

⁸⁷ «El derecho a la intimidad que reconoce el art. 18.1 de la CE por su propio contenido y naturaleza, se refiere a la vida privada de las personas individuales, en la que nadie puede inmiscuirse sin estar debidamente autorizado, y sin que en principio las personas jurídicas, como las Sociedades mercantiles, puedan ser titulares del mismo, ya que la reserva acerca de las actividades de estas Entidades, quedarán, en su caso, protegidas por la correspondiente regulación legal, al margen de la intimidad personal y subjetiva constitucionalmente decretada». ATC 257/1985, de 17 de abril (FJ. 2).

⁸⁸ «[...] la inviolabilidad del domicilio protege la intimidad. Y [...] la persona jurídica carece de la misma, por lo que parece un contrasentido atribuirle la inviolabilidad del domicilio (como, al igual, sería absurdo reconocerles un derecho a la vida o a la integridad física)». *Vid.* MATIA PORTILLA, F.J., *El derecho fundamental a la inviolabilidad del domicilio*, McGraw-Hill, Madrid, 1997, págs. 113 y ss.

⁸⁹ STC 22/1984, de 17 de febrero (FJ. 2).

⁹⁰ RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, págs. 164 y ss.

la comunicación, difícilmente pueden hallarse diferencias en la necesidad de proteger ese secreto: trátase de una persona física o jurídica⁹¹.

La titularidad de derechos fundamentales por parte de personas jurídico-públicas presenta mayores dificultades, pues la propia concepción originaria de los derechos fundamentales como derechos públicos subjetivos, se presta a que sean entendidos como espacios de inmunidad de los particulares frente al poder público.

Por ello el Tribunal parte de afirmar que «en línea de principio, los derechos fundamentales y las libertades públicas son derechos individuales que tienen al individuo por sujeto activo y al Estado por sujeto pasivo en la medida en que tienden a reconocer y proteger ámbitos de libertades o prestaciones que los Poderes Públicos deben otorgar o facilitar a aquéllos»⁹².

No obstante, se ha reconocido expresamente la titularidad del derecho fundamental a la tutela judicial efectiva⁹³ y, en relación con él, el derecho a la igualdad en aplicación de la ley⁹⁴.

⁹¹ Para JIMÉNEZ CAMPO «no protege tanto la Constitución un derecho sobre la propia identidad personal, en sentido amplio, cuanto un derecho a disponer libremente de los espacios y procesos en que ésta se despliega, ámbitos no menos relevantes para la persona jurídica que para la física». Cfr. JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 54. También han defendido esta titularidad con base en el carácter formal del derecho ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, *op.cit.*, pág. 19 y NEIRA PENA, A.M., «La interceptación de las comunicaciones de la persona jurídica investigada», *Justicia: revista de derecho procesal*, 2, 2016, págs. 423 y ss.

⁹² STC 64/1988, de 12 de abril (FJ. 1).

⁹³ «Por lo que se refiere al derecho establecido en el art. 24.1 de la Constitución, como derecho a la prestación de actividad jurisdiccional de los órganos del Poder Judicial del Estado, ha de considerarse que tal derecho corresponde a las personas físicas y a las personas jurídicas, y entre estas últimas, tanto a las de Derecho privado como a las de Derecho público, en la medida en que la prestación de la tutela efectiva de los Jueces y Tribunales tiene por objeto los derechos e intereses legítimos que les corresponden». STC 64/1988, de 12 de abril (FJ. 1).

⁹⁴ «[...] no cabe negar la íntima conexión existente entre esa igualdad en la aplicación judicial de la Ley y el derecho a la tutela judicial efectiva, que también se lesiona por tratamientos jurídicos arbitrariamente desiguales. Un rasgo esencial del Estado de Derecho es el sometimiento de los poderes públicos a la jurisdicción, frente a la cual la situación de los poderes públicos no es radicalmente diferente a la de los particulares, también en lo que se refiere al derecho a no someterse a un trato desigualmente arbitrario por parte de los Jueces y Tribunales». STC 100/1993, de 22 de marzo (FJ. 2).

Es más, la STC 64/1988, de 12 de abril, que venimos citando, resulta especialmente significativa, por cuanto parece admitir incluso la posible titularidad de las personas jurídico-públicas de otros derechos fundamentales distintos a los aquí tratados.

Y es que, tras recordar su doctrina respecto a la titularidad de las personas jurídico-privadas —sobre aquellos derechos que, por su naturaleza, puedan ser ejercitados por ellas— señala que «[a] la misma conclusión puede llegarse en lo que concierne a las personas jurídicas de Derecho público, siempre que recaben para sí mismas ámbitos de libertad, de los que deben disfrutar sus miembros, o la generalidad de los ciudadanos, como puede ocurrir singularmente respecto de los derechos reconocidos en el art. 20 cuando los ejercitan corporaciones de Derecho público».

Esta afirmación, de difícil interpretación, ha sido entendida como una equiparación entre las personas jurídico-públicas y la posición en que, respecto de la titularidad de ciertos derechos fundamentales, el Tribunal había colocado a ciertos grupos sociales⁹⁵.

El Tribunal sostiene, en la misma resolución, que «la plena efectividad de los derechos fundamentales exige reconocer que la titularidad de los mismos no corresponde sólo a los individuos aisladamente considerados, sino también en cuanto se encuentran insertos en grupos y organizaciones, cuya finalidad sea específicamente la de defender determinados ámbitos de libertad o realizar los intereses y los valores que forman el sustrato último del derecho fundamental»⁹⁶.

⁹⁵ CRUZ VILLALÓN, P., «Dos cuestiones de titularidad de derechos...», *op.cit.*, pág. 81. En la misma dirección: RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. 169.

⁹⁶ Así, las «comunidades» en el caso de la libertad ideológica (16.1 CE), el derecho a participar en asuntos públicos a través de partidos políticos (23), el ejercicio del derecho de asociación por Asociaciones ya constituidas (22 CE) o el derecho de libertad sindical por los propios Sindicatos (28 CE). *Vid.* STC 64/1988, de 12 de abril (FJ. 1).

Y, en efecto, de esta cualidad de sujeto colectivo representativo de un derecho singular parece hacer depender el Tribunal la posibilidad de que las personas jurídicas de derecho público detenten la titularidad de derechos fundamentales. Este parece ser el sentido de la declaración del Tribunal — «que recaben para sí mismas ámbitos de libertad, de los que deben disfrutar sus miembros, o la generalidad de los ciudadanos»— y así se entiende el ejemplo que la acompaña —«como puede ocurrir singularmente respecto de los derechos reconocidos en el art. 20 cuando los ejercitan corporaciones de Derecho público»—, que parece referirse a *los medios de comunicación social dependientes del Estado*⁹⁷.

Trasladando este razonamiento al derecho fundamental aquí considerado, se ha negado con carácter general su titularidad por las personas jurídico-públicas, «con la salvedad quizás de aquellas cuyo objeto sea precisamente organizar un servicio de telecomunicaciones, garantizando su secreto como parte de él»⁹⁸.

Otros autores, no obstante, han apostado por ampliar la titularidad de las personas jurídicas públicas en los mismos términos en que el Tribunal lo ha hecho con las privadas, esto es, en función de que la naturaleza del derecho posibilite por aquellas su ejercicio, por lo que también se verían beneficiadas del secreto de las comunicaciones⁹⁹.

⁹⁷ CRUZ VILLALÓN, P., «Dos cuestiones de titularidad de derechos...», *op.cit.*, pág. 81. El mismo criterio serviría para otorgar la titularidad a las Universidades, como ente público al que se ha confiado «en especial la realización de un derecho fundamental», del derecho fundamental a la libertad de cátedra. *Vid.* DÍAZ LEMA, J.M., «¿Tienen derechos fundamentales las personas jurídico-públicas?», *Revista de Administración Pública*, 120, 1989, pág. 125.

⁹⁸ RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. 169. También FERNÁNDEZ RODRÍGUEZ, J. J., *Secreto e intervención de las comunicaciones...*, *op.cit.*, pág. 93.

⁹⁹ LASAGABASTER, I., «Derechos fundamentales y personas jurídicas de derecho público», AA.VV., *Estudios sobre la Constitución Española. Homenaje al profesor Eduardo García de Enterría*, Vol. 2, Civitas, Madrid, 1991, pág. 673. También es esta, desde un entendimiento participativo de los derechos fundamentales, la posición defendida por ALÁEZ CORRAL, para quien «el mismo argumento que utiliza el Tribunal para reconocerles ocasionalmente ciertos derechos de corte procesal debiera servir [...] para fundamentar la titularidad general por parte de las personas jurídico-públicas de aquellos derechos que por su naturaleza puedan

Finalmente, también son titulares de este derecho los menores de edad. A pesar de que la Constitución no se pronuncia sobre este extremo¹⁰⁰, es pacífico entre la doctrina que la titularidad viene determinada por la personalidad y, por tanto, los menores son, desde su nacimiento, titulares de todos los derechos fundamentales¹⁰¹.

Esta titularidad, además de ser reconocida por textos internacionales y por la jurisprudencia constitucional¹⁰², ha sido plasmada en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, cuyo art. 3 dispone que «[l]os menores gozarán de los derechos que les reconoce la Constitución y los Tratados Internacionales de los que España sea parte...».

Los preceptos sucesivos de esta norma desarrollan algunos derechos fundamentales, entre los que se incluye, con una redacción algo confusa, el derecho que aquí estudiamos¹⁰³. Y es que el artículo 4.1 señala: «Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones».

Además de diferenciar —en principio sin consecuencias— entre la inviolabilidad de la correspondencia y el secreto de las comunicaciones, el legislador orgánico parece inclinarse también aquí por una cierta relación de

ejercer». Cfr. BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 90.

¹⁰⁰ Sí existe una referencia a los derechos de los menores, pero en sede de principios rectores. Así, dispone el art. 39.4 CE: «Los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos».

¹⁰¹ No obstante, algunos autores han entendido que el menor carece de la titularidad de algunos derechos (sufragio o libertad sindical desde los 16 años). Para otros, sin embargo, dicha delimitación temporal incide en el ejercicio del derecho fundamental, pero no en su titularidad. *Vid.* PASCUAL MEDRANO, A., «Los derechos fundamentales y la Ley de Protección del Menor», *Revista jurídica de Navarra*, 22, 1996, págs. 249-264 y ALÁEZ CORRAL, B., *Minoría de edad y derechos fundamentales*, Tecnos, Madrid, 2003, pág. 101.

¹⁰² SSTC 36/1991, de 14 de febrero (FJ. 6), y 141/2000, de 29 de mayo (FJ. 5).

¹⁰³ La norma recoge una selección no exhaustiva de los derechos fundamentales del menor, tal vez determinada, se ha dicho, por los casos «en los que la minoría de edad puede provocar más matices en orden a su ejercicio, dando por supuestos algunos otros: vida, integridad, seguridad... establecidos por la Constitución y por la Convención sobre Derechos del Niño». PASCUAL MEDRANO, A., «Los derechos fundamentales y la Ley...», *op.cit.*, pág. 254.

vinculación entre los derechos del artículo 18 CE, ya que expresamente dispone que uno de los derechos enunciados en primer término —entendemos que el derecho a la intimidad— *comprende* la inviolabilidad del domicilio y el secreto de las comunicaciones.

En todo caso, los problemas que este derecho pueda suscitar respecto a la minoría de edad no vendrán determinadas por su titularidad, sino, en su caso, por su ejercicio. Y ello en un doble sentido. Por un lado, porque, si lo que se protege son las comunicaciones a través de medio técnico, el menor deberá poder tener acceso a ese medio y alcanzar progresivamente la capacidad de comunicarse¹⁰⁴. Por otro, por la incidencia —variable— que la especial relación paternofilial tiene sobre su ejercicio durante la minoría de edad.

¹⁰⁴ ALÁEZ CORRAL, B., *Minoría de edad...*, *op.cit.*, pág. 99.

VI. SUSPENSIÓN DEL DERECHO

La Constitución española prevé dos situaciones en que determinados derechos fundamentales pueden ser suspendidos: la denominada suspensión general, que puede ser activada en los casos de excepcionalidad constitucional (art. 55.1 CE, en conexión con el art. 116 CE) y la facultad de suspensión individual en la investigación del terrorismo (55.2 CE).

Ambos casos afectan al contenido del derecho, es decir, a las facultades jurídicas que su titular posee para defender el objeto garantizado. Se va a producir, por tanto, una *modificación* del contenido *normal* del derecho por aquel constitucionalmente previsto para los casos en que se decrete la suspensión y con las condiciones en que hubiere sido legislativamente desarrollado¹⁰⁵.

VI.1. Suspensión general (55.1 CE)

El art. 55.1 CE prevé la posibilidad de suspender ciertos derechos fundamentales en casos de excepcionalidad constitucional, declaración que se producirá «cuando circunstancias extraordinarias hiciesen imposible el mantenimiento de la normalidad mediante los poderes ordinarios de las Autoridades competentes»¹⁰⁶.

En cualquier caso, esta suspensión es solo posible en los estados de excepción y de sitio, pero no en el de alarma.

La adjetivación de *general* se atribuye en función de los destinatarios de esta suspensión, ya que afectará a todos los que se encuentren en el territorio

¹⁰⁵ Las garantías del derecho se ven aminoradas, pero su titular podrá exigir que la injerencia se lleve a cabo en los términos establecidos para tal situación excepcional. REQUEJO RODRÍGUEZ, P., «¿Suspensión o supresión de los derechos fundamentales?», *Revista de Derecho Político*, 51, 2001, pág. 111.

¹⁰⁶ Artículo 1.1 de la Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio. Sobre el régimen jurídico de esta suspensión, puede verse FERNÁNDEZ SEGADO, F., «Naturaleza y régimen legal de la suspensión general de los derechos fundamentales», *Revista de derecho político*, 18-19, 1983, págs. 31-58.

determinado por la declaración del estado excepcional¹⁰⁷. Pero no es general en cuanto a los derechos sobre los que puede recaer, que son únicamente aquéllos que expresamente se determinan en el art. 55.1 CE y entre los que se encuentra el derecho fundamental al secreto de las comunicaciones¹⁰⁸.

Tampoco es general desde el punto de vista de sus fines, ya que dicha suspensión deberá orientarse exclusivamente, según dispone el art. 1.2 LOEAES, a «asegurar el restablecimiento de la normalidad».

En el caso del derecho fundamental del art. 18.3 CE, el legislador orgánico, pese al amplio margen de actuación del que dispone en este caso, ha optado por un desarrollo no excesivamente gravoso en cuanto a la merma de sus garantías respecto al régimen ordinario¹⁰⁹.

Se atribuye la posibilidad de intervenir las comunicaciones directamente a la autoridad gubernativa, pero no desaparece la presencia del juez, a quien deberá ser comunicada, «inmediatamente», tal intervención.

Este podrá, en caso de no haberse observado los requisitos legislativamente establecidos, ordenar el cese de la intervención. Y es que, como dijimos, la suspensión recae sobre el «contenido típico» del derecho, pero la intervención permanece sujeta a determinadas condiciones¹¹⁰.

Así, este régimen excepcional será de aplicación únicamente para aquellas intervenciones necesarias «para el esclarecimiento de los hechos

¹⁰⁷ REQUEJO RODRÍGUEZ, P., «¿Suspensión o supresión...?», *op.cit.*, pág. 114.

¹⁰⁸ En cualquier caso, «la suspensión no es automática, pues la declaración del Gobierno o del Congreso de los Diputados de suspender el secreto de las comunicaciones se somete a controles legales, guiada por las exigencias de necesidad de suspensión, y de prohibición de derogación de tal derecho fundamental». ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 249.

¹⁰⁹ Art. 18.1 LOEAES: «1. Cuando la autorización del Congreso comprenda la suspensión del artículo 18.3 de la Constitución, la autoridad gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y telefónicas. Dicha intervención sólo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público. 2. La intervención decretada será comunicada inmediatamente por escrito motivado al Juez competente».

¹¹⁰ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 77.

presuntamente delictivos o el mantenimiento del orden público» y siempre que con ello se persiga el «restablecimiento de la normalidad»¹¹¹.

Por tanto, deberá entenderse que se ha vulnerado el derecho al secreto de las comunicaciones cuando la intervención se realice sin autorización judicial y con una finalidad diferente a la señalada.

VI.2. Suspensión individual (55.2 CE)

Por su parte, el art. 55.2 permite también la suspensión de ciertos derechos fundamentales, pero con carácter individual, respecto de aquellas personas relacionadas con la «actuación de bandas armadas o elementos terroristas».

Se trata en todo caso de un potencial encargo al legislador —*una ley orgánica podrá...*—, que fue tempranamente asumido. Primero, mediante el desarrollo de tal posibilidad en concretas leyes antiterroristas¹¹² y, desde la Ley Orgánica 4/1988, de 25 de mayo, a través de su previsión en la Ley de Enjuiciamiento Criminal¹¹³.

No obstante, es un encargo condicionado, ya que constitucionalmente se imponen las garantías de «la necesaria intervención judicial y el adecuado control parlamentario».

¹¹¹ También se ha dicho que, desde el punto de vista subjetivo, la suspensión solo podrá tener como destinatarios a los sujetos «vinculados con los hechos que originaron la crisis o que puedan contribuir de algún modo a superarla». REQUEJO RODRÍGUEZ, P., «¿Suspensión o supresión...?», *op.cit.*, pág. 116.

¹¹² Ley Orgánica 11/1980, de 1 de diciembre, sobre los supuestos previstos en el artículo 55.2 de la Constitución y Ley Orgánica 9/1984, de 26 de diciembre, contra la actuación de bandas armadas y elementos terroristas y de desarrollo del artículo 55.2 de la Constitución.

¹¹³ La regulación se mantiene hoy en la Ley de Enjuiciamiento Criminal, si bien con las modificaciones —mínimas— introducidas por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Sobre el debate doctrinal acerca de la pertinencia de que la ley de desarrollo sea transitoria o permanente, *vid.* VÍRGALA FORURIA, E., «La suspensión de derechos por terrorismo en el ordenamiento español», *Revista Española de Derecho Constitucional*, 40, 1994, págs. 61-132.

Respecto del derecho al secreto de las comunicaciones resultan evidentes los problemas interpretativos que se derivan de la exigencia de intervención judicial. Pues si, como dijimos, el contenido del 18.3 CE consiste precisamente en la reclamación de la garantía de intervención judicial, la prevista en el art. 55.2 deberá entenderse, para no vaciar este artículo de contenido, en términos diversos al régimen iusfundamental ordinario.

La solución legislativa ha pasado por variar el momento en que tal intervención judicial se produce: mientras que en la normal intervención de las comunicaciones la autorización del juez debe ser siempre previa a su práctica, en este excepcional régimen de suspensión la intervención se produce *a posteriori*, permitiendo que sea ordenada preliminarmente por el ejecutivo¹¹⁴.

El Tribunal Constitucional ha entendido constitucionalmente conforme esta solución, pues la regla general de autorización judicial previa no excluye que «en ciertos casos la efectividad de la suspensión misma requiera una actuación inmediata de la autoridad gubernativa, sin perjuicio de la intervención sucesiva del órgano judicial»¹¹⁵.

De esta forma, la suspensión del derecho al secreto de las comunicaciones en el caso del 55.2 CE se convierte más bien en un aplazamiento de su contenido.

¹¹⁴ No es está, sin embargo, la única interpretación posible. Para JIMÉNEZ CAMPO la *ratio* del 55.2 CE, su especialidad frente al régimen común del 18.3, no se halla en la posibilidad de posponer la intervención judicial —que debe ser siempre previa—, sino que consiste en la posibilidad de ampliar los sujetos cuyas comunicaciones pueden ser intervenidas, recayendo, no solo en quien esté siendo investigado en un proceso penal, «sino también, con fines exploratorios o preventivos, sobre aquellos que, sin tener dicha condición, se estiman relacionados con el área específica de criminalidad que se contempla en la norma constitucional». JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, págs. 81-82.

¹¹⁵ «[...] esta modalización de la necesaria intervención judicial para hacer posible la suspensión entra en la lógica misma de la previsión incluida en el art. 55.2 de la Constitución. Si la intervención judicial en estos casos fuera idéntica a todos los efectos a la existente en el régimen común de los derechos de los arts. 17.2 y 18.2 y 3 de la Constitución, no cabría hablar, como la Constitución hace, de suspensión de tales derechos». STC 199/1987, de 16 de diciembre (FJ. 7).

Sin embargo, tal modo de actuación no es posible en todos los casos. Además de circunscribirse a una determinada modalidad delictiva (terrorismo), la excepcionalidad que supone el aplazamiento referido debe responder, para entenderse constitucionalmente justificado, a algo más.

Así, el desarrollo legislativo del art. 55.2 CE ha limitado esta posibilidad únicamente a supuestos de urgencia, es decir, a situaciones en que no sea posible, para que no se vea frustrada la investigación, esperar a obtener la autorización judicial para poner en práctica la intervención comunicativa¹¹⁶.

En la actualidad la regulación se encuentra en dos artículos de la Ley de Enjuiciamiento Criminal (579.3 y 588 ter.d), ya que, desde la modificación llevada a cabo en 2015, se regulan separadamente la *detención y apertura de la correspondencia escrita y telegráfica* y la *intervención de las comunicaciones telefónicas y telemáticas*.

Pero ambos preceptos se expresan en idénticos términos:

«En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida».

¹¹⁶ Las sucesivas regulaciones han mantenido una redacción muy similar. *Vid.* art. 5.2 LO 11/1980, art. 17.2 LO 9/1984 y art. 579.4 LECrim en la redacción dada por la LO 4/1988.

Se ha entendido que la orden de intervención del ejecutivo puede ser verbal pues, de exigirse una orden escrita «podría utilizarse ese tiempo en conseguir una resolución judicial»¹¹⁷.

En todo caso, la comunicación de la intervención al juez debe ser motivada, debiendo explicitar en ella las razones de urgencia que justificaron la ordenación gubernativa de la medida¹¹⁸.

El juez, por su parte, deberá revocar o confirmar la injerencia en el plazo improrrogable de setenta y dos horas desde su puesta en marcha, recuperando así su papel de garante de los derechos fundamentales en el proceso penal.

¹¹⁷ VÍRGALA FORURIA, E., «La suspensión de derechos...», *op.cit.*, pág. 116. En todo caso, podría haberse mantenido la presencia inicial del juez, aunque se pospusiera la motivación de la autorización de intervención, ya que, como mantiene REQUEJO RODRÍGUEZ, «igual que se dispone de tiempo suficiente para recabar la orden de la autoridad administrativa, también se podría haber acudido al juez para que, al menos, diera una autorización verbal que luego habría de motivar». Además, añadimos, esa atribución al poder ejecutivo no parece poder justificarse en una mayor disponibilidad respecto de la que tiene el judicial con el actual esquema de los servicios de guardia. REQUEJO RODRÍGUEZ, P., «¿Suspensión o supresión...?», *op.cit.*, pág. 125.

¹¹⁸ STC 199/1987, de 16 de diciembre (FJ. 10).

CAPÍTULO SEGUNDO

LA COMUNICACIÓN PROTEGIDA EN EL ART. 18.3 CE

I. CONCEPTO CONSTITUCIONAL DE COMUNICACIÓN

- I.1. Una comunicación consiste en una transmisión de expresiones de sentido
- I.2. Entre personas *previamente* determinadas. Difusión pública y comunicación privada
 - A. Predeterminación de destinatarios frente a audiencias potencialmente ilimitadas
 - B. Interactividad *versus* pasividad: la conmutabilidad de roles en la relación comunicativa
 - C. La singularidad del destinatario en las comunicaciones privadas
- I.3. Comunicación técnicamente mediada y a través de canal cerrado
 - A. Soporte e intermediación técnica: comunicación *versus* conversación directa
 - B. Características del medio. Las denominadas «comunicaciones abiertas»

II. ÁMBITO TEMPORAL DEL DERECHO: INTERVENCIÓN Y ACCESO

- II.1. Inicio del proceso comunicativo
- II.2. Finalización del proceso comunicativo
 - A. La protección del sistema comunicativo
 - B. La protección de la comunicación hasta el conocimiento del contenido por el destinatario
 - C. La estricta limitación de la protección a la comunicación en tránsito y la participación del tercero

III. MODALIDADES COMUNICATIVAS PROTEGIDAS

- III.1. Comunicaciones postales y telegráficas
- III.2. Comunicaciones bidireccionales simultáneas
- III.3. Comunicaciones telemáticas alternativas

I. CONCEPTO CONSTITUCIONAL DE COMUNICACIÓN

La correcta delimitación del objeto del derecho fundamental consagrado en el artículo 18.3 CE requiere determinar el significado que posee el concepto de comunicación en dicho precepto.

Para esta tarea, sin embargo, no contamos con una definición constitucionalmente expresa, aunque de su enunciado quepa inferir un contenido normativo que ayuda a precisar el concepto.

En primer lugar, la norma garantiza el secreto de las comunicaciones, por lo que el término genérico «comunicación» registrado en el texto alude tan sólo a aquéllas determinadas por el calificativo de «secreto» que le delimita. De tal modo que el objeto del derecho queda ajustado a aquellas comunicaciones cuyo secreto es susceptible de ser garantizado¹.

En segundo lugar, el art. 18.3 CE señala expresamente, recuérdese que en enunciado abierto, un elenco de modalidades de comunicación — «postales, telegráficas y telefónicas»— unidas por unas características comunes que, además de agruparlas, las distinguen del resto de procesos comunicativos. Por tanto, estas últimas formarán parte del objeto protegido sólo si satisfacen las características constitucionalmente descritas².

¹ ITALIA, V., *Libertà e segretezza della corrispondenza e delle comunicazioni*, Giuffrè, Milán, 1963, pág. 29.

² Este es el sentido de la STC 281/2006, de 9 de octubre (FJ. 3), cuando afirma que «[...] ha de tenerse en cuenta que el término “comunicaciones” al que se refiere el art. 18.3 CE, sirve para denotar el objeto de protección de este derecho constitucional sea cual sea el medio a través del cual la comunicación tiene lugar —postal, telegráfico, telefónico...—; de modo que la noción constitucional de comunicación ha de incorporar los elementos o características comunes a toda clase de comunicación».

El legislador orgánico no ha desarrollado el objeto del derecho en su dimensión sustantiva, privando a los operadores jurídicos de criterios identificadores complementarios de una definición del concepto de comunicación. Ello comporta cierto déficit de certeza y seguridad jurídica en el manejo de un derecho fundamental que, como el que nos ocupa, posee una importancia exponencial en la actualidad.

El legislador se ha dedicado exclusivamente a establecer los requisitos para la limitación del derecho, señalando las condiciones de legitimidad de la injerencia estatal para enervar su secreto en el marco de una investigación penal³.

Nos hallamos en este sentido ante un derecho que se ha calificado de «construcción pretoriana», ya que ha sido el Tribunal Constitucional el que, a través de sus pronunciamientos, ha ido perfilando los contornos del concepto de comunicación protegida⁴.

Al análisis de tales criterios, dispersos en la jurisprudencia y no siempre precisados de modo satisfactorio, dedicaremos los sucesivos apartados.

I.1. Una comunicación consiste en una transmisión de expresiones de sentido

Un proceso comunicativo no incluye cualquier objeto transmitido entre emisor y receptor: la comunicación constitucionalmente relevante requiere transmisión entre personas que contenga una expresión de sentido.

³ Además, solo recientemente se han colmado las ausencias que contenía la ley procesal, tras las continuas advertencias de la jurisprudencia constitucional que, no obstante, pudo frenar con su doctrina las diversas condenas del TEDH por falta de calidad de la ley. OCÓN GARCÍA, J., «La incidencia de las resoluciones del TEDH en la configuración del derecho fundamental al secreto de las comunicaciones», AA.VV., *Diálogos judiciales en el sistema europeo de protección de derechos: una mirada interdisciplinar*, Tirant Lo Blanch, Valencia, 2018, págs. 259-272.

⁴ RIDAURA MARTÍNEZ, M.J., «El legislador ausente del artículo 18.3...», *op.cit.*, pág. 350.

Este requisito, de tardía aparición en la jurisprudencia del Tribunal Constitucional —STC 281/2006, de 9 de octubre—, pero tempranamente señalado por la doctrina⁵, se ha utilizado para excluir de la garantía de secreto el envío de paquetes postales. Criterio que, por lo demás, ha sufrido una revolucionaria novación, ante la emergencia de procesos comunicativos tecnológicamente novedosos —como el intercambio de archivos en redes P2P o los procesos comunicativos entre *máquinas*—.

Así, residenciado por el Tribunal Constitucional el fundamento primario del derecho al secreto de las comunicaciones en la dignidad de la persona y el libre desarrollo de la personalidad, considera que las comunicaciones protegidas no pueden ser sino aquellas «indisolublemente unidas por naturaleza a la persona, a la propia condición humana; por tanto, la comunicación será el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos»⁶.

Esta afirmación requiere sin embargo un matiz de considerable importancia. Hacer depender la protección de una determinada comunicación de las cualidades del contenido que albergue conllevará que se produzca, en todos los casos, aquello que precisamente la norma trata de evitar: un debilitamiento o incluso desactivación del secreto para asegurar que debió ser

⁵ «La comunicación, como segunda consideración, es un proceso de transmisión de mensajes, un proceso en cuyo curso se hacen llegar a otro expresiones del propio pensamiento articuladas en signos no meramente convencionales. No estaremos, así, ante una comunicación, en el sentido constitucional del concepto, cuando lo transmitido no sean contenidos intelectuales expresados, directa o indirectamente, a través del lenguaje», *vid.* JIMÉNEZ CAMPO, J.; «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 46.

⁶ STC 281/2006, de 9 de octubre (FJ. 3). La vinculación que el Tribunal realiza aquí entre dignidad humana y derecho fundamental cumple sólo un papel de refuerzo interpretativo, sin que de ello se deriven mayores consecuencias para la delimitación del derecho. Se trata de un modo de proceder ampliamente utilizado por el Tribunal Constitucional, recurriendo al principio de dignidad de la persona como refuerzo de interpretaciones o juicios que «el tribunal ya extrae o hubiera podido extraer de otras prescripciones constitucionales más precisas». En este caso, el propio concepto de comunicación sugiere ya una transmisión interpersonal de expresiones. *Vid.* PASCUAL MEDRANO, A., «La dignidad humana como principio jurídico del ordenamiento constitucional español», CHUECA RODRÍGUEZ, R. (Dir.), *Dignidad humana y derecho fundamental*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015, págs. 320 y ss.

garantizado. O, alternativamente, presumir que cualquier comunicado, incluso sin contenido material alguno, está protegido por el derecho.

Por tanto, para determinar si una comunicación queda o no amparada deberá estarse a verificar la satisfacción de unas condiciones específicas. Ello significa abrazar un concepto formal de comunicación, ajeno a cualquier comprobación de la existencia cierta de un contenido⁷.

Pero si el secreto posee, como sostenemos, carácter formal y, por tanto, protege la comunicación, con o sin contenido, no parece viable hacer depender el secreto de la existencia de un contenido comunicativo.

La comunicación protegida deberá ser, si queremos mantener la coherencia interna del derecho y su potencial garantista, no ya la transmisión de expresiones de sentido, sino aquella mantenida mediante formas comunicativas generalmente utilizadas, o susceptibles de soportar, la transmisión de expresiones de sentido⁸.

De modo que asegurar la indemnidad del derecho requiere inexcusablemente amparar como secretas aquellas formas de comunicación hábiles para compartir expresiones de sentido; más allá de que así lo sea en el caso concreto.

Tomaremos, como ejemplo obvio, el modo de comunicación postal, usualmente bajo formato de sobre cerrado. Deberá entenderse que el envío postal cerrado satisfará en todo caso los requisitos de comunicación protegida por el artículo 18.3 CE; lo que así será al margen de que contenga contenido comunicacional alguno⁹.

⁷ RIVERO SÁNCHEZ-COVISA, F.J., *Revisión del concepto constitucional del secreto de las comunicaciones*, Dykinson, Madrid, 2017, pág. 13.

⁸ Por todos, GIANFRANCESCO, E., «Profili ricostruttivi della libertà e segretezza di corrispondenza e comunicazione», *Diritto e società*, 2, 2008, pág. 233.

⁹ Cfr. CARUSO, C., «La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale», *Forum di Quaderni Costituzionali*, 10, 2013, pág. 6. En similar sentido, cfr. LUCAS MURILLO DE LA CUEVA, P., «Notas sobre el derecho fundamental al secreto de las

Contrariamente, no tendrán la consideración constitucional de comunicación aquellos medios cuya principal y general función no es transmitir pensamientos, como sucede en el envío de paquetes postales, aunque efectivamente alberguen esta clase de contenidos¹⁰. Ello, por lo demás, evidencia el alcance y limitaciones de la configuración formal del objeto de derecho.

Con el mismo fundamento se ha entendido que el artículo 18.3 CE protege únicamente «fenómenos de comunicación entre personas»¹¹. No tendrán la consideración de comunicación, por tanto, los intercambios automáticos de información entre dispositivos o terminales, como sucede entre los teléfonos móviles y los repetidores —estaciones BTS (*Base Transceiver Station*)—, las comunicaciones entre dispositivos a través de tecnología NFC (*near field communication*) —hoy ampliamente utilizada en el ámbito de los pagos electrónicos— o, en definitiva, las diversas relaciones que se producen en el denominado «internet de las cosas» (*IoT*)¹².

comunicaciones», AA.VV., *Constitución, Estado de las Autonomías y justicia constitucional (Libro homenaje al profesor Gumersindo Trujillo)*, Tirant Lo Blanch, Valencia, 2005, pág. 677.

¹⁰ «Desde esta perspectiva, no gozan de la protección constitucional aquellos objetos —continentes— que por sus propias características no son usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías (ATC 395/2003, de 11 de diciembre, FJ 3), de modo que la introducción en ellos de mensajes no modificará su régimen de protección constitucional». STC 281/2006, de 9 de octubre, FJ. 3. La misma argumentación, pero aplicada a la dimensión *online*, podría servir para excluir de la protección del 18.3 CE «la transmisión de mensajes personales por medio de archivos en carpetas compartidas de red o en servidores ftp, o subiendo el archivo que contenga el mensaje a un servicio de almacenamiento de archivos y, en general, todas las que se realicen mediante el empleo de cualquier otra herramienta informática o de red no concebida específicamente para la transmisión de mensajes». Cfr. VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», HERMIDA, C. y SANTOS, J.A. (coords.), *Una Filosofía del Derecho en acción. Homenaje al profesor Andrés Ollero*, Congreso de los Diputados, Madrid, 2015, pág. 1616.

¹¹ STC 170/2013, de 7 de octubre (FJ. 4).

¹² En estos casos, además de la ausencia del factor humano, tampoco se intercambian «expresiones de sentido» en los términos antes apuntados. Puede hallarse una explicación más precisa del funcionamiento de estas tecnologías en RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, págs. 37 y ss. También considera excluidos estos fenómenos de la protección del 18.3 CE la Circular de la Fiscalía General del Estado 2/2019, sobre interceptación de comunicaciones telefónicas y telemáticas, si bien reconoce que «existen comunicaciones entre máquinas que, puestas en relación con otros datos, sí pueden afectar a alguno de estos derechos, como el derecho a la intimidad»; *vid.* apdo. 2, pág. 4. Se

Consideramos, no obstante, que no será requisito indispensable la participación activa de la persona en todo el proceso comunicativo, siempre que medie una acción precisa para la generación de esa comunicación, sin la que no sería posible su activación¹³.

Así sucede con las llamadas telefónicas aunque el factor humano no esté presente en uno de los interlocutores, como en el caso de comunicaciones emitidas no replicadas, pero diferidas en la recepción del contenido comunicacional mutuamente aceptado, al activar ambos su registro en un buzón de voz; igualmente en las comunicaciones entabladas por asistentes virtuales o las que originan los automóviles dotados de un servicio de emergencias (*eCall*) en caso de siniestro¹⁴. La misma lógica ampara los correos electrónicos remitidos como consecuencia de la activación del sistema de respuestas automáticas por su titular.

I.2. Entre personas *previamente* determinadas. Difusión pública y comunicación privada

La comunicación protegida es aquella cuyo secreto sea susceptible de garantía.

Ello requiere de un proceso comunicativo entre sujetos determinados. La noción de comunicación presente en el artículo 18.3 CE precisa, por tanto, que la intención del emisor sea que la información discorra exclusivamente

ha discutido igualmente la inclusión de este tipo de procesos comunicativos en el ámbito de la Directiva sobre privacidad y comunicaciones electrónicas (Directiva 2002/58/CE); *vid.* STORMS, S., VALCKE, P. y KINDT, E., «Rage against the machine: does machine-to-machine communication fall within the scope of the confidentiality principle?», *International Journal of Law and Information Technology*, 27, 2019, págs. 372-408.

¹³ RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, pág. 28.

¹⁴ «[...] también en estos casos existe una comunicación entre personas, pues el contestador automático es simplemente otro soporte técnico de la comunicación interpersonal», *vid.* MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 53.

hasta la esfera de conocimiento del destinatario y con exclusión, por tanto, de terceros¹⁵.

El número de destinatarios debe estar, por tanto, determinado al tiempo del inicio del proceso comunicativo, pero pudiendo variar durante su curso cuando, por ejemplo, resultare fallida la comunicación respecto de alguno¹⁶. Emisor y receptor pueden ser —claro está— uno o varios, pero siempre previamente determinados.

Esto permite declarar protegidas aquellas formas comunicativas configuradas para la participación simultánea de varios interlocutores, como multiconferencias o grupos de intercambio de mensajería instantánea, modelo hoy generalizado, y hasta universalizado, en plataformas como *WhatsApp*, *Telegram* u otras.

Estos requisitos de intersubjetividad y determinación de los destinatarios, consustanciales a las tres modalidades comunicativas que expresamente se prevén en la norma constitucional, son útiles, además, para configurar un parámetro de inclusión de cualquier otra actividad comunicativa en el objeto del derecho.

Pero esos mismos requisitos servirán también para discriminarlo respecto del objeto de los derechos de libre expresión o información (art. 20.1. CE). Un criterio que establece en definitiva una línea de división entre comunicación privada y difusión pública.

¹⁵ La determinación lo es de intervinientes o destinatarios en la comunicación y no de personas. Piénsese, por ejemplo, en el correo electrónico enviado a dos cuentas de correo diferentes, pero cuyo titular es la misma persona. Del mismo modo, acertadamente se ha dicho que «resulta intrascendente que el emisor y el receptor sean la misma persona», lo que sucede en el caso de envío de un correo electrónico a la propia cuenta del emisor para, por ejemplo, guardar de esa forma un determinado archivo que se envía como adjunto. ZOCO ZABALA, C., «Intervención de las comunicaciones e intervención de las conversaciones: una misma protección *iusfundamental*», HERRERO GUTIÉRREZ, F.J. y MATEOS MARTÍN, C. (coords.), *Del verbo al bit*, Sociedad Latina de Comunicación Social, La Laguna, 2017, pág. 355.

¹⁶ RIVERO SÁNCHEZ-COVISA, F.J., *Revisión del concepto constitucional...*, *op.cit.*, pág. 16.

Esta escisión en el modelo de los soportes comunicativos tradicionales otorgaba un papel relevante a las características técnicas del medio y a su adecuación al fin perseguido: mantener el mensaje al margen del conocimiento ajeno (correspondencia, telégrafo o teléfono) o perseguir la divulgación informativa tratando de alcanzar la mayor audiencia posible (prensa, radio o televisión)¹⁷. De modo que la opción por un medio u otro orientaba la inclusión de la actividad comunicativa en uno u otro ámbito iusfundamental.

Sin embargo, y según sabemos, las transformaciones tecnológicas han propuesto un nuevo entorno comunicativo, al surgir nuevas plataformas de comunicación que han debilitado sensiblemente la frontera entre comunicación reservada y comunicación masiva¹⁸. Hoy ya no es posible —a ciencia cierta— ubicar una concreta actividad comunicativa en el espacio de uno de aquellos derechos recurriendo a la mera referencia al medio utilizado.

Y ello por varias razones.

De un lado, algunos medios de comunicación tecnológicamente novedosos permiten dirigir fácilmente comunicaciones de forma simultánea a un gran número de destinatarios. En este caso, aun estando previamente determinado el número ilimitado de destinatarios, parece necesario reconsiderar la contraposición —obviamente obsoleta— que oponía comunicación reservada a difusión masiva¹⁹.

Por otro, en determinadas plataformas de divulgación de contenidos se ha relativizado sustancialmente la nota de pasividad que caracterizaba hasta

¹⁷ COSTANZO, P., «Le intercettazioni delle comunicazioni interpersonali (un vademecum costituzionale)», *Consulta Online*, 2, 2016, pág. 232.

¹⁸ GIANFRANCESCO, E., «Profili ricostruttivi della libertà e segretezza...», *op.cit.*, pág. 232.

¹⁹ Nos referimos en este caso a la posibilidad de enviar correos electrónicos a multitud de usuarios, incluso millones, a través de técnicas de comunicación potencialmente masivas como las *mailing list*. O instrumentos como los denominados «supergrupos» de la aplicación *Telegram* que, aunque privados —en el sentido de dirigirse a destinatarios determinados— permiten envíos simultáneos de mensajes a cohortes de hasta 200.000 miembros.

ahora a los receptores de envíos masivos²⁰. Los últimos sistemas incluyen, y hasta potencian, determinado nivel de interacción de los receptores²¹.

Finalmente, la mayoría de las plataformas agrupadas bajo el término genérico de redes sociales ofrecen crecientemente gamas de interacción. Aquéllas orientadas principalmente a la difusión de información han ido incorporando funcionalidades que permiten mantener comunicaciones privadas. Pero también viceversa.

Así, aquellas aplicaciones cuya función principal es la de publicar en una cuenta de usuario *datos* más que información (historias, noticias, videos, imágenes, etc.), como las ampliamente extendidas *Facebook*, *Twitter* o *Instagram*, pueden configurarse para discriminar el universo al que se dirige el mensaje informativo, lo que implica una selección de destinatarios²². Pero, junto a ello, ofrecen herramientas de intercambio de mensajería instantánea que permiten mantener conversaciones reservadas (a través de la aplicación *Messenger*, en el caso de la primera, o de los conocidos como mensajes *directos* en otros casos).

Otras plataformas, orientadas a comunicaciones privadas, incluyen prestaciones más encaminadas a compartir información públicamente, como sucede con los denominados «estados» de *WhatsApp* o «canales» de *Telegram*.

Con estos condicionantes, el nexo entre medio comunicacional y derecho protegido que presidía las comunicaciones tradicionales queda

²⁰ CHELI, E., «Conclusioni», AA.VV., *Comunicazioni: verso il diritto della convergenza?*, 2003, págs. 184-185, en CARUSO, C., «La libertà e la segretezza...», *op.cit.*, pág. 18.

²¹ Así sucede con la general posibilidad de hacer comentarios a los contenidos «colgados» en las redes sociales o, también, en las plataformas de video (como *YouTube*) y las páginas web de medios informativos.

²² En el argot utilizado en redes sociales una cuenta es la página personal de cada usuario, identificada con un nombre de usuario —en ocasiones precedido de una arroba (@)—, un avatar —imagen que identifica al usuario— y un perfil que contiene determinada información que proporciona el usuario (descripción, edad, ubicación, etc.). Hacemos ahora referencia a las denominadas *cuentas privadas*, en las que la información publicada solo puede ser vista por determinados usuarios que han sido seleccionados por su titular.

diluido, pudiendo incluso inducir la desnaturalización de la delimitación del objeto de los derechos fundamentales involucrados²³. Es, por tanto, necesario acudir a otros criterios:

A. Predeterminación de destinatarios frente a audiencias potencialmente ilimitadas

La predeterminación de los destinatarios mantiene, no obstante, su validez como criterio delimitador en algunas situaciones.

Ha sido, además, utilizado también para excluir de plano determinadas actividades comunicacionales. La Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, excluye del concepto de comunicación a efectos de dicha norma, en su considerando 16, «[l]a información [...] dirigida a una audiencia potencialmente ilimitada»²⁴.

La «audiencia potencialmente ilimitada» y no el medio utilizado o el canal por el que discurra la comunicación es, por tanto, uno de los criterios de exclusión utilizados²⁵.

De esta forma, resulta sencillo excluir de la noción constitucional de comunicación aquellas que se producen a través de los tradicionales medios de masas, como prensa escrita, radio o televisión; así como sus análogos pero

²³ Esta afirmación parece haber sido asumida también por la Directiva 2018/1972, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, cuando señala, en su Considerando 15, que «[...] una definición de los servicios de comunicaciones electrónicas que vaya a utilizarse en el futuro no debe basarse puramente en parámetros técnicos, sino más bien en un planteamiento funcional».

²⁴ En similar sentido, pero con una redacción más desafortunada —al hablar de *multiplicidad de usuarios*—, se expresa el Preámbulo de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones: «La Ley excluye expresamente de su regulación los contenidos difundidos a través de servicios de comunicación audiovisual, que constituyen parte del régimen de los medios de comunicación social, y que se caracterizan por ser transmitidos en un solo sentido de forma simultánea a una multiplicidad de usuarios».

²⁵ «Es el carácter “determinado” e “identificable” del número de destinatarios el que permite afirmar que estamos ante una “comunicación”». RIVERO SÁNCHEZ-COVISA, F.J., *Revisión del concepto constitucional...*, *op.cit.*, pág. 15.

más avanzados tecnológicamente, periódicos digitales, *blogs* o plataformas audiovisuales.

Tampoco forman parte del concepto constitucional de comunicación las plataformas en que la información es abierta, pudiendo ser consultada por cualquier usuario sin hallar mayores restricciones de acceso²⁶. En esta categoría cabrían los foros públicos y las cuentas abiertas de redes sociales horizontales (el «muro» de *Facebook* y los perfiles de *Twitter* o *Instagram*, entre los ejemplos más conocidos)²⁷.

El mismo criterio ha servido para considerar excluidos del concepto de comunicación secreta los intercambios de información que se producen mediante redes *peer to peer* —P2P— como *eMule*, *eDonkey* y similares²⁸, ya que, en palabras del Tribunal Supremo, quienes utilizan estos programas asumen que «muchos de los datos se convierten en públicos para los usuarios de Internet» y, por tanto, «[n]o se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma»²⁹.

²⁶ RODRÍGUEZ LAINZ, J.L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», *Diario La Ley*, 8142, 2013, pág. 7. En el mismo sentido se expresa la Fiscalía General del Estado: «En estos casos, cuando las conversaciones o comunicaciones son accesibles para cualquier usuario de Internet, las mismas no pueden tener la consideración de conversaciones privadas. Por ello, estas modalidades no pueden considerarse comprendidas dentro del ámbito del derecho fundamental al secreto de las comunicaciones, por lo que no precisan de autorización judicial para su grabación u observación», *vid.* Circular de la Fiscalía General del Estado 1/2013, apdo. 12, pág. 53.

²⁷ Sí debieran estar amparadas por el secreto de las comunicaciones las que se mantienen a través de las herramientas que esas mismas redes sociales ofrecen para comunicarse reservadamente con otros usuarios (*Messenger*, *DM's*, etc.). En el mismo sentido, VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, pág. 1614. También considerando excluidas de protección del 18.3 CE las cuentas «abiertas» en redes sociales, ELVIRA PERALES, A., «Derecho al secreto de las comunicaciones», MATÍA PORTILLA, F.J. y LÓPEZ DE LA FUENTE, G. (Dir.), *De la intimidad a la vida privada y familiar. Un derecho en construcción*, Tirant Lo Blanch, Valencia, 2019, pág. 135.

²⁸ RODRÍGUEZ LAINZ, J.L., «En torno al concepto de comunicación...», *op.cit.*, pág. 7.

²⁹ STS, Sala de lo Penal, de 9 de mayo de 2008 (FJ. 2). Se podría argumentar además que tampoco cumplen con los criterios señalados en el apartado precedente. Por un lado, parece dudosa la participación humana en estos tipos de intercambios, por otro, nos hallamos ante una actividad comunicacional que se asemeja más al envío de paquetes postales que a la correspondencia, ya que estamos ante un medio generalmente no reconocido como apto para el intercambio de expresiones de sentido. Sobre el intercambio de archivos a través de

Mayores dudas puede generar el caso del *mailing list* o listas de correo electrónico. Hay quienes han entendido que el alto número de sus destinatarios y su identificación por procedimientos automáticos e impersonales empaña su determinación, hallándonos por tanto ante una comunicación masiva y no ante una reservada³⁰.

Se ha propuesto incluso como criterio —entre otros— para valorar su naturaleza privada, el de la determinación de los destinatarios desde un punto de vista cuantitativo, según la regla de que «cuantos más destinatarios reciban el mensaje, menos garantizado será su secreto»³¹.

No podemos, sin embargo, estar de acuerdo con estas propuestas. Por muy alto que sea su número, los destinatarios no devendrán ilimitados. Están identificados y determinados con precisión al tiempo de iniciar la comunicación, a través de un medio —el correo electrónico— adecuado, además, para mantener comunicaciones reservadas³².

El hecho de que las posibilidades tecnológicas permitan que la comunicación llegue fácilmente a un número muy elevado de destinatarios no puede conllevar, para el derecho considerado, un tratamiento diferenciado de la relación entre emisor y receptor³³.

redes P2P, llegando a una conclusión diferente a la aquí mantenida sobre su tutela por el 18.3 CE, *vid.* LLORIA GARCÍA, P., «El secreto de las comunicaciones: su interpretación en el ámbito de los delitos cometidos a través de Internet. Algunas consideraciones», BOIX REIG, J. (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, págs. 171-198.

³⁰ GIANFRANCESCO, E., «Profili ricostruttivi della libertà e segretezza...», *op.cit.*, pág. 232.

³¹ CARUSO, C., «La libertà e la segretezza...», *op.cit.*, pág. 19.

³² La determinación se realiza por referencia a un conjunto —todos los integrantes de la lista de correo en el momento del envío—, pero los destinatarios son en todo caso determinables.

³³ El número de destinatarios no puede tener incidencia en el secreto que garantiza el art. 18.3 CE. El criterio cuantitativo podrá tener incidencia, en su caso, en el grado de reserva que, sobre el contenido comunicado, pudiera pretender el emisor sobre el destinatario. Pero la difusión que éste realice sobre el mensaje recibido se integrará, en su caso, en el derecho a la intimidad, pero no en el secreto de las comunicaciones, que no opera entre los comunicantes y que protege únicamente las comunicaciones en tránsito.

B. Interactividad *versus* pasividad: la conmutabilidad de roles en la relación comunicativa

La noción técnica de comunicación utilizada en las normas citadas que, como hemos visto, incorpora el criterio de la determinación de destinatarios, puede, sin embargo, no ser completamente coincidente con el concepto constitucional de comunicación³⁴.

En este sentido, la Directiva 2002/58/CE citada, tras excluir del concepto de comunicación aquellas dirigidas a una «audiencia potencialmente ilimitada», dispone que «[n]o obstante, en casos en que se pueda identificar al abonado o usuario individual que recibe dicha información, por ejemplo, con servicios de vídeo a la carta, la información conducida queda incluida en el significado del término “comunicación” a efectos de la presente Directiva».

Para tratar de resolver aquellos casos todavía más problemáticos en los que el criterio de predeterminación de los destinatarios no basta por sí solo — como en el ejemplo apuntado de los servicios de vídeo a la carta, donde los destinatarios de la información transmitida están determinados—, la doctrina ha propuesto otros criterios complementarios.

Uno de ellos es el de la conmutabilidad de roles en la relación comunicativa. De este modo, sólo serían comunicaciones protegidas ex 18.3 CE las mantenidas a través de aquellos medios en los que el receptor de la comunicación pueda, haciendo uso del mismo, comunicarse con el emisor, intercambiando por tanto las posiciones iniciales³⁵.

³⁴ MATALLIN EVANGELIO, A., «El efecto expansivo de los derechos fundamentales a la intimidad y al secreto de las comunicaciones telefónicas», GONZÁLEZ CUSSAC, J.L. y CUERDA ARNAU, M.L. (Dir.), *Nuevas amenazas a la seguridad nacional: Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Tirant Lo Blanch, Valencia, 2013, pág. 397.

³⁵ CARUSO, C., «La libertà e la segretezza...», *op.cit.*, pág. 5. La conmutabilidad se refiere a los roles de los sujetos en la relación comunicativa. Esto es, en las comunicaciones bidireccionales simultáneas ambos comunicantes asumen los roles de emisor y receptor, roles que se conmutan espontáneamente en función de quién haga uso de la palabra. Del mismo modo, en las comunicaciones alternativas, quien inicialmente asume el rol de receptor (de una carta o de un *email*, por ejemplo) puede, a través del mismo medio (correspondencia o

Construido por la doctrina italiana para excluir del secreto de las comunicaciones los envíos por correspondencia de suscripciones periódicas de prensa y, según entendemos, con fundamento en la nota de pasividad que caracteriza a los destinatarios de los medios de masas, la nota de conmutabilidad de roles puede hoy ser útil para no considerar como comunicaciones reservadas las celebradas entre sujetos previamente determinados pero que discurren en sentido unidireccional emisor-audiencia; tal como sucede en los servicios de televisión por pago, vídeo bajo demanda o videoconferencias dirigidas a sujetos determinados pero sin posibilidad de interacción³⁶.

C. La singularidad del destinatario en las comunicaciones privadas

Los criterios anteriores dejan sin resolver el encuadramiento de otros tipos de comunicación en que se cumple tanto la nota de determinación de destinatarios como, en cierto modo, la de conmutabilidad de roles, pero que, sin embargo, no parecen satisfacer el carácter secreto de la comunicación.

Nos referimos tanto a las que se producen a través de cuentas de redes sociales que han sido configurados por su titular para que la información publicada sólo sea conocida por un número de destinatarios determinado por aquél (*seguidores*)³⁷; o también en foros «cerrados» que requieren un acto de

correo electrónico), comunicarse con el inicial emisor, conmutando de tal forma los roles en la relación comunicativa. Este intercambio de roles no es en principio posible en la transmisión unidireccional de contenidos que se produce en determinadas actividades comunicacionales.

³⁶ GIANFRANCESCO, E., «Profilo ricostruttivi della libertà e segretezza...», *op.cit.*, pág. 253. Esta idea parece haber sido asumida también por el legislador europeo al requerir que las comunicaciones interpersonales cumplan también con la condición de ser «interactivas», esto es, aquellas en las que «el servicio permite que el receptor de la información responda», *vid.* Directiva 2018/1972, Considerando 17.

³⁷ La limitación del número de usuarios que pueden conocer la información publicada en una determinada cuenta (conocidas como «cuentas privadas») se establece generalmente como posibilidad de activación por su titular en las redes sociales *horizontales* —aquellas dirigidas a todo tipo de usuarios y sin un eje temático determinado (como *Twitter* o *Instagram*)—, pero su configuración por defecto permite visualizar sin restricciones el contenido publicado.

aceptación de los potenciales miembros por el administrador —categoría en la que también podemos incluir los grupos cerrados de *Facebook*—.

En estos casos existe un número restringido de usuarios —determinación— que interactúan —conmutabilidad de roles— en una relación comunicacional que se lleva a cabo a través de soporte.

Desde este punto de vista pudiera no haber, en principio, grandes diferencias entre estos fenómenos, en los que un sujeto publica determinada información que otros pueden *comentar* (por ejemplo, un foro que requiera la agregación de participantes —foro cerrado— en el que participen 20 miembros o una cuenta *privada* de una red social con 50 seguidores), y otros consistentes en comunicaciones en las que intervienen una pluralidad de partícipes y que deben considerarse protegidos por el derecho fundamental al secreto de las comunicaciones (una videollamada o una comunicación grupal mediante un programa de mensajería instantánea con 40 participantes, por ejemplo). En uno y otro caso parecen verificarse los criterios utilizados hasta el momento, pues los destinatarios están delimitados y poseen, en principio, un cierto grado de capacidad para interactuar con el emisor de la información.

Esto ha hecho que parte de la doctrina se incline por considerar que aquellas actividades comunicacionales deberían quedar también garantizadas por el 18.3 CE, afirmando que «es el poder de exclusión propio de la dimensión negativa de la libertad de comunicaciones la clave definidora de cuáles [*sic*] informaciones que compartimos a través de las redes de comunicaciones deben o no entenderse amparadas por tal secreto»³⁸.

³⁸ «[...] estarían comprendidas dentro de su ámbito de protección aquellas que de una forma u otra restringen el acceso a un círculo cerrado de usuarios. Usuarios que para pertenecer a la red o comunidad deben superar un proceso de aceptación, bien sea expresa o tácita, conocido en el argot popular como agregación; bien de todos los miembros del grupo, o solamente de algunos de ellos; con o sin establecimiento de niveles de acceso». *Vid.* RODRÍGUEZ LAINZ, J.L., «En torno al concepto de comunicación...», *op.cit.*, pág. 7.

Otros autores, sin embargo, entienden que este tipo de fenómenos debieran quedar excluidos del concepto de comunicación objeto de la garantía constitucional de secreto³⁹.

Esta postura es, según creemos, la más acertada, ya que los supuestos descritos poseen un conjunto de características que determinan su calificación como actividad de divulgación de información y no como comunicación reservada, aun cuando el soporte permita ambas posibilidades siquiera parcialmente.

Así, por un lado, los destinatarios de la información que este tipo de plataformas ofrece no son escogidos, primariamente, para mantener una comunicación privada. Los destinatarios no son, en este sentido, *insustituibles*, cualidad habitualmente presente en los intervinientes en las relaciones comunicativas amparables como secretas⁴⁰.

Y no pueden serlo porque el emisor no conoce quienes serán los posibles destinatarios, ya que, si bien su número es limitado, no está tan claro que estén predeterminados. Esto es, en las comunicaciones interpersonales cuyo secreto se garantiza constitucionalmente, el emisor conoce previamente al inicio del proceso el número máximo de destinatarios potencialmente receptores. De modo que la irrupción de un nuevo participante en un grupo comunicacional (como un grupo de *WhatsApp* o una lista de correo) le permitirá conocer tan sólo los contenidos agregados desde ese momento, pero sin poder acceder a los mensajes previamente intercambiados.

³⁹ «[...] puedo “colgar” mis ideas, historias, mi vida e imágenes en un perfil de una red social, pero ello no significa que esté constituyendo una comunicación con posibles destinatarios, por mucho que el interesado haya reducido o limitado el acceso a su perfil». RIVERO SÁNCHEZ-COVISA, F.J., *Revisión del concepto constitucional...*, *op.cit.*, pág. 63.

⁴⁰ La doctrina italiana habla en este sentido de «fungibilità e delimitazione» de los destinatarios. CARUSO, C., «La libertà e la segretezza...», *op.cit.*, pág. 5. ASSCHER, por su parte, distingue entre comunicación dirigida y no dirigida: «el direccionamiento de la información refleja objetivamente la intención del remitente de que esa información esté destinada a uno o más destinatarios específicos y no a otros»; *vid.* ASSCHER, L.F., *Communicatiegrondrechten: een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, University of Amsterdam, Amsterdam, 2002, pág. 22.

Sin embargo, en los casos que estudiamos (cuentas privadas de redes sociales y foros cerrados), esta condición, determinante en la toma de decisión de quien pretende comunicar una información en privado, no se produce, pudiendo los nuevos miembros incorporados tomar conocimiento de la información publicada previamente⁴¹.

Por otro lado, en estos casos los destinatarios no poseen ningún tipo de control sobre la comunicación una vez finalizado el proceso, como sí ocurre en las comunicaciones reservadas de relación alternativa.

En los envíos de correspondencia, mensajes *SMS*, correos electrónicos y chats de mensajería instantánea, el destinatario, finalizado el proceso comunicativo, mantiene cierto dominio sobre el contenido comunicado: bien en exclusiva —caso de la correspondencia, donde la comunicación se traslada físicamente entre uno y otro—; o bien de forma compartida —en el resto de los ejemplos, donde el emisor conserva también el contenido comunicativo de los mensajes enviados—. En cualquier caso, el destinatario puede desde ese momento decidir sobre el contenido de la comunicación, pudiendo guardarla o deshacerse de ella (destruyendo la carta o borrando el mensaje).

Este escenario es incompatible, por el contrario, con el caso de las texturas comunicacionales del tipo de los foros o las redes sociales privadas. Y ello porque los usuarios de estas plataformas no son, en puridad, destinatarios, no son receptores de una comunicación, sino que únicamente poseen una capacidad de acceso al contenido. La información permanece en todo caso bajo el dominio de quien la ha publicado, y sólo él puede suprimirla o mantenerla publicada en la plataforma. Del mismo modo, si bien estas herramientas permiten, como dijimos, una cierta interacción, la información

⁴¹ Trasladando esta situación al mundo *offline* tal vez sea más evidente que no estamos ante una comunicación en el sentido del 18.3 CE. Para ello, podríamos comparar estos fenómenos con la publicación de información en un tablón situado en un espacio con acceso limitado de personas.

que los usuarios puedan publicar como respuesta o comentario al contenido inicial también va a permanecer, en principio, bajo su dominio.

Por todo ello, la noción constitucional de comunicación, en los términos precisados *supra*, configura un objeto de derecho fundamental que no parece posible llegue a incluir este tipo de procesos.

En definitiva, el criterio de la predeterminación de los destinatarios es efectivo para deslindar las comunicaciones cuyo secreto garantiza la Constitución, pudiendo ser complementado, para la resolución de situaciones dudosas, con los de conmutabilidad de roles en la relación comunicativa e individualización en la selección de destinatarios.

I.3. Comunicación técnicamente mediada y a través de canal cerrado

A. Soporte e intermediación técnica: comunicación *versus* conversación directa

Las formas comunicativas expresamente enumeradas en el artículo 18.3 CE comparten también la doble característica del soporte y la intermediación técnica, imprescindible para la transmisión entre emisor y destinatario.

El Tribunal Constitucional ha destacado que esta doble condición determina el carácter autónomo del derecho al secreto de las comunicaciones. «[S]u específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación»⁴².

⁴² STC 123/2002, de 20 de mayo (FJ. 5). La presencia del tercero en el proceso comunicativo está, como vimos, en la génesis de este derecho fundamental, cuyo nacimiento vino impulsado por los abusos del servicio de correo con la creación de los *cabinets noirs*. Esta ha sido también la interpretación que ha realizado el Tribunal Constitucional Federal Alemán del art. 10.1 GG: «El artículo 10.1 de la Ley Básica está destinado a contrarrestar los riesgos sobre la confidencialidad de los mensajes que surgen del proceso de transmisión»; *BVerfGE* 106, 28, de 9 de octubre de 2002 (§20). En igual sentido, *BVerfGE* 85, 386, de 25 de marzo

La norma atribuye el carácter de secreto a estas comunicaciones precisamente porque durante la participación del tercero intermediario se sustrae a los comunicantes el control del mensaje⁴³.

De ahí que la noción de comunicación del art. 18.3 CE, más allá del tenor literal del precepto («se garantiza el secreto de las comunicaciones...»), no puede alcanzar a subsumir un concepto de comunicación indefinido e ilimitado. La comunicación protegida no es, por tanto, toda transmisión mediante un código común a emisor y receptor, sino tan solo la que satisfaga la doble condición de ser soportada técnicamente.

Esta ha sido igualmente la opinión mayoritaria de la doctrina que, en lógica consecuencia, ha entendido que no forman parte del ámbito de protección de este derecho las conversaciones directas, mantenidas en persona y sin soporte técnico⁴⁴.

La comunicación directa podrá ser, eventualmente, «reservada», vale decir, dependiente de la disposición de los interlocutores; pero no secreta. La determinación constitucional de secreto sólo es predicable con relación al soporte técnico, que, al poseer naturaleza instrumental, nunca despeja su vulnerabilidad⁴⁵.

Este recurso al medio habilita necesariamente una protección formal, por cuanto los comunicantes pierden el dominio del proceso y la capacidad de asegurar el secreto del mensaje y/o el éxito en la entrega. En las

de 1992 (§46); *BVerfGE* 100, 313, de 14 de julio de 1999 (§175); y *BVerfGE* 115, 166, de 2 de marzo de 2006 (§75).

⁴³ VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, pág. 1611. «The underlying rationale to warrant such protection is that communicants entrust communication to an intermediary, thus losing control in relation to the intermediary or third parties»; *vid.* ZUIDERVEEN BORGESIU, F.J., y STEENBRUGGEN, W., «The right to communications confidentiality...», *op.cit.*, pág. 299.

⁴⁴ Por todos, JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 49; ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, *op.cit.*, pág. 16; y MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 52.

⁴⁵ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 49

conversaciones personales, donde el mensaje se articula mediante la intermediación emisor-receptor, ambos pueden adoptar determinadas medidas para asegurar o procurar la inaccesibilidad de terceros, es decir, la reserva del contenido; nunca, claro, el secreto de la relación comunicativa⁴⁶.

No obstante, algunos autores han entendido que esta tradicional interpretación doctrinal se ha basado en la imposibilidad de acceder —en el estado del conocimiento científico-tecnológico del momento constituyente— al contenido de conversaciones directas. La existencia actual de tecnologías (drones, micrófonos «espía» o direccionales para captar conversaciones a larga distancia, etc.) capaces de captar comunicaciones ambientales, pondrían en riesgo objetivo la libertad de comunicarse secretamente en persona y limitarían la posibilidad de vedar el acceso a las comunicaciones no mediadas por soporte técnico. Por esta razón parte de la doctrina propone ampliar la protección a las conversaciones directas en el marco del art. 18.3 CE⁴⁷.

Para otros autores, la inmisión de un elemento técnico en la relación establecida entre los comunicantes, jurisprudencialmente entendido como «indispensable para configurar el ilícito constitucional» vulnerador del 18.3 CE

⁴⁶ VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, pág. 1612.

⁴⁷ «También porque es difícil valorar, desde un punto de vista jurídico, si la opción por la utilización de la comunicación técnica supone la asunción de un mayor riesgo voluntario por parte de los comunicantes, o deriva de otro orden de razones: la distancia física de emisor y receptor, o la eficacia, en tiempo, de lo que se pretende transmitir». ZOCO ZABALA, C., «Intervención de las comunicaciones e intervención de las conversaciones...», *op.cit.*, págs. 358 y ss. Otros autores han considerado, sin mayores explicaciones, que la captación y grabación de comunicaciones orales «afecta siempre al derecho fundamental al secreto de las comunicaciones contenido en el art. 18.3 CE, precepto mediante el cual el constituyente no ha querido proteger exclusivamente el secreto de las comunicaciones íntimas, sino cualquier clase de comunicación»; DÍAZ MARTÍNEZ, M., «La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos», DÍAZ MARTÍNEZ, M. y LÓPEZ-BARAJAS PEREA, I. (Coords.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant Lo Blanch, Valencia, 2018, pág. 94. Se considera también vulnerado el secreto de las comunicaciones en CASANOVA MARTÍ, R., «La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos», *Diario La Ley*, 8674, 2016, pág. 2; y ROSALES LEAL, M.A., «Captación y grabación de comunicaciones orales directas», *Revista de Derecho Constitucional Europeo*, 30, 2018.

—STC 114/1984, de 29 de noviembre (FJ. 7)— basta con que provoque una interferencia, sin que sea preciso que alcance a mediar en el proceso comunicativo. De esta forma, constituiría también una injerencia en el secreto de las comunicaciones la utilización de artificios o dispositivos dirigidos a captar el contenido, o constatar su mera existencia, de una conversación directa⁴⁸.

Hasta la STC 145/2014, de 22 de septiembre, la existencia de un soporte o medio técnico como elemento delimitador de las comunicaciones protegidas ex 18.3 CE ha sido una cuestión pacífica en la jurisprudencia constitucional⁴⁹.

Dicha resolución propuso, sin embargo, una innovación de calado al considerar que una grabación de conversaciones orales entre detenidos se incluía en el objeto del derecho fundamental al secreto de las comunicaciones. Consideró que «el art. 18.3 CE no dispone una distinta protección de las conversaciones telefónicas [...] que de otras comunicaciones como las verbales, sino solo una garantía común y genérica frente a la impenetrabilidad por terceros ajenos a la comunicación misma». En consecuencia, no existiendo una habilitación legal previa y suficiente para la práctica de dicha diligencia —excluyendo la posible aplicación del art. 579.2 LECrim y la doctrina jurisprudencial sobre los requisitos para la intervención de comunicaciones telefónicas—, declaró la nulidad de la prueba obtenida, al

⁴⁸ RIVERO SÁNCHEZ-COVISA, F.J., *Revisión del concepto constitucional...*, *op.cit.*, pág. 44. En contra, y en opinión que compartimos, se ha dicho que: «Cuando hablamos de la exigencia de un soporte técnico nos referimos al de la comunicación y no al de la interferencia, independientemente de que la interceptación de cierto tipo de comunicaciones requiere hoy día una cierta sofisticación tecnológica». Cfr. MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 52.

⁴⁹ Con anterioridad habían sido varios los pronunciamientos del Tribunal Constitucional que habían refrendado la posición doctrinal mayoritaria: entre otras, SSTC 123/2002, de 20 de mayo (FJ.5); 281/2006, de 9 de octubre (FJ. 3); y 170/2013, de 7 de octubre (FJ. 4). Aunque referida al ámbito de las relaciones laborales, la STC 98/2000, de 10 de abril (FJ. 6), residencia la colocación por parte del empresario de un micrófono ambiental para captar las conversaciones de sus empleados en el derecho a la intimidad. Consideran incluidas las conversaciones directas en el 18.3 CE, HERNÁNDEZ DOMÍNGUEZ, J.J. y MARTÍNEZ MARTÍN J.I., *Secreto de las Comunicaciones. Alcance de protección constitucional de su interpretación y casuística*, Dilex, Madrid, 2015, págs. 98-101.

serlo mediante vulneración del derecho fundamental al secreto de las comunicaciones⁵⁰.

Esta interpretación invita a varias consideraciones. La primera, quizá obvia, se refiere al profundo cambio jurisprudencial que propone; y a su trascendencia —posibilitando que se declare la nulidad de la diligencia de grabación de conversaciones en un número importante de procedimientos—. Lo que resulta llamativo al no acompañarse tamaña afirmación de una sólida estructura argumental orientada a justificar un cambio doctrinal de tanta trascendencia jurídica.

Por otra parte, la estimación del amparo por ausencia de habilitación legal debiera haber venido precedida de un ordenado análisis para determinar si la diligencia recurrida formaba o no parte del objeto del derecho fundamental alegado⁵¹. Sin embargo, más allá del pasaje transcrito *supra*, la Sala no considera preciso pronunciarse sobre la naturaleza de comunicación, en el sentido del art. 18.3, de las conversaciones orales intervenidas. Algo especialmente llamativo si nos atenemos a los reiterados pronunciamientos previos a los que no se alude en tan importante sentencia.

En sentido inverso, son varias las razones que, a nuestro juicio, permiten afirmar que la inclusión de conversaciones directas registradas mediante medio técnico en el objeto del derecho al secreto de las comunicaciones no es constitucionalmente correcta.

En primer lugar, porque no hay patrón para ello, en términos de derecho comparado, en aquellas constituciones que configuran este derecho en términos similares a la nuestra. La mayoría de las constituciones de referencia

⁵⁰ Un análisis de esta sentencia puede verse en RODRÍGUEZ LAINZ, J.L., «Sobre la inconstitucionalidad de las vigilancias policiales mediante micrófonos ocultos (A propósito de la STC 145/2014, de 22 de septiembre)», *Diario La Ley*, 8438, 2014, págs. 1-14.

⁵¹ El recurrente residencia la vulneración producida únicamente en el art. 18.3 CE y no, como quizá hubiera sido acertado, incluso de modo subsidiario, en el derecho a la intimidad previsto en el art. 18.1 CE.

atribuyen la garantía de secreto a la correspondencia o, en su caso, a las telecomunicaciones⁵².

También en términos de «correspondencia» se expresan distintos instrumentos internacionales de protección de derechos, como el art. 12 de la Declaración Universal de los Derechos Humanos de 1948, el art. 17.1 del Pacto Internacional de Derechos Civiles y Políticos de 1966 y el art. 8.1 del Convenio Europeo de Derechos Humanos de 1950.

La jurisprudencia del TEDH, por su parte, ha interpretado el término «correspondencia» presente en el Convenio en sentido amplio, considerando incluidas otras comunicaciones mantenidas a través de medio técnico, como las telegráficas o las telefónicas⁵³.

En los casos en que ha enjuiciado la colocación de dispositivos de grabación de conversaciones directas, el TEDH ha considerado que esta

⁵² En estos términos se expresan, por ejemplo, la Constitución alemana de 1949, cuyo artículo 10.1 declara inviolable «[...] el secreto de la correspondencia, así como el del correo y las telecomunicaciones». En tal sentido, el TCFA ha afirmado que «[c]uando se utilizan equipos de telecomunicaciones, la comunicación está expuesta a riesgos particulares de conocimiento por parte de terceros y, por lo tanto, está sujeta a protección especial [...]. A diferencia de una conversación entre los presentes, los interlocutores no tienen la oportunidad de determinar las condiciones marco de la comunicación solos y controlar su privacidad y las personas involucradas. Debido a la distancia espacial entre ellos, los comunicadores dependen de un proceso de transmisión técnica que no está dentro de su esfera de influencia exclusiva»; cfr. *BVerfGE* 106, 28, de 9 de octubre de 2002 (§20). En iguales términos, *vid. BVerfGE* 67, 157, de 20 de junio de 1984 (§53); *BVerfGE* 85, 386, de 25 de marzo de 1992 (§46); *BVerfGE* 100, 313, de 14 de julio de 1999 (§175); *BVerfGE* 115, 166, de 2 de marzo de 2006 (§65); y *BVerfGE* 120, 274-350, de 24 de febrero de 2008 (§182). También las constituciones, temporalmente cercanas a la española, de Grecia y Portugal, que protegen, respectivamente, «[...] el secreto de las cartas, así como el de cualquier otro medio de libre correspondencia o comunicación» (art. 19.1 de la Constitución griega de 1975) y «la correspondencia, telecomunicaciones, u otros medios de comunicación» (art. 34.4 de la Constitución portuguesa de 1976). Especialmente precisas resultan algunas constituciones europeas más modernas. Por ejemplo, el artículo 22.2 de la Constitución eslovaca de 1992 declara inviolable «el secreto de la correspondencia, así como el de otras comunicaciones o mensajes escritos que han sido mantenidos de forma privada o son enviados por correo o por cualquier otro medio» y también «el secreto de las comunicaciones telefónicas, telegráficas o por otros dispositivos similares». Igualmente, el artículo 43 de la Constitución estonia de 1992 reconoce el derecho a «la confidencialidad de los mensajes enviados o recibidos por correo, telégrafo, teléfono u otros medios comúnmente usados».

⁵³ Entre otras, SSTEDH de 6 de septiembre de 1978 (asunto *Klass* y otros c. Alemania, §41) y de 2 de agosto de 1984 (asunto *Malone* c. Reino Unido, §64). *Vid.* RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. 64.

práctica puede afectar a los derechos reconocidos en el art. 8.1 CEDH. No obstante, en su habitual valoración indiferenciada de los diversos derechos que dicho precepto alberga (respeto a la vida privada y familiar, al domicilio y a la correspondencia), o bien ha declarado la injerencia en base al art. 8.1 CEDH, sin mayores especificaciones, o bien ha situado la injerencia expresamente en el derecho al respeto de la vida privada, sin mención alguna a la correspondencia⁵⁴.

Por tanto, tampoco de las resoluciones del TEDH puede deducirse la obligación de considerar amparadas en el art. 18.3 las conversaciones directas *via* art. 10.2 CE, sino que será igualmente respetuoso con dicho precepto entender que forman parte del objeto protegido por el derecho a la intimidad del artículo 18.1 CE⁵⁵.

Justamente por ello, cabe rechazar algunos de los argumentos esgrimidos habitualmente a favor de la inclusión en el art. el 18.3 CE de las conversaciones sin mediación.

Por una parte, la actual existencia de riesgos de confidencialidad no puede ser argumento válido para forzar una dilatación del concepto constitucional de comunicación, por cuanto del mismo parece derivarse, sin que sea correcto, que, de no considerar amparada la intervención de

⁵⁴ Del primer tipo son, entre otras, las SSTEDH de 12 de mayo de 2000 (asunto *Khan* c. Reino Unido, §25) y de 31 de mayo de 2005 (asunto *Vetter* c. Francia, §20). Por su parte, la STEDH de 25 de septiembre de 2001 (asunto *P.G. y J.H.* c. Reino Unido, §60), parece residenciar específicamente esta medida en el respeto a la vida privada, en los siguientes términos: «*The Court concludes therefore that the recording of the applicants' voices when being charged and when in their police cell discloses an interference with their right to respect for private life within the meaning of Article 8 § 1 of the Convention*».

⁵⁵ VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, págs. 1613. Sobre los problemas de interpretación derivados de la existencia de normas nacionales e internacionales dirigidas a garantizar un mismo derecho de manera no necesariamente idéntica, *vid.* ROSOUX, G., «Au cœur de la protection “multi-niveaux” et du dialogue juridictionnel: la “dématisation” des droits fondamentaux comme clé de lecture du raisonnement actuel dans le domaine des droits fondamentaux», *Fundamentos. Cuadernos monográficos de teoría del estado, derecho público e historia constitucional*, 9, 2016, págs. 71-99.

conversaciones en el art. 18.3 CE, éstas quedarían radicalmente desprotegidas por el ordenamiento.

Tales supuestos pueden hallar protección en el derecho a la intimidad, que es el bien dañado propiamente en una acción de inmisión en una conversación sin mediación⁵⁶. Algo obviamente distinto.

Al no depender la comunicación de un soporte técnico, como es el caso de la comunicación *ex art.* 18.3 CE, corresponderá a los interlocutores la absoluta disposición sobre el grado de reserva y, por tanto, la exclusividad del control de una comunicación cara a cara. No se tratará nunca, por tanto, de conversaciones formalmente secretas, sino que se integrarán o no en «el ámbito propio y reservado [de los interlocutores] frente a la acción y conocimiento de los demás», atendidas lógicamente las circunstancias de la conversación entablada⁵⁷.

Así, la exclusión de terceros de una comunicación directa dependerá de la actitud de los comunicantes, «ya que corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno»⁵⁸, determinada en función de varias circunstancias (tales como el volumen de voz, el lugar escogido, el número de participantes, ...). E incluso de otras características, como la condición de personaje público de alguno de los interlocutores o el interés informativo de la conversación mantenida.

⁵⁶ El desarrollo normativo de la diligencia de investigación de captación de conversaciones orales tampoco despeja las dudas sobre su protección por uno u otro derecho fundamental. Como señala ELVIRA PERALES, la Ley Orgánica 13/2015 rubrica el Título VIII que incorpora a la LECrim como «De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución», sin distinguir en los posteriores capítulos los diferentes derechos implicados y dejando, por tanto, su interpretación en manos de los tribunales. *Vid.* ELVIRA PERALES, A., «Derecho al secreto...», *op.cit.*, pág. 126. No obstante, la LECrim no permite en el caso de la grabación de conversaciones orales la intervención de la policía sin resolución judicial previa en casos de urgencia para la investigación de delitos de terrorismo, como sí lo hace en el caso de la intervención de comunicaciones (art. 588 ter d.3 LECrim); y ello, según creemos, porque el derecho a la intimidad no está sujeto a la posibilidad de su suspensión individual en el art. 55.2 CE.

⁵⁷ STC 231/1988, de 2 de diciembre (FJ. 3).

⁵⁸ STC 83/2002, de 22 de abril (FJ. 5).

Esta interpretación encuentra además respaldo en el desarrollo normativo del derecho a la intimidad, que reputa como injerencia —inmisión contraria a norma— el recurso a aparatos de escucha para obtener información sobre aspectos de la vida íntima de las personas⁵⁹.

Por otra parte, una propuesta de interpretación amplia del concepto de comunicación del artículo 18.3, que acogiera toda transmisión de información, plantearía serias dificultades para la re-delimitación del objeto. Ello obligaría a forzar una distinción, con alcance imprevisible, entre comunicación verbal y no verbal (más allá de lenguajes codificados como el de signos), alcanzando así a la puramente gestual, aunque capaz de vehicular contenidos comunicativos⁶⁰.

Añádase además que las conversaciones directas no satisfacen tampoco otras condiciones que analizaremos posteriormente. Como se verá, la comunicación protegida es aquella transmitida a través de determinados canales cerrados, condición no presente en las conversaciones aludidas, que discurren por el medio propio de la intercomunicación física⁶¹.

En suma, cabe pues concluir que las comunicaciones protegidas por el art. 18.3 CE son sólo aquellas que se realizan a través de soporte o medio técnico, sin que quepa considerar que la intervención de conversaciones

⁵⁹ Artículo 7.1 y 2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (en adelante, LOPH). La ley recoge también aquellos criterios para valorar si una determinada conversación debe quedar amparada por el derecho a la intimidad. Así, por un lado, el artículo 2 LOPH señala como criterio delimitador de los derechos que desarrolla los propios actos de su titular y, por otro lado, el artículo 8.1 no considera intromisiones ilegítimas aquellas en las que predomine «un interés histórico, científico o cultural relevante».

⁶⁰ RODRÍGUEZ LAINZ, J.L., «Sobre la inconstitucionalidad de las vigilancias policiales...», *op.cit.*, pág. 7.

⁶¹ También se ha argumentado que estas conversaciones no forman parte del objeto protegido por el artículo 18.3 CE con base en el mismo enunciado lingüístico original del precepto. La ausencia de justificación en la enmienda que introdujo la cláusula «en especial» para separar el término «comunicaciones» de la enumeración ejemplificativa de sus modalidades ha sido entendida como una mejora técnica en previsión de las posibles futuras formas de comunicación mediante soporte, *pero no de cualquier otra forma de comunicación*. RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, pág. 30.

ambientales suponga una injerencia en el derecho al secreto de las comunicaciones, al no quedar éstas incluidas en su objeto.

B. Características del medio. Las denominadas «comunicaciones abiertas»

Más allá de la voluntad del emisor de comunicarse en privado —abordada en el apartado I.2— y de la necesidad de hacerlo mediante soporte —lo que nos ha hecho excluir las conversaciones directas—, para que la comunicación logre garantía de secreto debe llevarse a cabo a través de determinados medios o canales «cerrados»⁶².

En este sentido, es patente la limitada precisión terminológica en ciertas manifestaciones doctrinales y decisiones jurisprudenciales que introducen un criterio taxonómico —abierto/cerrado— para clasificar la comunicación o el medio o canal utilizado.

El objetivo del presente apartado es tratar de, al menos, identificar algunas imprecisiones asociadas a aquellos criterios.

En las comunicaciones de base tecnológica, los conceptos de medio y canal identifican el soporte utilizado para transmitir la información y hacen referencia tanto al medio físico (medios confinados) como a la frecuencia portadora de la información (medios no confinados)⁶³.

En los primeros, las ondas se confinan en un medio sólido, como los cables de par trenzado, cables coaxiales o la fibra óptica. En los medios no

⁶² «Asimismo, en nuestra labor de delimitación del ámbito de cobertura del derecho, hemos precisado que el art. 18.3 CE protege únicamente ciertas comunicaciones: las que se realizan a través de determinados medios o canales cerrados»; STC 170/2013, de 7 de octubre (FJ. 4).

⁶³ Vid. definiciones de «canal» en *Diccionario LID de Tecnologías de Información y comunicación*, 2007, pág. 93 y de «medio de transmisión» en *Diccionario Español de Ingeniería, sección Telecomunicaciones* (consulta online en: <http://diccionario.raing.es/es>).

confinados la información se transmite por el éter, mediante radiofrecuencias, que a su vez pueden recurrir a satélites.

La caracterización de un medio o canal como cerrado o abierto depende de sus características técnicas *actuales*, es decir, de su capacidad para garantizar técnicamente un razonable grado de dificultad para quebrar el secreto⁶⁴. Por tanto, se trata de un concepto gradual y cambiante, expuesto a un constante grado de revisión de su capacidad protectora medida en términos estrictamente tecnológicos.

Así, serán canales cerrados aquellos que permitan las comunicaciones punto a punto o multipunto, esto es, aquellas en que la transmisión de información se produce entre un punto fijo especificado y otro u otros puntos fijos especificados, sin posibilidad de acceso por terceros de acuerdo con un grado de dificultad estándar y cambiante⁶⁵.

De este modo, la garantía tecnológica de secreto no puede ser entendida como la imposibilidad absoluta de terceros de interceptar la comunicación. De aceptar tal premisa, con los actuales avances tecnológicos la eficacia del derecho —en sentido material—, en términos fácticos o de verosimilitud técnica, sería nula⁶⁶.

Ello hace jurídicamente irrelevante el carácter abierto o cerrado de un soporte comunicacional, al tratarse de una cualificación de carácter puramente tecnológico. El carácter abierto o cerrado del canal en función del grado de dificultad tecnológico oponible a la enervación del secreto, no puede en ningún modo determinar el ámbito del objeto del derecho fundamental del art. 18.3 CE.

⁶⁴ RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. 67. También en este sentido GIANFRANCESCO, E., «Profili ricostruttivi della libertà e segretezza...», *op.cit.*, pág. 238.

⁶⁵ *Diccionario Español de Ingeniería, sección Telecomunicaciones*.

⁶⁶ CARUSO, C., «La libertà e la segretezza...», *op.cit.*, pág. 19; y RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. 69.

Ciertamente ello no permite prescindir de la distinción, que conserva una importante función. Serán comunicaciones por canal cerrado aquellas para cuya inmisión es necesario recurrir a tecnología especial *ad hoc*, o bien —añadamos— a la colaboración del prestador del servicio de comunicaciones. Por su parte, serán comunicaciones por canal abierto aquellas que pueden ser captadas «con aparatos cuyo uso principal es distinto y perfectamente legítimo»⁶⁷.

El ejemplo más evidente podemos hallarlo en las diferencias existentes entre determinadas comunicaciones por radioteléfonos y las comunicaciones por telefonía celular. En ambos casos la comunicación se mantiene a través de soportes portátiles y discurren —canal— por el espectro radioeléctrico.

Sin embargo, no pueden formar parte de la noción de comunicación protegida por el artículo 18.3 CE las comunicaciones por radioteléfonos a través de frecuencias de uso público, en las que las ondas de radio circulan libremente y pueden, por tanto, ser captadas por un receptor de radio ordinario. Estaríamos en este sentido ante una comunicación por canal abierto⁶⁸.

Por el contrario, las comunicaciones por telefonía celular o móvil se desarrollan a través de un canal cerrado. Cuando iniciamos la comunicación la estación base adjudica una frecuencia específica, de entre todas en que se divide el ancho de banda de frecuencia, y, establecida la conexión, ese canal se conserva hasta que finaliza la llamada, impidiendo que se produzcan otras comunicaciones en el mismo rango de frecuencia.

Hasta aquí no hay mayores problemas. Sin embargo, las dificultades pueden llegar cuando lo calificado jurisprudencialmente como abierto no es el

⁶⁷ RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. 79.

⁶⁸ STS, Sala de lo Penal, de 22 de diciembre de 2011 (FJ. 2). Cfr. también RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, págs. 7 y ss.; RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, pág. 28; y Circular de la Fiscalía General del Estado 1/2013, apdo. 5.11, págs. 36-37.

canal, en el sentido explicado, sino la comunicación en sí; lo que ha sucedido en dos ámbitos.

En primer lugar, en el caso de los paquetes postales, la STC 281/2006, de 9 de octubre (FJ. 3), considera que «quedan fuera de la protección constitucional aquellas formas de envío de la correspondencia que se configuran legalmente como comunicación abierta»⁶⁹.

En segundo lugar, las SSTC 241/2012, de 17 de diciembre (FJ. 7), y 170/2013, de 7 de octubre (FJ. 4), califican también como comunicaciones abiertas las producidas en el marco de una relación laboral y utilizando para ello medios propiedad de la empresa.

En ambos casos el fundamento es el mismo: la existencia del poder de inspección de un tercero, en un caso los servicios postales, en otro el empresario.

Sin embargo, según entendemos, la calificación de *abierto* opera en sentidos diferentes, en cuanto a la delimitación del derecho, según recaiga sobre el canal o sobre la comunicación.

El primer caso opera en el *objeto* del derecho, ya que las comunicaciones por canal abierto —en oposición a cerrado— no forman parte de la noción de comunicación del artículo 18.3 CE.

El segundo caso, sin embargo, opera en el *contenido* del derecho. Las comunicaciones calificadas jurisprudencialmente como abiertas —opuesto aquí a secretas— en las Sentencias 241/2012 y 170/2013 se mantienen, respectivamente, a través de programas de intercambio de mensajería instantánea y correo electrónico y, por tanto, cumplen con todos los requisitos necesarios para considerarlas comunicación *ex* artículo 18.3 CE. Sin embargo, no se benefician de la garantía de resolución judicial, que constituye

⁶⁹ «Así sucede cuando es legalmente obligatoria una declaración externa de contenido, o cuando bien su franqueo o cualquier otro signo o etiquetado externo evidencia que, como acabamos de señalar, no pueden contener correspondencia, pueden ser abiertos de oficio o sometidos a cualquier otro tipo de control para determinar su contenido».

el contenido del derecho, por cuanto los intervinientes, conociendo la existencia de una facultad de inspección, con la puesta en marcha del proceso comunicativo han consentido —al menos tácitamente— la posibilidad de que ese sujeto fiscalizador alzara el secreto sin necesidad de intermediación judicial⁷⁰.

Esta diferenciación hace que las consecuencias sean también diversas. Así, en el primer caso, nada impide que, no hallándonos ante una comunicación protegida por el secreto de las comunicaciones, esa actividad encuentre eventualmente amparo en el art. 18.1 CE. En el segundo, sin embargo, un consentimiento válidamente prestado servirá también como renuncia a determinadas garantías del derecho a la intimidad.

⁷⁰ También de este modo ha sido entendido por la jurisprudencia recaída en asuntos sobre envío de paquetes postales bajo el régimen de «etiqueta verde», al considerar que «[a]l aceptar el envío bajo etiqueta verde se aceptan todas sus condiciones y entre ellas la posibilidad de apertura para control del contenido; hay renuncia expresa al posible derecho de secreto del contenido del paquete». *Vid.* SSTS, Sala de lo Penal, de 23 de marzo de 1995 (FJ. 3) y de 1 de febrero de 1996 (FJ. Único).

II. ÁMBITO TEMPORAL DEL DERECHO: INTERVENCIÓN Y ACCESO

La transmisión de contenido en que consiste la comunicación debe ser entendida como un proceso compuesto de una serie de fases precisas para que aquélla se produzca.

En puridad, lo protegido por el derecho es precisamente el proceso de comunicación que se garantiza, según dijimos, en un sentido formal: esto es, con independencia de que exista un contenido y al margen de su carácter íntimo o reservado.

La comunicación así entendida se desarrolla en un espacio temporal con unos límites inicial y final más o menos definidos. No obstante, esos límites del proceso comunicacional en abstracto —el curso temporal de una comunicación— pueden no ser plenamente coincidentes con el alcance temporal del derecho al secreto de las comunicaciones.

Por ello, es preciso fijar rigurosamente los límites del proceso comunicativo relevantes para la norma iusfundamental, lo que nos permitirá delimitar el espacio temporal protegido por el derecho considerado y, a su vez, las fases del proceso que quedan, en su caso, al amparo de otros derechos⁷¹.

Este entendimiento de la comunicación protegida como un proceso es pacífico tanto en la doctrina como en la jurisprudencia, y así lo ha declarado el Tribunal Constitucional al precisar que «[l]a protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo»⁷².

⁷¹ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 43.

⁷² STC 70/2002, de 3 de abril (FJ. 9). También la STC 56/2003, de 24 de marzo (FJ. 2), tras reproducir la cita de la resolución señalada, añade que «la protección de este derecho alcanza a las interferencias habidas o producidas en un proceso de comunicación».

Sin embargo, aquella unanimidad no llega a la determinación del alcance temporal de ese proceso en que la comunicación consiste; a ello dedicamos el presente apartado⁷³.

II.1. Inicio del proceso comunicativo

La activación del derecho al secreto de las comunicaciones requiere que el proceso comunicativo haya comenzado.

Si la comunicación protegida se produce a través de determinados soportes es necesario, en primer lugar, que se plasme en dichos soportes; pero no solo eso. Pues si el fundamento del carácter autónomo de este derecho reside en la necesaria participación de un tercero que hace posible la comunicación, su correcta interpretación requiere que el inicio del proceso comunicativo protegido sea simultáneo a la participación del tercero.

Esta interpretación parece ser la mantenida por el Tribunal Constitucional en la STC 137/2002, de 3 de junio (FJ. 3), donde se descarta la vulneración del derecho al secreto de las comunicaciones al no existir interferencia alguna en el proceso comunicacional, ya que «el paquete postal se interceptó y abrió antes de depositarse en las oficinas postales para su remisión al destinatario».

De este modo, el derecho comenzará a operar desde que el emisor cede el control de la comunicación al tercero prestador del servicio, esto es, cuando se deposita la carta, se realiza la llamada telefónica o se clica el botón de envío de un correo electrónico en la aplicación informática⁷⁴.

No quedarán cubiertas por este derecho las acciones previas a dicho momento, tal como la redacción de la carta, ya que el emisor no ha perdido

⁷³ Los problemas derivados de la protección iusfundamental fuera de esos límites temporales (acceso al mensaje o a los datos de tráfico) se abordan al analizar, en el capítulo tercero, los contenidos protegidos por el secreto.

⁷⁴ En el mismo sentido, LUCAS MURILLO DE LA CUEVA, P., «Notas sobre el derecho fundamental...», *op.cit.*, pág. 677.

aún el control de la comunicación que, además, en términos estrictos, no ha comenzado, pues todavía no existe un contenido definido finalizado y transmisible. Así, no estarán amparados por el 18.3 CE, por ejemplo, los correos electrónicos redactados y almacenados no remitidos o las misivas escritas que obren todavía en poder del emisor⁷⁵.

II.2. Finalización del proceso comunicativo

El criterio señalado para establecer el inicio de la comunicación protegida no ha presentado hasta el momento especiales problemas o dificultades. No obstante, no cabe decir lo mismo cuando, manteniendo criterio similar en relación con el objeto del derecho, pretendemos delimitar el momento final del proceso comunicativo.

No plantea problemas el contenido ya transmitido que atestigua la finalización del proceso comunicativo. En este caso no cabe protección jurídica con base en el art. 18.3 CE, sino, en su caso, en «las normas que tutelan la intimidad u otros derechos»⁷⁶.

Sin embargo, tanto en la doctrina como en la jurisprudencia existen diversas opiniones sobre el alcance del derecho en su fase final, situando en diferentes momentos el término de la protección de la comunicación.

Los problemas se producen en el caso de los procesos comunicativos unidireccionales (correspondencia, correo electrónico, intercambio de mensajería, ...) en relación con el tratamiento otorgado a la comunicación recibida. En el caso de las comunicaciones interactivas simultáneas (conversación telefónica o videoconferencia) parece fácil convenir que el

⁷⁵ No existe además una justificación razonable para otorgar a estos documentos una protección formal y, por tanto, más intensa que a otros guardados por el destinatario, ya sea en papel o en formato digital, cuyo riesgo de acceso por parte de terceros son similares. En este sentido, VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, pág. 1619.

⁷⁶ Por todas, STC 70/2002, de 3 de abril (FJ. 9).

proceso finaliza con el de la conversación, esto es, cuando todos los intervinientes desactivan el soporte⁷⁷.

Analizaremos a continuación las tres posiciones mantenidas respecto al alcance final de la garantía de secreto.

A. La protección del sistema comunicativo

Una primera posición doctrinal, ampliamente garantista, ha llevado a algunos autores a extender la protección del derecho fundamental a los mensajes recibidos por el destinatario, mientras se encuentren almacenados en el dispositivo y software gestor de la comunicación (servidor de correo electrónico o aplicación de mensajería móvil)⁷⁸.

Aunque esta posición se ha justificado como la más respetuosa con la jurisprudencia que considera como vulneración del artículo 18.3 CE «el conocimiento antijurídico de lo comunicado»⁷⁹, la protección no se hace depender, como en la sentencia citada, de que el destinatario haya accedido a la comunicación, sino simplemente de la ubicación de la comunicación recibida.

Así, se afirma que «el contenido dejará de considerarse amparado por el art. 18.3 CE en los casos en los que el texto del mensaje haya sido guardado fuera del correo electrónico o del teléfono móvil», pasando a ser tutelado, en su caso, por el derecho a la intimidad⁸⁰.

⁷⁷ LUCAS MURILLO DE LA CUEVA, P., «Notas sobre el derecho fundamental...», *op.cit.*, pág. 677.

⁷⁸ ELVIRA PERALES, A., «¿Qué hay de nuevo en torno al derecho al secreto de las comunicaciones?», AA.VV., *La Constitución política de España. Estudios en homenaje a Manuel Aragón Reyes*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pág. 605; y RIDAURA MARTÍNEZ, M.J., «El legislador ausente del artículo 18.3...», *op.cit.*, pág. 375.

⁷⁹ ELVIRA PERALES, A., «¿Qué hay de nuevo en torno al derecho ...?», *op.cit.*, pág. 605. El entrecorillado corresponde a la STC 114/1984, de 29 de noviembre (FJ. 7).

⁸⁰ ELVIRA PERALES, A., «¿Qué hay de nuevo en torno al derecho ...?», *op.cit.*, pág. 605. En el mismo sentido se expresa RIDAURA MARTÍNEZ, para quien el correo «mientras esté

Un criterio similar, al menos en cuanto a su nivel de protección, ha sido el mantenido por la Fiscalía General del Estado. Si bien no se afirma indubitadamente que el acceso a mensajes y correos electrónicos ya leídos, pero archivados en el dispositivo, constituya una injerencia en el secreto de las comunicaciones, se considera necesario contar para su examen con autorización judicial⁸¹.

No obstante, este criterio ha sido jurisprudencialmente poco fecundo, salvo excepciones. Así, la Sentencia del Tribunal Supremo, Sala de lo Penal, de 5 de febrero de 2010 (FJ. 1), con base en la confusa jurisprudencia sobre los datos de tráfico motivada por una mejorable recepción de la jurisprudencia del TEDH, consideró que el acceso policial a los mensajes archivados en un teléfono móvil constituye una vulneración del derecho fundamental al secreto de las comunicaciones.

B. La protección de la comunicación hasta el conocimiento del contenido por el destinatario

Un segundo criterio para la aplicación de la garantía del artículo 18.3 CE se cifra en el conocimiento del contenido del mensaje por su receptor.

Este entendimiento nació ya en la pionera STC 114/1984, de 29 de noviembre, que, si bien *obiter dicta*, afirmaba la posibilidad de conculcar el derecho por el «simple conocimiento antijurídico de lo comunicado», añadiendo como ejemplo de lo anterior el de la apertura de la correspondencia ajena guardada por su destinatario, ampliado en resoluciones posteriores a los mensajes por correo electrónico o a través de telefonía móvil⁸².

protegido por clave de acceso creemos que constituye secreto de la comunicación», *vid.* RIDAURA MARTÍNEZ, M.J., «El legislador ausente del artículo 18.3...», *op.cit.*, pág. 375.

⁸¹ Circular de la Fiscalía General del Estado 1/2013, apdo. 5.6, pág. 30 (mensajes) y apdo. 10, pág. 49 (correos electrónicos).

⁸² SSTC 142/2012, de 2 de julio (FJ. 3); 241/2012, de 17 de diciembre (FJ. 4); y 115/2013, de 9 de mayo (FJ. 3).

Para esta posición, mayoritaria en la doctrina, la finalización del proceso comunicativo y, por tanto, de la eficacia del derecho, tiene lugar con la toma de conocimiento por parte del destinatario del contenido de la comunicación o, más bien, dada la dificultad de constatar el conocimiento efectivo, con el acceso al mensaje en términos que opera como presunción de conocimiento. La comunicación recibida pero no abierta es, para estos autores, comunicación en curso y, por tanto, amparada por el derecho fundamental al secreto de las comunicaciones. Una vez abierta o accedida, sin embargo, deberá acogerse a otros derechos como la intimidad o la protección de datos⁸³.

También este criterio ha sido ampliamente utilizado por la jurisprudencia de la Sala Segunda del Tribunal Supremo. Así, ha señalado que «los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones», ya que «la comunicación ha visto ya culminado su ciclo»⁸⁴.

Del mismo modo, la Fiscalía General del Estado ha afirmado rotundamente que «[d]esde luego, los mensajes enviados al destinatario pero aún no leídos por éste deben entenderse protegidos por el derecho al secreto de las comunicaciones»⁸⁵.

⁸³ FERNÁNDEZ RODRÍGUEZ, J. J., *Secreto e intervención de las comunicaciones...*, *op.cit.*, pág. 95. También en este sentido, JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 44 y ZOCO ZABALA, C., «Intervención de las comunicaciones e intervención de las conversaciones...», *op.cit.*, pág. 354.

⁸⁴ STS, Sala de lo Penal, de 17 de abril de 2013 (FJ. 8). En el mismo sentido, STS, Sala de lo Penal, de 27 de junio de 2002 (FJ. 3): «[...] la interferencia de la Policía en la comunicación [...] se produjo una vez consumado el proceso comunicativo del mensaje y de que el destinatario de éste hubiera tomado conocimiento de su contenido»; y SSTS, Sala de lo Penal, de 25 de noviembre de 2008 (FJ. 3), 24 de febrero de 2015 (FJ. 4), y 4 de diciembre de 2015 (FJ. 1).

⁸⁵ Circular de la Fiscalía General del Estado 1/2013, apdo. 5.6, pág. 29. Con el mismo criterio, para el caso del correo electrónico, *vid.* apdo. 10, pág. 48.

No obstante, el Tribunal Constitucional ha sido escasamente contundente en este sentido, no fijando con claridad el límite final de aplicación del derecho recogido en el artículo 18.3 CE, aunque no le han faltado oportunidades para ello⁸⁶.

En todo caso, más allá de la cita reproducida *supra*, el criterio de la apertura o lectura del mensaje por parte del destinatario parece desprenderse de alguna de sus resoluciones. Así, por ejemplo, en la STC 173/2011, de 7 de noviembre (FJ. 3), declaró que los correos electrónicos pueden estar protegidos por el derecho a la intimidad del artículo 18.1 CE «en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado».

C. La estricta limitación de la protección a la comunicación en tránsito y la participación del tercero

El criterio anterior, basado en la presunción de conocimiento del contenido comunicado por parte del destinatario, es irreprochable al menos en dos sentidos.

Por un lado, desde una noción general de comunicación, es sencillo convenir con los autores que lo defienden que el proceso de comunicación no termina hasta el momento en que se produce el acceso intelectual del destinatario al contenido del mensaje. En ese momento, la transmisión de información completa su curso⁸⁷.

⁸⁶ Especialmente ejemplificativas resultan las SSTC 241/2012, de 17 de diciembre, y 170/2013, de 7 de octubre. En ambos casos, pese a que los mensajes —intercambiados por chat y por correo electrónico, respectivamente— habían sido ya leídos por su destinatario, el Tribunal Constitucional resuelve la posible vulneración del derecho fundamental al secreto de las comunicaciones, sin embargo, con base en una confusa argumentación sobre el carácter abierto de la comunicación.

⁸⁷ VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, pág. 1623.

Por otro lado, es también difícilmente rebatible que, una vez abierto el mensaje y conocido su contenido, la comunicación deja de estar protegida por la garantía de secreto.

Lo que nos planteamos ahora es precisamente si el momento de la apertura del mensaje debe ser considerado en todo caso como el límite de exclusión del derecho o si, por el contrario, la coherencia de la norma iusfundamental exige adelantarlo a un momento previo.

Nos referimos a si la comunicación ya recibida, aunque no abierta ni leída por su destinatario, debe seguir protegida por el secreto de las comunicaciones o sí, por el contrario, la recepción supone ya finalización del proceso comunicativo en un sentido constitucional.

Esta segunda opción, que consideramos más adecuada, parece ser avalada por lo declarado en la STC 70/2002, de 3 de abril, cuando el Tribunal, en el Fundamento Jurídico 9, afirma que «la protección constitucional de lo *recibido* se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos»⁸⁸.

Del mismo modo que la noción constitucional de comunicación contiene unos contornos más estrictos que su definición general, una correcta interpretación de la norma conlleva que también los términos temporales en los que el derecho despliega su eficacia sean estrictamente delimitados.

Por tanto, consideramos que, al igual que la protección se inicia con la participación del tercero en el proceso comunicativo, también debe finalizar cuando el prestador del servicio deja de estar presente, lo que normalmente

⁸⁸ Cursiva añadida. En contra de esta afirmación, FRÍGOLS BRINES, E., «La protección constitucional de los datos de las comunicaciones...», *op.cit.*, págs. 62 y ss. También el TCFA ha interpretado en estos términos la eficacia temporal del derecho garantizado por el art. 10.1 GG, al afirmar que «[l]a protección del secreto de las telecomunicaciones termina cuando el mensaje llega al destinatario y el proceso de transmisión ha finalizado [...]. Los peligros específicos de la comunicación espacialmente distante no existen en el dominio del destinatario, que puede tomar sus propias medidas de protección contra el acceso no deseado a los datos», *BVerfGE* 115, 166, de 2 de marzo de 2006 (§73). En igual sentido, *BVerfGE* 120, 274-350, de 24 de febrero de 2008 (§185).

tiene lugar con la recepción de la carta o correo electrónico por parte de su destinatario⁸⁹.

También este criterio ha tenido eco en la jurisprudencia ordinaria, declarando el Tribunal Supremo que «[e]l derecho al secreto de las comunicaciones rige mientras se desarrolla el proceso de comunicación. Una vez cesado éste, *llegado el mensaje al receptor*, salimos del ámbito del art. 18.3 CE, sin perjuicio, en su caso, del derecho a la intimidad proclamado en el número 1 del mismo precepto»⁹⁰.

Esta interpretación salva, por un lado, los problemas para determinar tanto el conocimiento efectivo del mensaje por parte del destinatario, cuanto la apertura de la comunicación. Nótese que los nuevos formatos de comunicación ofrecen a sus usuarios una variada gama de modalidades de gestión de las comunicaciones que difuminan los criterios hasta ahora utilizados.

La tecnología actual permite reconducir mensajes accedidos y leídos a la previa condición de no leídos. O acceder al contenido de mensajes sin

⁸⁹ LUCAS MURILLO DE LA CUEVA, P., «Notas sobre el derecho fundamental...», *op.cit.*, pág. 677.

⁹⁰ STS, Sala de lo Penal, de 10 de diciembre de 2015 (FJ. 3); cursiva añadida. Resulta especialmente clara la explicación de la reciente STS, Sala de lo Penal, de 14 de octubre de 2019 (FJ. 1.3), que, por ello, reproducimos: «Las especiales características del instrumento técnico sobre el que se asentó la investigación judicial (*smartphone*) que, por un lado, permite la comunicación telemática en sus distintas modalidades de conversación oral o escrita y, aun en esta, por distintos instrumentos como son los mensajes electrónicos por *emails*, o la mensajería instantánea *sms* (*short message service*, por sus siglas en inglés) , o a través de plataformas de comunicación específicas como *WhatsApp* o *telegram*, y que por otro lado realiza un registro de todos los datos referidos a estas conversaciones, además de otras circunstancias que dependen de la configuración personal del usuario, tales como fotografías, vídeos, historial de geolocalización, navegación por internet, o el rastro de las distintas iniciativas que haya impulsado el usuario durante la utilización de las distintas utilidades o aplicaciones informáticas que tenga instaladas, justifica principiar por la aclaración, ya reiterada en numerosas sentencia de esta Sala, que distingue entre las comunicaciones en marcha, de aquellos otros procesos de correspondencia o de relación que ya están cerrados. Solo las primeras se encuentran afectadas por el derecho al secreto de las comunicaciones, mientras que aquellas que terminaron y cuya existencia presente deriva de un proceso técnico o electrónico de conservación o documentación, a lo que conciernen es al derecho a la intimidad y/o, en su caso, a la autodeterminación informativa mediante el control de datos personales».

recurrir al protocolo de apertura estándar que acredita su apertura y acceso⁹¹. O, también, en sistemas comunicativos que soportan archivos diversos — como texto, imagen, video o audio—, lo que sucede en aplicaciones de intercambio de mensajería instantánea (como *WhatsApp*), la posibilidad de tomar conocimiento parcial, es decir, sólo de determinados contenidos⁹².

Pero, sobre todo, esta es la interpretación más coherente y ajustada a la naturaleza constitucional del derecho. El Tribunal Constitucional ha declarado que la específica protección constitucional de este derecho «reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación»⁹³.

De este modo, y al igual que lo señalado para el inicio del proceso comunicativo, parece lógico que la garantía de secreto venga únicamente orientada a contrarrestar la vulnerabilidad de las comunicaciones mientras se soportan por el medio técnico⁹⁴.

Dicha vulnerabilidad está vinculada a la idea de *dominio* sobre la comunicación. Mientras la comunicación transita, los comunicantes pierden el control en favor del prestador del soporte, pero, recibido el mensaje, y con independencia del momento en que acceda a su contenido, el destinatario recupera el control sobre la comunicación y sólo a él corresponde defender su confidencialidad⁹⁵.

⁹¹ Nos referimos a la posibilidad de leer, desde un *smartphone* o *tablet*, los mensajes recibidos desde la barra de notificaciones o mediante un sistema de notificaciones emergentes — así como a través de los cada vez más utilizados relojes inteligentes— y sin que sea necesario, por tanto, acceder al programa de gestión de la comunicación, permaneciendo el mensaje, desde un punto de vista informático, como «no leído».

⁹² Por ejemplo, acceder a los mensajes intercambiados en un chat, pero sin descargar o reproducir los archivos de audio o video que se insertan en la conversación.

⁹³ SSTC 123/2002, de 20 de mayo (FJ. 5) y 281/2006, de 9 de octubre (FJ. 3).

⁹⁴ VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, pág. 1618.

⁹⁵ *Ibidem*, pág. 1623.

Con la recepción nace para el destinatario la posibilidad de conservar o deshacerse del mensaje⁹⁶. Por tanto, desaparecido el riesgo que supone la pérdida del control de la comunicación, no existe ya una justificación razonable para la garantía formal de secreto. La comunicación recibida en nada se distingue ya del resto de documentación o información a disposición de su titular que, aunque se trate de información sensible o esté protegida mediante los estándares al uso, encontrará protección en otros derechos como la intimidad o la inviolabilidad del domicilio⁹⁷.

Por la misma razón, también deberá considerarse protegida por el secreto de las comunicaciones la intervención que tenga lugar en el mismo momento de recepción de la comunicación por su destinatario, lo que se produce, por ejemplo, en los casos de registro remoto de dispositivos comunicativos y en los que el receptor no tiene posibilidad alguna de decidir el destino de la comunicación, pues recibe la comunicación de forma simultánea al sujeto que la interviene⁹⁸.

Esta idea de control parece estar presente también en alguna resolución del Tribunal Supremo, al afirmar que «[l]as copias de los mensajes recibidos y transmitidos por la menor, *que pueden ser borrados del terminal una vez leídos pero fueron guardados*, equivalen a la correspondencia que pueda ser conservada por la menor entre sus papeles privados»⁹⁹.

⁹⁶ RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, págs. 36.

⁹⁷ RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho...», *op.cit.*, pág. 4. Sobre ello se ha dicho, con razón, que hoy en día los contenidos comunicados a menudo se almacenan en servidores de proveedores de servicios de comunicación, incluso después de que los comunicantes hayan eliminado el rastro de la comunicación del programa de gestión. *Vid.* ZUIDERVEEN BORGESIU, F.J., y STEENBRUGGEN, W., «The right to communications confidentiality...», *op.cit.*, págs. 318 y ss. No obstante, añadimos, esta información conservada por los proveedores de servicios de comunicaciones no encuentra, una vez transmitida, diferencias reseñables con otros contenidos que se hallan en poder de terceros —datos bancarios o archivos almacenados en la *nube*— que la convierta en merecedora de la protección formal de secreto.

⁹⁸ *Vid. infra*, Capítulo tercero, apdo. III.3.

⁹⁹ STS, Sala de lo Penal, de 26 de noviembre de 2014 (FJ. 9); cursiva añadida.

La eficacia del derecho ajustada al tiempo en que la comunicación se encuentra en poder de un tercero está presente, además, desde sus primeros reconocimientos constitucionales, ya que, al proclamarse típicamente la inviolabilidad de la correspondencia «confiada al correo» se protege «en aquel momento en el que se muestra más vulnerable: mientras se encuentra en tránsito y bajo la custodia de un servicio postal generalmente dependiente del poder público»¹⁰⁰.

Cabe por tanto concluir que el derecho fundamental al secreto de las comunicaciones protege, estrictamente, frente a la *intercepción* de comunicaciones por parte de terceros durante su transmisión, consista ésta en la mera interrupción del curso normal del proceso comunicativo, o en la toma de conocimiento de la existencia de la comunicación, de su contenido o de otros datos generados por el acto de transmisión (identificación de los comunicantes, duración, etc.)¹⁰¹.

El acceso a las comunicaciones ya recibidas estará protegido, en su caso, por las normas que tutelan los derechos bien a la intimidad o bien a la protección de datos personales, según dicha información se encuentre, respectivamente, en poder del destinatario o en poder de terceros — generalmente el prestador del servicio—¹⁰².

¹⁰⁰ RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho...», *op.cit.*, pág. 9.

¹⁰¹ El secreto se garantiza frente a las acciones que supongan, en puridad, «interceptar», en el sentido de «apoderarse de algo antes de que llegue a su destino» —*Diccionario de la lengua española*—. Interceptación sería, así, la «aprehensión oculta, en tiempo real, de una comunicación en curso entre dos o más personas por parte de otro sujeto, ajeno al coloquio», *vid.* USAI, S., «Registrazione di conversazione tra privati: per attività di PG necessaria l'autorizzazione», *Sigurezza e Giustizia*, 2, 2015, pág. 14. El confusionismo reinante en la relación entre alcance temporal del derecho y contenidos protegidos ha tenido especial incidencia, como veremos, en la eficacia del derecho respecto de los denominados datos de tráfico asociados a las comunicaciones. *Vid. infra*, Capítulo cuarto.

¹⁰² Especialmente expresiva de la distinción entre estas dos conductas se muestra la *Electronic Communications Privacy Act* estadounidense, que distingue entre la interceptación de mensajes en tránsito (Título I) y el acceso a la información almacenada electrónicamente (Título II). Cfr. TINTO GIMBERNAT, M., «El secreto de las comunicaciones electrónicas en los ordenamientos jurídicos español y norteamericano», DAVARA RODRÍGUEZ, M.A. (coord.), *III Jornadas sobre informática y sociedad*, Universidad Pontificia Comillas, Madrid, 2001, págs. 251-257.

III. MODALIDADES COMUNICATIVAS PROTEGIDAS

En el presente apartado se pretende aplicar, siquiera brevemente, las consideraciones realizadas a las diferentes modalidades comunicativas protegidas por el derecho fundamental objeto de estudio.

III.1. Comunicaciones postales y telegráficas

La creación de un servicio postal y la prevención frente a sus abusos está en la génesis inicial del derecho al secreto de las comunicaciones.

No obstante, el hecho de que el constituyente español estableciese como protegidas las comunicaciones postales, en lugar de aludir al término más común de correspondencia, ha provocado algunas dudas, tanto en la doctrina como en la jurisprudencia, sobre la inclusión en el objeto del derecho del envío de paquetes postales.

La Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal (en adelante, LSPU), diferencia en sus definiciones entre «envío postal» y «envío de correspondencia».

Así, mientras que el primer término, de carácter más amplio, se define como «todo objeto destinado a ser expedido a la dirección indicada por el remitente» e incluye, expresamente, los paquetes postales, el envío de correspondencia se limita a «la *comunicación* materializada en forma escrita sobre un soporte físico de cualquier naturaleza» (art. 3.3 LSPU).

Por su parte, si bien el artículo 6 LSPU proclama la inviolabilidad —en términos de fidelidad en la custodia y gestión— de todos los envíos postales, su artículo 5 restringe la garantía de secreto solamente a las «comunicaciones postales»¹⁰³.

¹⁰³ «Se considerará incumplimiento de dicho deber la detención contraria a derecho, el intencionado curso anormal, la apertura ilegal, la sustracción, la destrucción, la retención indebida y la ocultación de los citados envíos postales» (art. 5.1 LSPU).

Una interpretación integrada de los artículos citados deriva necesariamente en la comprensión de que los únicos envíos postales cubiertos por el secreto son aquellos que adoptan la forma de correspondencia, por ser ésta, según las definiciones de la propia norma, comunicación.

Jurisprudencialmente, y pese al basamento normativo existente, la exclusión de los paquetes postales del objeto garantizado por el artículo 18.3 CE no ha sido cuestión pacífica¹⁰⁴.

Así, la tesis dominante en las primeras resoluciones del Tribunal Supremo, tras la entrada en vigor de la Constitución, se inclinó por considerar de aplicación a los paquetes postales la garantía de secreto del artículo 18.3 CE.

La STS, Sala de lo Penal, de 25 de junio de 1993 (FJ. 3), afirmaba en este sentido que «[l]a correspondencia postal a la que alude la CE y la LECrim se refiere a todos aquellos envíos que puedan facturarse utilizando la vía del servicio postal de correos y por extensión de entidades privadas que ofrezcan análogos servicios», y añadía «[b]ajo la protección del derecho a la intimidad [síc] se encuentran no solamente las cartas o correspondencia personal, sino todo género de correspondencia postal, como dice textualmente la CE y la LECrim, ya que a su través se pueden enviar mensajes o efectos personales de carácter confidencial que están asimismo bajo la salvaguarda del derecho fundamental»¹⁰⁵.

Pese a la existencia de algunas resoluciones que, con mejor criterio, excluían a los paquetes postales del ámbito de aplicación del artículo 18.3

¹⁰⁴ El art. 10 del Decreto 1653/1964, de 14 de mayo, por el que se aprueba el Reglamento de los Servicios de Correos, al diferenciar las categorías de envíos postales, establecía ya que «las cartas y tarjetas postales constituyen la llamada correspondencia epistolar y forman una categoría de envíos postales», y, en similar sentido que la norma actual, sólo a esta correspondencia atribuía la garantía de secreto (art. 27).

¹⁰⁵ Igualmente, v.gr., SSTS, Sala de lo Penal, de 19 de noviembre de 1994 (FJ. 4); de 23 de diciembre de 1994 (FJ. 6); y de 13 de marzo de 1995 (FJ. 2).

CE¹⁰⁶, el Acuerdo no jurisdiccional de la Sala Segunda del Tribunal Supremo de 4 de abril de 1995 ratificó el parecer mayoritario de considerarlos protegidos, si bien afirmando que «el reconocimiento de los envíos postales puede ejecutarse de oficio y sin formalidades especiales sobre objetos abiertos y sobre cuantos ostenten etiqueta verde».

Contrariamente, y salvo algunas excepciones¹⁰⁷, la doctrina científica mayoritaria consideró que el artículo 18.3 CE no garantizaba un derecho fundamental al secreto postal, sino que la referencia a las comunicaciones postales debía entenderse en términos más estrictos, asemejándose al concepto de correspondencia epistolar y, por tanto, excluyente de los paquetes postales donde «no existe “comunicación”, sino simple transporte»¹⁰⁸.

Por su parte, el Tribunal Constitucional, si bien parece reconocer implícitamente el secreto de los paquetes postales en la STC 137/2002, de 3 de junio (FJ. 3), no realiza un examen de fondo hasta la STC 281/2006, de 9 de octubre.

Esta resolución viene a recoger, en su fundamento jurídico 3, la opinión de la doctrina, afirmando en este sentido que «[l]a noción constitucional de comunicación postal es [...] una noción restringida que no incluye todo intercambio realizado mediante los servicios postales» y, por tanto, el secreto

¹⁰⁶ «[...] correspondencia equivale a comunicación por escrito de una persona con otra, y en cuanto tal comunicación se produzca deberá estimarse la existencia de aquélla. Ahora bien, obviamente la remisión de unos paquetes, aunque se efectúan a través del servicio de Correos, no pueden transformar lo que en sí no es más que un transporte de mercancía, aunque se haya elegido aquél medio, y convertirlo en correspondencia». STS, Sala de lo Penal, de 10 de marzo de 1989 (FJ. 2).

¹⁰⁷ «[...] el paquete postal, bien sea enviado a través del servicio de correos o por mensajería privada, es también vía idónea para transmitir cualquier tipo de mensaje o comunicación, que sí deben quedar protegidos, sin que quepa diferenciar a priori el contenido». DÍAZ REVORIO, F.J., «El derecho fundamental al secreto de las comunicaciones», *op.cit.*, pág. 163.

¹⁰⁸ VEGAS TORRES, J., «Detención y apertura de paquetes postales. Especial consideración de la apertura de paquetes en el marco de las entregas vigiladas», *Tribunales de Justicia*, 8-9, 1997, pág. 851. También, JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 47; y MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 54.

«sólo protege el intercambio de objetos a través de los cuales se transmiten mensajes mediante signos lingüísticos»¹⁰⁹.

La correspondencia epistolar —término inclusivo de cartas y tarjetas postales— es, por tanto, la comunicación postal protegida por la garantía de secreto del artículo 18.3 CE, ya que, además de su expresa mención en este precepto y en otras normas infraconstitucionales, estamos ante un soporte generalmente reconocido como apto para transmitir expresiones de sentido entre personas previamente determinadas¹¹⁰.

Respecto a su alcance temporal, según dijimos, la norma cubrirá todas las fases del curso de la comunicación desde que es depositada por el emisor en el servicio postal hasta que es entregada a su destinatario.

Finalmente, resta hacer una breve referencia a las comunicaciones telegráficas, ya que, si bien son prácticamente residuales, se trata de una de las formas de comunicación expresamente mencionadas en la norma iusfundamental.

Las comunicaciones telegráficas intercambian mensajes codificados — a través de código morse— mediante impulsos eléctricos.

Este tipo de comunicación contiene, por tanto, las características determinantes para beneficiarse de la garantía de secreto. No obstante, más allá de que la información discorra a través de un canal, en principio técnicamente cerrado, la comunicación telegráfica cuenta con la singularidad de requerir para su buen fin de la intervención de otras personas —los

¹⁰⁹ Esta doctrina fue, como no podía ser de otra forma, asumida por el Tribunal Supremo a partir de la Sentencia, de la Sala de lo Penal, de 20 de febrero de 2007 (FJ. 2). Sobre la evolución de la jurisprudencia del Tribunal Supremo en relación con la aplicación del secreto de las comunicaciones a los paquetes postales, *vid.* HERNÁNDEZ DOMÍNGUEZ, J.J., «Apertura de paquetes postales. Alcance del secreto de las comunicaciones», *Diario La Ley*, 8265, 2014, págs. 1-12.

¹¹⁰ Pese a que las características de las tarjetas postales permiten una mayor accesibilidad a su contenido deben considerarse como comunicación protegida, constituyendo «una evidente vulneración del derecho su lectura, copia o examen intencionado antes de que llegue al receptor». Cfr. BELDA PÉREZ-PEDRERO, E., «El derecho al secreto de las comunicaciones», *op.cit.*, pág. 178.

telegrafistas que se ocupan de enviar, descodificar y entregar el mensaje— que van a tener acceso al contenido íntegro de la comunicación¹¹¹.

Por ello, el carácter cerrado del canal debe venir complementado en este caso por un férreo deber de confidencialidad de los telegrafistas, cuestión que ha sido históricamente prevista en normas de régimen interno y acompañadas de un severo régimen disciplinario¹¹².

También estas comunicaciones cuentan con una especialidad en la fase de intervención judicial de su contenido, ya que no se produce en este caso una interceptación de la comunicación en sentido estricto, esto es, mientras la misma está en tránsito, sino que el acceso a las mismas se produce mediante la facilitación por parte del servicio telegráfico de las copias de los telegramas solicitados¹¹³.

III.2. Comunicaciones bidireccionales simultaneas

El artículo 18.3 CE otorga también protección expresa a las comunicaciones telefónicas y, pese a que el art. 8.1 CEDH sólo se refiere explícitamente a la correspondencia, el TEDH ha interpretado que en ese término quedarían igualmente incluidas las comunicaciones telefónicas (Sentencia de 6 de septiembre de 1978, *Klass y otros c. Alemania*)¹¹⁴.

¹¹¹ BELDA PÉREZ-PEDRERO, E., «El derecho al secreto de las comunicaciones», *op.cit.*, pág. 179.

¹¹² Así, por ejemplo, el Reglamento Orgánico del cuerpo y servicio de Telégrafos de 31 de marzo de 1856 establecía en su art. 116 el deber de todo el personal de prestar juramento de «guardar secreto acerca de las comunicaciones y documentos que se les confíen»; mientras que el art. 58 disponía que «[e]l Telegrafista que revelare á persona que no sea su Jefe el contenido de cualquier comunicación telegráfica que reciba ó trasmita, aunque sea de asunto insignificante y no reservado por su índole, será irremisiblemente castigado con la destitución, sin perjuicio de lo que judicialmente proceda».

¹¹³ ALONSO PÉREZ, F., *Intervención de las comunicaciones postales, telegráficas y telefónicas*, Dykinson, Madrid, 2001, pág. 47.

¹¹⁴ «Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision» (§41).

Ello sentado, a nuestro juicio, existen además similitudes suficientes que justifican abordar conjuntamente con ellas otras comunicaciones bidireccionales simultáneas, como las videoconferencias o videollamadas¹¹⁵.

Nos referimos ahora, por tanto, a aquellas comunicaciones que permiten el intercambio sincrónico de audio —llamadas— o audio y video —videollamadas— entre dos o más personas determinadas; y ello con independencia de la tecnología utilizada, siempre que se realicen por canal cerrado.

Así, forman parte de esta categoría tanto la comunicación telefónica tradicional —red fija cableada—, como la telefonía móvil o celular —inalámbrica mediante ondas electromagnéticas— y la telefonía y videotelefonía a través de Internet —voz y audio sobre IP—, hoy ampliamente utilizadas a través de determinadas funcionalidades que ofrecen plataformas como *Skype*, *WhatsApp* o *Telegram*.

Pocas objeciones se pueden realizar a la inclusión de estas comunicaciones en la noción de comunicación cuyo secreto garantiza el derecho fundamental, más allá de algunos reparos frente a la telefonía móvil en sus inicios.

La Sentencia de la Sala Segunda del Tribunal Supremo, de 8 de febrero de 1999, determinó respecto de las comunicaciones telefónicas que «[e]l ámbito de protección de este medio de comunicación, no tiene limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse. No sólo la primitiva telefonía por hilos sino también las modernas formas de interconexión por satélite o cualquier otra señal de comunicación a través de las ondas, se encuentran bajo la tutela judicial».

¹¹⁵ El artículo 2.31 de la Directiva 2018/1972, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas define el término *llamada* como «una conexión establecida por medio de un servicio de comunicaciones interpersonales disponible para el público que permita la comunicación de voz bidireccional».

Del mismo modo, el Tribunal Constitucional, si bien respecto del delito de escuchas ilegales, afirmó que «las comunicaciones enabladadas por telefonía móvil automática deben ser consideradas comunicaciones telefónicas: el teléfono inalámbrico de estas características es eso, un teléfono, aunque el sonido no se transmita por cable»¹¹⁶.

Supuesto distinto es, como ya hemos visto, el de las comunicaciones realizadas mediante radioteléfonos a través de frecuencias de uso público y las videoconferencias que, aunque dirigidas a destinatarios predeterminados, se realizan en sentido unidireccional.

En cuanto a la delimitación del alcance temporal protegido, las comunicaciones bidireccionales, en tanto que sincrónicas, no plantean tampoco grandes problemas. Su proceso de comunicación tendrá lugar desde que el emisor efectúa la llamada hasta que ambos desactivan el soporte.

También quedan protegidas por este derecho, en la medida en que no sólo protege el contenido sino la comunicación misma, las llamadas telefónicas infructuosas —o «llamadas perdidas»—, aquellas en las que, iniciada la comunicación por el emisor, no se obtiene réplica por parte de su destinatario¹¹⁷.

Las principales dificultades han surgido en este caso en dos frentes a los que nos dedicaremos en los siguientes capítulos de este trabajo. Por un lado, el de la inclusión en el espacio garantizado de los denominados datos de tráfico asociados a estas comunicaciones y, por otro, el de los problemas en el alzamiento judicial del secreto generados por la ausencia, hoy colmada, de un completo desarrollo legislativo sobre los criterios de injerencia.

¹¹⁶ STC 34/1996, de 11 de marzo (FJ. 5).

¹¹⁷ LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, La Ley, Madrid, 2011, pág. 66. Igualmente deben considerarse protegidas las llamadas que, no siendo contestadas por el destinatario, su contenido es registrado por el emisor en un buzón de voz o contestador automático. No obstante, el acceso al resultado de la comunicación, a la grabación del mensaje efectuada en dicho contestador, debe considerarse excluido del derecho aquí considerado, ya que el proceso comunicativo ha finalizado.

III.3. Comunicaciones telemáticas alternativas

En el apartado anterior hemos hecho referencia ya a determinadas realidades, como el intercambio de audio y video por IP, que, aunque responden a la estructura de las comunicaciones telefónicas —e incluso pueden utilizar como soporte un teléfono—, son realmente comunicaciones telemáticas, categoría que incluye aquellos fenómenos en los que participa un sistema informático en el curso de la comunicación¹¹⁸.

Se trata ahora de analizar otras comunicaciones, inclusivas de dicha categoría, cuyas características son más cercanas a la correspondencia y la telegrafía, ya que el intercambio de información se produce de forma alternativa y, usualmente, de forma escrita.

Nos referimos tanto al correo electrónico como a las plataformas de intercambio de mensajería instantánea. Además, y pese a las dudas que puede generar su calificación como telemáticas, incluimos también aquí, por su analogía estructural con el *email*, las comunicaciones que se producen mediante los sistemas de *Short Message Service* (SMS) y *Multimedia Messaging Service* (MMS).

A todos estos fenómenos y a los que depare el futuro tecnológico, siempre que cumplan con los requisitos que hemos considerado determinantes en la noción constitucional de comunicación, son a los que se refiere el Tribunal Constitucional cuando afirma que «los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del

¹¹⁸ La intervención de comunicaciones telemáticas se encuentra hoy regulada, junto a las telefónicas, en los arts. 588 ter.a y ss. LECRIM. Sobre los problemas de distinción entre ambas clases de comunicación, *vid.* Circular de la Fiscalía General del Estado 2/2019, apdo. 2, págs. 5-6.

objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos»¹¹⁹.

Ciertamente, en las comunicaciones mantenidas a través del correo electrónico se verifican las condiciones de intersubjetividad, predeterminación de los destinatarios, intermediación técnica de un tercero y transmisión por canal cerrado.

Constituye, por tanto, una forma de comunicación privada y, en este sentido, debe entenderse protegida por el secreto garantizado en la norma constitucional, habiendo sido así reconocido, sin mayores problemas, por la jurisprudencia y la doctrina científica¹²⁰.

Así, diversas sentencias del Tribunal Constitucional han reconocido que el derecho fundamental al secreto de las comunicaciones puede resultar vulnerado por la apertura de «un mensaje emitido por correo electrónico o a través de telefonía móvil»¹²¹.

Igualmente, la STC 170/2013, de 7 de octubre, si bien enjuicia un supuesto de acceso a mensajes de correo electrónico, no expresa valoración alguna sobre la inclusión de este medio en la noción constitucional de comunicación, más allá de afirmar que con la protección de este derecho «se pretende que todas las comunicaciones —*incluidas las electrónicas*— puedan realizarse con libertad»¹²².

Similares consideraciones pueden realizarse sobre los mensajes enviados a través de telefonía móvil, ya que se trata en ambos casos de intercambios de texto (SMS) u otros contenidos (MMS) que quedan a

¹¹⁹ STC 70/2002, de 3 de abril (FJ. 9).

¹²⁰ HERNÁNDEZ GUERRERO, F.J., «La intervención de las comunicaciones electrónicas», *Estudios Jurídicos del Ministerio Fiscal*, 3, 2001, pág. 412 y GARCÍA RUIZ, J.M., «Correo electrónico y proceso penal», *Diario La Ley*, 5805, 2003, pág. 9.

¹²¹ SSTC 142/2012, de 2 de julio (FJ. 3), 241/2012, de 17 de diciembre (FJ. 4), y 115/2013, de 9 de mayo (FJ. 3).

¹²² Cursiva añadida. También la Circular de la Fiscalía General del Estado 1/2013 señala que «[e]l correo electrónico es un medio de comunicación y los concretos mensajes de correo electrónico, son actos de comunicación» (apdo. 10, pág. 48).

disposición del destinatario hasta que éste accede a la aplicación que los alberga¹²³.

Sobre este tipo de mensajes se ha pronunciado el Tribunal Supremo, para el que «estamos, sin duda, ante auténticas y genuinas comunicaciones personales, similares a las que se remiten y reciben por correo o telégrafo, pero cuyo vehículo de transmisión en este supuesto, es el teléfono, por lo que, de hecho, se trata de una especie de comunicación de una misiva personal efectuada vía telefónica, que no se “oye” por su destinatario, sino que se “lee” al aparecer en la pantalla del aparato y mediante esa lectura se conoce el contenido del mensaje o de la misiva, por lo que resulta incuestionable que esta clase de comunicaciones se encuentran tuteladas por el secreto que establece el art. 18.3 CE»¹²⁴.

Finalmente, también debe entenderse garantizado el secreto de las comunicaciones intercambiadas a través de aquellas plataformas de mensajería instantánea que se llevan a cabo entre personas previamente determinadas, con independencia del mayor o menor número de destinatarios¹²⁵.

De esta categoría forman parte no sólo las comunicaciones que se producen mediante aplicaciones —tantas veces aludidas— cuya función principal es precisamente el intercambio de mensajes —*WhatsApp*, *Telegram*, *Skype* o *WeChat*—, sino también las llevadas a cabo a través de plataformas con fines divulgativos, pero que permiten además el intercambio de mensajes

¹²³ La definición que hace la Directiva 2002/58/CE sobre «correo electrónico» se expresa en términos tan amplios que pudieran entenderse incluidos en ella tanto la mensajería a través de telefonía móvil como los chats de mensajería instantánea: «todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo» (art. 2.h.).

¹²⁴ STS, Sala de lo Penal, de 27 de junio de 2002 (FJ. 2).

¹²⁵ Diversos autores entienden que estas comunicaciones forman parte del ámbito protegido por el derecho. *Vid.* ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 46 y LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, *op.cit.*, pág. 79.

entre personas determinadas, como sucede en la aplicación *Messenger* de la red social *Facebook* o en los denominados «mensajes directos» de *Twitter* o *Instagram*.

Por su parte, el Tribunal Constitucional sólo se ha enfrentado en una ocasión a una supuesta vulneración del art. 18.3 CE por el acceso a comunicaciones que habían sido mantenidas por un programa de intercambio de mensajería instantánea (denominado *Trillian*), reconociendo implícitamente que este tipo de comunicaciones forman parte del concepto protegido por el derecho¹²⁶.

También las referencias son escasas en la jurisprudencia del Tribunal Supremo, aunque se ha afirmado, si bien *obiter dicta*, que «los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas»¹²⁷.

El proceso comunicativo protegido en estas formas de comunicación se extiende desde que el emisor envía el mensaje hasta que este es recibido por el destinatario, esto es, cubre estrictamente la comunicación en tránsito, con independencia, por tanto, del momento en que se acceda su contenido, que quedará, desde su recepción, bajo la tutela de otros derechos.

¹²⁶ STC 241/2012, de 17 de diciembre.

¹²⁷ STS, Sala de lo Penal, de 2 de abril de 2014 (FJ. 5). También la Fiscalía General del Estado ha entendido que el régimen de protección de los correos electrónicos debe aplicarse «a las diversas modalidades de mensajería instantánea (*instant messaging*) cuyo uso generalizado ha colocado a este medio en pieza esencial en las comunicaciones interpersonales (*v.gr. whatsapp* o *messenger*)». Circular de la Fiscalía General del Estado 1/2013, apdo. 10, pág. 48.

CAPÍTULO TERCERO

EL SECRETO CONSTITUCIONALMENTE PROTEGIDO

I. EL SECRETO EN EL ORDENAMIENTO JURÍDICO

- A. Secreto como límite al conocimiento
- B. Secreto como concepto relacional
- C. Secreto como atribución normativa de carácter teleológico
- D. El secreto presenta una doble dimensión imperfecta

II. OBJETO DEL DERECHO: EL SECRETO —¿Y LA LIBERTAD?— DE LAS COMUNICACIONES

II.1. El secreto de las comunicaciones

- A. Ámbito objetivo del secreto
- B. Dimensión temporal del secreto
- C. Ámbito subjetivo del secreto
- D. El deber de confidencialidad del prestador del servicio

II.2. La libertad de las comunicaciones

- A. Libertad de las comunicaciones expresamente garantizada
- B. Delimitación de la libertad de las comunicaciones
 - B.1. Libertad de las comunicaciones como derecho al medio o servicio de comunicaciones
 - B.2. Libertad de las comunicaciones como libertad de acción
 - B.3. Libertad de las comunicaciones como prohibición de alterar su curso normal
 - B.4. Libertad de las comunicaciones como libertad para compartir expresiones de sentido exclusivamente con sujetos determinados

III. EL SECRETO TECNOLÓGICAMENTE GARANTIZADO

III.1. El cifrado de comunicaciones

III.2. Incidencia del cifrado en el derecho fundamental al secreto de las comunicaciones

III.3. Intervención de comunicaciones cifradas

- A. Interceptación del contenido comunicacional mediante ataques de suplantación
- B. Remoción de las técnicas de cifrado con auxilio de terceros
- C. Descifrado mediante técnicas de criptoanálisis
- D. Registro remoto de dispositivos como técnica de intervención de comunicaciones

I. EL SECRETO EN EL ORDENAMIENTO JURÍDICO

La noción jurídica de secreto es extremadamente compleja, como lo acredita la diversidad de posiciones doctrinales sobre su concepto, todas en cambio unánimes en afirmar su dificultad¹.

Se le ha motejado así como «uno de los conceptos jurídicos más atormentados e inciertos»². La complejidad se incrementa, además, por la diversidad de subcategorías que el ordenamiento contiene bajo un único término: secreto profesional, secretos de empresa, secretos oficiales, secreto de sumario, etc., lo que ha llevado a negar la posibilidad de construir «un concepto unitario de secreto»³.

No siendo tal problema dogmático el que directamente nos ocupa, sí que será preciso en nuestro estudio deducir algunas características del secreto que parecen comunes en sus múltiples usos por el ordenamiento.

A. Secreto como límite al conocimiento

Frente a la complejidad de la acepción jurídica de secreto se ha puesto de manifiesto, por el contrario, la claridad de su acepción común⁴.

¹ Como se ha dicho, «[r]esulta significativo que la doctrina sólo parezca ponerse de acuerdo en admitir la dificultad de lograr una definición satisfactoria». MORÓN LERMA, E., *El Secreto de Empresa: Protección Penal y Retos que Plantea ante las Nuevas Tecnologías*, Aranzadi, Cizur Menor, 2002, pág. 39.

² ITALIA, V., *Libertà e segretezza della corrispondenza...*, *op.cit.*, pág. 66.

³ MORENO CATENA, V.M., *El secreto en la prueba de testigos del proceso penal*, Montecorvo, Madrid, 1980, pág. 77.

⁴ «[P]ocas nociones habrá tan claras en su acepción vulgar e ingenua, pero asimismo tan oscuras y disputadas en lo jurídico como la del secreto», *vid.* OLMO FERNÁNDEZ-DELGADO,

Secreto es, como sustantivo, la «cosa que cuidadosamente se tiene reservada y oculta» y, como adjetivo, aquello que está «oculto, ignorado, escondido y separado de la vista o del conocimiento de los demás»⁵.

Del mismo modo, etimológicamente «secreto» procede del verbo latino *secernere*, que significa «separar, distinguir, poner a parte»⁶.

Por tanto, la ocultación, la existencia de un pretendido impedimento a la toma de conocimiento, es la principal característica del secreto⁷.

B. Secreto como concepto relacional

De estas definiciones se deriva también otra característica fundamental: el secreto posee una naturaleza relacional, transitiva.

El conocimiento se mantiene oculto siempre y en todo caso respecto de alguien y algo. El secreto consiste, así, en una «limitación a la cognoscibilidad ajena»⁸.

Hablar de secreto presupone, por tanto, una pluralidad de sujetos. Por un lado, aquellos que poseen el conocimiento y, por otro, aquellos respecto

L., *El descubrimiento y revelación de secretos documentales y de las telecomunicaciones. Estudio del artículo 197.1º del Código Penal*, Dykinson, Madrid, 2009, pág. 105.

⁵ *Diccionario de la lengua española*, Real Academia Española.

⁶ Cfr. la voz «secreto» en GÓMEZ DE SILVA, G., *Breve diccionario etimológico de la lengua española*, México: Fondo de Cultura Económica, México D.F., 1998.

⁷ La referencia a la ocultación y reserva en la voz «*secreto*» se encuentra en todos los diccionarios de la Real Academia Española desde su aparición en 1780 —«Silencio cuidadoso de no revelar ni descubrir lo que conviene que esté oculto. La misma especie, o cosa, que se debe tener oculta, o callada»—, y aún antes, en casi idéntica redacción, en el conocido como *Diccionario de autoridades* de 1739. Esta definición del término se mantuvo con igual redacción hasta la décima edición, a partir de la cual se define como «Lo que cuidadosamente se tiene reservado y oculto», permaneciendo inmutable hasta la vigésima segunda edición (2001) en la que se adopta la actual definición. *Vid.* Nuevo tesoro lexicográfico (Disponible en: <http://www.rae.es/recursos/diccionarios/diccionarios-antiguos-1726-1992/nuevo-tesoro-lexicografico>). También la idea de ocultación está presente en el *Diccionario Ideológico de la Lengua Española*, que define la voz «*secreto*» como «Lo que se tiene reservado y oculto». Cfr. CASARES SÁNCHEZ, J., *Diccionario Ideológico de la Lengua Española*, Editorial Gustavo Gili, Barcelona, 1990.

⁸ MORENO CATENA, V.M., *El secreto en la prueba de testigos...*, *op.cit.*, pág. 78.

de los cuales se mantiene oculto⁹. La estructura del secreto exige pues transitividad: «el secreto es la ocultación de algo, pero con referencia a otros»¹⁰.

La estructura del secreto resulta así relacional y divisiva, porque exige la presencia de dos elementos: quien conoce y quien no conoce. De tal modo que, en la mayoría de las ocasiones en que el ordenamiento jurídico recurre al secreto, lo hace con el objetivo de proteger —o excepcionar de protección— un conocimiento poseído por diversas personas: el cliente y el abogado, el paciente y el médico, el periodista y el informante, etc.¹¹

Con todo, no es necesario que el conocimiento recaiga sobre una pluralidad de personas para que el ordenamiento lo proteja a través del secreto¹². En este sentido, por ejemplo, cuando la Constitución otorga al sufragio el carácter de «secreto» —arts. 68.1, 69.1 y 140— está protegiendo la ocultación de un conocimiento que solo el titular del derecho posee, cual es el sentido de su voto. La garantía del carácter secreto del sufragio —características técnicas de sobres y papeletas electorales, cabinas en el colegio electoral...— brindan al elector los recursos para asegurar su voluntad de mantener —o no— el secreto de su voto.

⁹ MORÓN LERMA, E., *El Secreto de Empresa...*, *op.cit.*, pág. 41.

¹⁰ OLMO FERNÁNDEZ-DELGADO, L., *El descubrimiento y revelación de secretos...*, *op.cit.*, pág. 105. Este carácter relacional se ve claramente en las definiciones que sobre esta voz ofrecen algunos diccionarios. Así, por ejemplo, cuando se nos dice que *secreto* —como adjetivo— «se aplica a las cosas cuyo conocimiento se guarda entre un reducido número de personas con cuidado de que no trascienda a las demás»; *vid.* MOLINER RUÍZ, M., *Diccionario del uso del español*, Tomo II, Gredos, Madrid, 2004. También el *Diccionario del español jurídico*, en la sección penal, define el secreto como el «conocimiento sobre algo desconocido para los demás» (disponible en: <https://dej.rae.es/>).

¹¹ Incluso cuando se veda expresamente determinada compartición de secretos, como en el art. 22.5 CE.

¹² Algunas definiciones de secreto pueden llevar a error. Así, cuando se define *secreto* como «noticia o conocimiento que se guarda *entre un reducido número de personas*», *cfr.* MOLINER RUÍZ, M., *Diccionario del uso del español*, *op.cit.*

C. Secreto como atribución normativa de carácter teleológico

Más allá de las consideraciones realizadas hasta el momento, predicables de un concepto general de secreto, conviene aproximarse ahora más específicamente al secreto como concepto jurídico.

En este sentido, la protección de una determinada relación a través del concepto de secreto no responde —o no solo— a la cualidad intrínseca de lo que se tutela, ni a un deseo o añagaza de quien dispone del conocimiento que oculta¹³.

La voluntad de transmitir un conocimiento, en la confianza de que se mantendrá oculto, o bajo promesa de no revelarlo, hará nacer, en su caso, un deber moral de guardar secreto¹⁴. Pero la garantía jurídica de secreto debe exigir, en coherencia con la vocación de generalidad de las normas, algo más, un plus que confiera legitimidad al Estado para amparar la ocultación de determinados conocimientos.

El Derecho protege un determinado conocimiento a través de su calificación como secreto cuando su ocultación aprovecha —o su revelación daña— a un bien que el ordenamiento tutela. No basta pues una actitud de mantener un conocimiento oculto, sino que esa voluntad debe encontrar

¹³ MORENO CATENA, V.M., *El secreto en la prueba de testigos...*, *op.cit.*, pág. 78.

¹⁴ El *Compendium Salmanticense* ya recoge una clasificación de tres tipos de secreto: *adquirido*, «obligación de callar lo que sabemos por casualidad, industria, ó de otra manera, sin haber prometido guardarlo», *promiso*, «quando de sí no trae la cosa obligación de callarse, ni tampoco encarga otro el secreto, si no que el que la sabe promete guardarlo», y *comiso* «quando expresa ó tácitamente se dice la cosa baxo de secreto, y el que adquiere su noticia promete al que se la comunica guardarlo». SANTA TERESA, M. (trad.), *Compendio Moral Salmanticense según la mente del angélico doctor*, Tomo I, Madrid, 1808, pág. 591.

fundamento en «un interés jurídicamente apreciable»¹⁵, en forma de bienes jurídicos o derechos¹⁶.

El secreto es, por tanto, una atribución normativa teleológicamente fundamentada.

Esta relación habilita una dualidad o (potencial) disociación entre el secreto normativamente previsto y el bien jurídico que a su amparo se pretende proteger.

El secreto de que hablamos posee pues un carácter instrumental previsto por el ordenamiento al servicio de un interés jurídicamente relevante precisado de tutela. Un medio de protección de bienes e intereses jurídicos de relevancia¹⁷.

Así, el secreto se utiliza por el ordenamiento como instrumento para proteger la intimidad —deber de secreto profesional¹⁸—, la propiedad industrial e intelectual y la libre competencia —secretos de empresa¹⁹—, la libertad religiosa —secreto *sacramental* (dice la vieja LECrim)²⁰—, los derechos a comunicar y recibir información veraz —secreto profesional del periodista²¹—, la protección de datos personales —secreto estadístico²²—, el

¹⁵ «[...] la voluntad originaria y motriz del titular (tanto público como privado) que pretende la reserva de un segmento sustantivamente calificado de sus actividades o vivencias (hecho, cosa o situación) debe estar también necesariamente acompañada de un componente de derecho: un interés jurídicamente apreciable, o sea, de un interés que se ve recogido en el sistema de derecho en atención a su intrínseca relevancia o trascendencia en dicho ámbito (del derecho)», cfr. MEYRE, L.H., «La protection du secret dans le contexte de la responsabilité», *Revue Droit des Sciences Économiques et de Gestion*, 1, 2003, pág. 112, en CERVINI, R., «El elemento estatutario del secreto como instrumento de efectiva realización de las garantías», *Revista de Derecho: Publicación de la Facultad de Derecho de la Universidad Católica de Uruguay*, 1, 2006, pág. 66.

¹⁶ BAJO FERNÁNDEZ, M., «El secreto profesional en el proyecto de Código penal», *Anuario de derecho penal y ciencias penales*, Tomo 33, 3, 1980, pág. 599.

¹⁷ MORENO CATENA, V.M., *El secreto en la prueba de testigos...*, *op.cit.*, págs. 93-94.

¹⁸ Arts. 199 CP y 542.3 LOPJ.

¹⁹ Arts. 278 y siguientes CP y Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

²⁰ Art. 417.1º LECrim.

²¹ Art. 20.1.d) CE.

²² Arts. 13 y siguientes de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

estatus funcional y la buena marcha de la Administración —deber de secreto de los funcionarios públicos²³—, la libre participación política —sufragio secreto²⁴—, la tutela judicial efectiva —secreto sumarial²⁵—, la libertad de las comunicaciones —secreto de las comunicaciones²⁶— o la seguridad del Estado —secretos oficiales²⁷—, entre otros²⁸.

Esta pluralidad de bienes jurídicos tutelados por el secreto requiere rechazar determinadas posiciones doctrinales que conectan, en una pretendida relación de determinación, secreto e intimidad²⁹.

Se trata de una confusión cuyo origen parece hallarse en la teoría de las esferas formulada por la doctrina alemana para delimitar el derecho a la intimidad. Esta vendría formada por un conjunto gradual de esferas concéntricas —esfera individual, esfera privada y esfera de secreto—, donde la esfera de menor radio coincide con el ámbito más reservado de la persona³⁰.

Pero no existe, como dijimos, una relación de subordinación, ni tampoco del tipo género-especie, entre intimidad y secreto. La intimidad es ajena al Derecho y, por tanto, este solo puede *reconocerla*. El secreto es, sin embargo,

²³ Arts. 415 a 417 CP.

²⁴ Arts. 68.1, 69.2 y 140 CE y 5, 86, 146.1.b) LOREG.

²⁵ Arts. 232.3 LOPJ y 466 CP.

²⁶ Arts. 18.3 CE y 197.1 CP.

²⁷ Arts. 598 y siguientes CP y Ley 9/1968, de 5 de abril, sobre secretos oficiales.

²⁸ Atendiendo al bien jurídico protegido por el secreto se ha propuesto una clasificación, en cierto modo estéril según creemos, entre secretos públicos y privados. Los primeros son aquellos que tutelan «un bien de carácter esencialmente público, por ejemplo, la defensa nacional, la seguridad del Estado o el buen funcionamiento de la Administración Pública», mientras que entre los secretos privados se hallarían otros bienes como «la intimidad del sujeto o la inviolabilidad de sus comunicaciones». Vid. OLMO FERNÁNDEZ-DELGADO, L., *El descubrimiento y revelación de secretos...*, *op.cit.*, pág. 107.

²⁹ «El secreto en general, como instituto protegido por un Estado con vocación democrática, está ineludiblemente vinculado a la tutela de un derecho fundamental como lo es la intimidad y privacidad, expresiones del paradigma de portada general de la libertad». CERVINI, R., «El elemento estatutario del secreto...», *op.cit.*, pág. 57.

³⁰ HUBMANN, H., *Das Persönlichkeitsrecht*, Böhlau, Köln-Graz, 1967, págs. 267 y ss., citado en CERVINI, R., «El elemento estatutario del secreto...», *op.cit.*, pág. 59.

una calificación normativa de determinadas relaciones para proteger distintos bienes jurídicos entre los que se encuentra, junto a otros, la intimidad.

Lo que hace posible una ruptura del secreto sin injerencia en la intimidad —como sucede en el caso de interceptaciones de comunicaciones sin contenido—, y violación de la intimidad sin ruptura del secreto —divulgación de contenido íntimo por uno de los comunicantes, para quienes no rige el secreto—³¹.

D. El secreto presenta una doble dimensión imperfecta

El ordenamiento jurídico recurre al concepto de secreto a través de diferentes categorías: imponiendo un deber de secreto, reconociendo un derecho al secreto o calificando como secreta una determinada realidad³².

Esta diversidad de categorías requiere realizar algunas matizaciones sobre su régimen jurídico y algunas precisiones terminológicas relativas a la relación existente entre secreto y confidencialidad.

Conviene comenzar afirmando que no hay secreto para quienes legítimamente poseen ese conocimiento oculto que se califica como tal. Para ellos regirá, en su caso, un deber de guardar oculto el conocimiento calificado como secreto: se tratará pues de un deber de reserva o confidencialidad. Por ello, la confidencialidad niega el secreto, ya que solo está obligado a ella quien, por conocerlo, puede disponer de él.

³¹ «[...] el secreto puede ir referido tanto a realidades propias de la esfera de intimidad como a intereses industriales, políticos, militares, etc.... Y también se olvida que la intimidad puede ser lesionada tanto con el descubrimiento de secretos como a través de injurias, escucha de conversaciones, etc.... Debe de quedar claro que el secreto no constituye el bien jurídico protegido en ningún precepto penal. Lo que se protege son los intereses políticos, militares, industriales, administrativos o lo que se llama "intimidad personal", contra comportamientos diversos, entre los que se incluyen ciertos descubrimientos de secretos». BAJO FERNÁNDEZ, M., «El secreto profesional en el proyecto de Código penal», *op.cit.*, pág. 605.

³² Así, el art. 542.3 LOPJ dice: «Los abogados *deberán guardar secreto* de todos los hechos o noticias de que conozcan por razón de cualquiera de las modalidades de su actuación profesional». Por su parte, el art. 24.1.d) CE dispone que «La ley regulará *el derecho* [...] *al secreto profesional*...». En fin, los arts. 68.1, 69.2 y 140 CE califican al sufragio como *secreto*.

No obstante, la calificación normativa de secreto no supone, de manera automática, el nacimiento de un deber de confidencialidad.

Así sucede, por ejemplo y como veremos con mayor atención, en el precepto que constituye el objeto de este estudio. El art. 18.3 garantiza el secreto de las comunicaciones, pero ni el secreto rige entre los comunicantes ni establece un deber de confidencialidad entre ellos.

Del mismo modo, el obligado por el deber de confidencialidad puede verse liberado según norma jurídica habilitante. En el mismo ejemplo, para el prestador del servicio de telecomunicaciones no rige el secreto sobre la información que conoce —o que es necesario que conozca—: aquellos datos requeridos para la prestación y, en su caso, facturación del servicio. Respecto de esa información estará vinculado por un deber de confidencialidad del que puede ser dispensado si la norma le habilita.

El secreto se configura, por tanto, como una barrera que impide el acceso al conocimiento vedado. Y para ello el ordenamiento dispone diversos mecanismos orientados a su tutela.

En ocasiones prohíbe, o condiciona, el acceso a un determinado conocimiento, anulando los efectos jurídicos del ilícitamente obtenido: nulidad procesal de la prueba así conseguida o sanción del acceso.

Este es el caso de los delitos que castigan la ruptura del secreto (arts. 197 CP —descubrimiento del secreto de las telecomunicaciones—, 278 CP —descubrimiento de secretos de empresa—, 598 CP —descubrimientos de secretos oficiales—, 146.1.b) LOREG —descubrimiento del secreto del voto—, etc.) o el acceso contra norma desatendiendo los requisitos oportunos (art. 11 LOPJ en conexión con el 18.3 CE).

En otras ocasiones, para impedir el acceso, el ordenamiento dispensa a los conocedores del deber general de formular denuncia o declarar en determinadas situaciones, típicamente en el proceso penal. Así sucede con la

dispensa del deber de declarar de los abogados y de los ministros de culto (arts. 416.2 y 417.1 LECrim).

No se trata de un derecho a disposición del abogado o el eclesiástico, en cuyo caso su titular podría decidir no ejercitarlo, sino de un deber que se impone al Estado de no disponer del conocimiento adquirido en el ejercicio de sus funciones que, para ello, se protege mediante secreto³³.

Por su parte, la confidencialidad presupone un círculo de cognoscibilidad limitado, que no obstante impide su disposición respecto de terceros. Los mecanismos que prevé el ordenamiento se dirigen, a diferencia del secreto, a los poseedores del conocimiento. Para proteger este deber de confidencialidad el ordenamiento les impone la prohibición de difundir o revelar ciertos conocimientos que, no obstante, han sido legítimamente obtenidos. Tal sucede en las normas penales que tipifican la revelación de secretos profesionales (art. 199 CP), empresariales (art. 279 CP), funcionariales (art. 417 CP) u oficiales (arts. 599 y ss. CP).

El ordenamiento recurre al secreto tanto para impedir que terceros accedan a un conocimiento poseído por un número limitado de personas, como para evitar que lo difundan³⁴. Pero se trata de una doble dimensión del secreto asimétrica por cuanto que no se cumple en todos los casos contemplados en el ordenamiento.

³³ GRIMA LIZANDRA, V., «Secreto profesional del abogado y derecho de defensa penal», BOIX REIG, J. (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, pág. 200. Sí posee tal carácter de derecho el secreto profesional de los periodistas previsto en el art. 20.1.d) CE, en la medida en que se trata de una facultad de estos de negarse a revelar ante otros sujetos sus fuentes de información. Vid. LAZCANO BROTONS, I., *El secreto profesional en el periodismo*, Lete Argitaletxea, Bilbao, 2007.

³⁴ Delimitado a la protección penal del secreto se ha dicho que «[t]eniendo en cuenta la estructura que presentan los tipos en los que aparece este término, el secreto requiere, además, o bien que el sujeto activo no tenga conocimiento de esos hechos o datos, o bien que, teniéndolo, sea confidente necesario y obligado por ello a la reserva o sigilo». Cfr. ROMEO CASABONA, C.M., *Los delitos de descubrimiento y revelación de secretos*, Tirant Lo Blanch, Valencia, 2004, pág. 66.

Así, el secreto de sufragio se configura únicamente como la prohibición de acceso a ese conocimiento reservado, pero en ningún caso impone un deber de reserva para su titular³⁵

Se cumple, en cambio, en determinados ámbitos del secreto profesional en que, como hemos visto, se dispone tanto el secreto como barrera de entrada al conocimiento protegido (dispensa de declarar del abogado) como la confidencialidad a modo de barrera de salida de ese conocimiento (castigando su revelación)³⁶.

En definitiva, el *secreto* es un concepto relacional al que recurre el ordenamiento para mantener un conocimiento oculto en posesión de un número de personas limitado y con exclusión del resto, para, a su través, y mediante diferentes técnicas, proteger bienes jurídicos determinados.

³⁵ «No se trata de que el voto tenga que mantenerse reservado por parte del elector, sino que no pueda conocerse en contra de su voluntad, por lo que no resulta afectado este principio si por las circunstancias que sean el individuo decide revelar si ha votado, o no, y en caso afirmativo cuál ha sido el sentido de su pronunciamiento». PRESNO LINERA, M.A., *El derecho de voto*, Tecnos, Madrid, 2003, págs. 213-214.

³⁶ Esta doble dimensión se aprecia con claridad en la redacción del art. 542.3 LOPJ: «Los abogados deberán guardar secreto de todos los hechos o noticias de que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos». No obstante, pese a que ambas dimensiones se refieren al secreto profesional se hace patente en este caso la diferencia entre el secreto y el bien jurídico protegido por aquel, ya que el bien jurídico protegido es diferente en cada una de las dimensiones del secreto: la intimidad en el caso del deber de confidencialidad y los derechos de defensa y a un juicio justo en el caso de la dispensa del deber de declarar.

II. OBJETO DEL DERECHO: EL SECRETO —¿Y LA LIBERTAD?— DE LAS COMUNICACIONES

El objeto de derecho fundamental proclamado en el artículo 18.3 de la Constitución —el espacio de autodeterminación garantizado— se identifica en su literalidad con el secreto de las comunicaciones.

No obstante, tanto la doctrina como la jurisprudencia constitucional consideraron tempranamente que la garantía de secreto constituía simplemente el medio para tutelar la libertad de las comunicaciones como bien constitucionalmente protegido³⁷.

Se trata ahora, por tanto, de afrontar el sentido que el concepto de secreto posee en el artículo 18.3 CE y de analizar la libertad de las comunicaciones como posible objeto del derecho.

II.1. El secreto de las comunicaciones

A. Ámbito objetivo del secreto

Una vez delimitado el sentido constitucional del término «comunicación» en el capítulo precedente, el secreto se configura como un atributo de los procesos comunicativos mediante medios técnicos.

Viene referido pues a las comunicaciones y, por tanto, el conocimiento que se veda —la «limitación a la cognoscibilidad ajena»— se identifica con el proceso comunicativo: «el secreto así dispuesto por la Constitución es atributo jurídico de la comunicación y no de su contenido»³⁸.

Siendo el secreto, como dijimos, un recurso para mantener oculto un determinado conocimiento, no es posible, sin quebrar su coherencia,

³⁷ «Rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto». STC 114/1984, de 29 de noviembre (FJ. 7).

³⁸ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 50.

condicionar su ocultación a que satisfaga requisito material alguno, pues su comprobación desactivaría su objeto.

Por ello, tempranamente la jurisprudencia constitucional consideró que «el concepto de “secreto” en el art. 18.3 tiene un carácter “formal”, en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado»³⁹.

El art. 18.3 CE garantiza, por tanto, la ocultación de aquellos procesos comunicativos que se llevan a cabo a través de determinados medios técnicos y ello con independencia de que el mensaje sea íntimo o notorio, o incluso con independencia de que tal mensaje exista⁴⁰.

Si el secreto se predica del proceso comunicativo, al margen de la existencia o carácter de su contenido, su ámbito objetivo, los conocimientos cuya ocultación se garantizan, deben ser todos aquellos que se generan con ocasión de dicha acción: desde la puesta en marcha y hasta la finalización del proceso comunicativo.

El Tribunal Constitucional ha afirmado que bajo el secreto se ampara «la existencia de la comunicación misma y el contenido de lo comunicado, así como la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino»⁴¹.

³⁹ STC 114/1984, de 29 de noviembre (FJ. 7).

⁴⁰ «El secreto de las comunicaciones constituye el objeto de un derecho fundamental que garantiza la inaccesibilidad del proceso de comunicación a través de medio técnico; lo “oculto” o “secreto” es el proceso comunicativo como tal, con independencia del contenido de lo comunicado; al margen de que el mensaje sea ilegible o inexistente; o con independencia de que la transmisión carezca del contenido propio de una comunicación intersubjetiva». ZOCO ZABALA, C., «Secreto de las comunicaciones en la frontera de la revolución tecnológica», CHUECA RODRÍGUEZ, R. (Dir.), *Las fronteras de los derechos fundamentales en la constitución normativa*, Centro de Estudios Políticos y Constitucionales, Madrid, 2019, pág. 311.

⁴¹ STC 123/2002, de 20 de mayo (FJ. 5).

B. Dimensión temporal del secreto

El proceso comunicacional se desarrolla en un marco temporal ya descrito y analizado *supra*.

Según dejamos dicho, la jurisprudencia constitucional ha afirmado que la protección del derecho fundamental considerado «alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos»⁴².

Por tanto, en atención a ello, y al propio fundamento constitucional del derecho, establecimos que el proceso comunicativo protegido *ex* 18.3 CE abarca la secuencia temporal en que la comunicación está en tránsito, esto es, mientras permanece soportada por el medio técnico con pérdida del dominio por parte de los comunicantes⁴³.

De esta manera, la ocultación de los conocimientos que conforman el proceso comunicativo —existencia de la comunicación, mensaje y datos externos— estará amparada por el 18.3 CE, si la ruptura del secreto se produce en ese espacio temporal⁴⁴.

Los accesos producidos con carácter previo a la activación del proceso comunicacional, o tras su término con la desactivación del soporte —comunicaciones bidireccionales simultáneas—, o con la recepción del mensaje —comunicaciones alternativas—, no poseen carácter secreto *ex art.*

⁴² STC 70/2002, de 3 de abril (FJ. 9).

⁴³En similar sentido se ha señalado que «[e]l secreto no se identifica con el proceso comunicacional, sino con el proceso de comunicación desde que se activa el soporte técnico y hasta su desactivación. La activación y desactivación del soporte para la comunicación operan, así, como términos temporales del proceso protegido por el art. 18.3 CE»; ZOCO ZABALA, C., «Secreto de las comunicaciones en la frontera...», *op.cit.*, págs. 315-316.

⁴⁴ «[...] la protección de este derecho alcanza a las interferencias habidas o producidas en un proceso de comunicación», STC 56/2003, de 24 de marzo (FJ. 2).

18.3 CE corriendo la protección, en su caso, a cargo de otros derechos o institutos jurídicos⁴⁵.

El correcto engranaje del ámbito objetivo y la dimensión temporal del secreto garantizado es de vital importancia para determinar el régimen jurídico de los datos de tráfico o asociados a la comunicación. Por ello, este ha sido uno de los ámbitos que mayor atención doctrinal ha recibido siendo, al mismo tiempo, el que mayores discrepancias ha generado. A ello dedicaremos el próximo capítulo.

C. Ámbito subjetivo del secreto

Si secreto es aquello cuyo conocimiento se veda y permanece ignoto, repitamos que será obvio que aquella obligación no podrá regir para sus autores.

Entre los actores del proceso destacan, por su determinante protagonismo en la comunicación, emisor y destinatario(s).

Por ello, acertada y tempranamente, el máximo intérprete constitucional afirmó que este derecho «no puede oponerse, sin quebrar su sentido constitucional, frente a quien tomó parte en la comunicación misma así protegida»⁴⁶.

El art. 18.3 exige para que se entienda vulnerado, en coherencia con el recurso al concepto de secreto para garantizar la inaccesibilidad de las comunicaciones, que provenga de un tercero ajeno a quienes ya lo poseen⁴⁷.

⁴⁵ Como acertadamente afirma ZOCO ZABALA, «[l]as comunicaciones pretéritas almacenadas en el dominio virtual (ya datos), no son proceso comunicacional en el sentido del art. 18.3 CE, como tampoco lo son los datos personales, imágenes e informaciones que circulan por la red o se acumulan en el disco duro del dispositivo técnico», cfr. ZOCO ZABALA, C., «Secreto de las comunicaciones en la frontera...», *op.cit.*, págs. 323-324.

⁴⁶ STC 114/1984, de 29 de noviembre (FJ. 7).

⁴⁷ «La presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación, es indispensable para configurar el ilícito constitucional aquí perfilado»; *ibidem*.

La comunicación es una transmisión de expresiones de sentido que, recibida por su destinatario, se integra en su esfera intelectual. Supone necesariamente el levantamiento de su ocultación a favor del destinatario comunicacional.

Por tanto, la retención del contenido de la comunicación por parte de su destinatario, sea de forma física, como en el caso de la correspondencia *intercambiada*, o mediante grabación o reproducción, no supone vulneración alguna del derecho en la medida en que no hay —no puede haber— ruptura de secreto⁴⁸.

La grabación podrá ser considerada como un acto previo y necesario para una posterior divulgación del contenido de la comunicación, que rebasa ya el objeto propio del derecho al secreto de las comunicaciones y que será, en su caso, contraria a derecho en atención a un incumplimiento de un deber de reserva al que estén sujetos los comunicantes.

Un deber de reserva que no nace del derecho fundamental que analizamos, sino que tendrá su origen, bien en el carácter íntimo del contenido de la comunicación⁴⁹, bien en la existencia de otro deber jurídico de secreto concurrente, ya que, como afirma JIMÉNEZ CAMPO, «el secreto de la comunicación puede coexistir con otros tipos de secreto también jurídicamente garantizados»⁵⁰.

⁴⁸ «Quien graba una conversación de otros atenta, independientemente de toda otra consideración, al derecho reconocido en el art. 18.3 de la Constitución; por el contrario, quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado»; *ibidem*.

⁴⁹ «Sobre los comunicantes no pesa tal deber, sino, en todo caso, y ya en virtud de norma distinta a la recogida en el art. 18.3 de la Constitución, un posible “deber de reserva” que —de existir— tendría un contenido estrictamente material, en razón del cual fuese el contenido mismo de lo comunicado (un deber que derivaría, así del derecho a la intimidad reconocido en el art. 18.1 de la Norma fundamental)»; *ibidem*.

⁵⁰ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 51. Piénsese, por ejemplo, en que la información intercambiada a través de comunicación protegida por el art. 18.3 CE caiga dentro del ámbito garantizado por el secreto profesional o pueda ser calificada, en atención a los términos legales, como un secreto de empresa. En el mismo sentido se expresa la Corte de Casación italiana cuando afirma que «[l]a comunicación, una vez que es libre y legítimamente consumada, sin ninguna intrusión

La grabación en sí misma considerada, sin atender por tanto a su posterior divulgación, podrá constituir una injerencia en el derecho fundamental a la propia imagen, lo que requiere realizar, aunque desborde en cierta medida el objeto de este trabajo, dos breves consideraciones.

Por un lado, la STC 114/1984, de 29 de noviembre (FJ. 8), avanzó ya que la grabación entre comunicantes «sólo podría constituir un ilícito sobre la base del reconocimiento de un hipotético “derecho a la voz” que no cabe identificar en nuestro ordenamiento». Un derecho que el Tribunal vincula en esta resolución a la intimidad y solamente en la medida en que fuese utilizado con determinadas finalidades.

Esta vinculación entre voz e intimidad parece tener origen en el primitivo entendimiento unitario de los derechos presentes en el art. 18.1 CE y en su tratamiento legislativo conjunto en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (en adelante, LOPDH).

No obstante, la evolución jurisprudencial y doctrinal que derivó en la tesis, hoy generalmente aceptada, de la existencia de tres derechos autónomos y diferenciados en el precepto citado, incardinó la voz como elemento del derecho a la propia imagen⁵¹.

por parte de los sujetos ajenos a ella, entra a formar parte del patrimonio del conocimiento de los interlocutores, con el efecto de que cada uno de ellos puede disponer de él, a menos que, por la particular cualidad que reviste o por el específico objeto de la conversación, existan prohibiciones específicas a la divulgación (por ejemplo: secreto profesional)». Cfr. Sentencia núm. 36747, de 24 de septiembre de 2003, de la Corte de Casación, Sección Única Penal. Asimismo, *vid.* USAI, S., «Registrazione di conversazione tra privati: per attività di PG necessaria l'autorizzazione», *Sigurezza e Giustizia*, 2, 2015, pág. 14.

⁵¹ «[...] el derecho fundamental a la propia imagen reconocido en el artículo 18.1 comprende la imagen en sentido estricto, esto es, la representación gráfica de la figura humana, pero también la voz y el nombre de las personas, si bien, el contenido del derecho difiere en cada caso». *Vid.* PASCUAL MEDRANO, A., *El Derecho Fundamental a la Propia Imagen. Fundamento, Contenido, Titularidad y Límites*, Aranzadi, Cizur Menor (Navarra), 2003, pág.62.

Más allá de que la voz haya ganado peso como atributo de este derecho en la jurisprudencia del Tribunal Constitucional⁵², el problema radica, para el caso que nos ocupa, en determinar si la mera captación de la voz no consentida por uno de los comunicantes puede suponer una injerencia en el derecho fundamental a la propia imagen de su interlocutor.

En este sentido, la STC 117/1994, de 25 de abril (FJ. 3), señalaba que:

«[...] es evidente que con la protección de la imagen se salvaguarda el ámbito de la intimidad y, al tiempo, el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de su imagen, su identidad o su voz. El derecho a la intimidad limita la intervención de otras personas y de los poderes públicos en la vida privada, intervención que en el derecho que ahora nos ocupa puede manifestarse tanto respecto de la observación y captación de la imagen y sus manifestaciones como de la difusión o divulgación posterior de lo captado».

Por tanto, y en atención a la precitada sentencia, el contenido de este derecho consiste en otorgar a su titular la facultad de limitar las intervenciones tanto en su imagen como en las *manifestaciones* de ésta (entre las que se encuentra la voz), ya consistan en su difusión, o en su mera captación.

No obstante, el desarrollo legislativo del derecho parece entender como intromisión ilegítima, para el caso concreto de la voz, su sola divulgación y en atención a fines específicos —«[l]a utilización [...] de la voz [...] de una persona para fines publicitarios, comerciales o de naturaleza análoga»; art. 7.6 LOPDH—, y no, por tanto, la mera captación; interpretación que ha sido doctrinalmente avalada⁵³.

⁵² Véanse SSTC 12/2012, de 30 de enero (FFJJ. 5 y 7) y 25/2019, de 25 de febrero (FJ. 9.b).

⁵³ «Mientras que el titular está facultado para decidir sobre la captación, reproducción o publicación de su propia imagen, cualquiera que sea la finalidad de dichos usos, respecto al nombre y a la voz, únicamente dispone de la facultad de decidir sobre su utilización comercial. La voz y el nombre se protegen así sólo en cuanto se utilicen con fines comerciales, publicitarios o similares»; PASCUAL MEDRANO, A., *El Derecho Fundamental a la Propia Imagen...*, *op.cit.*, págs. 62-63.

Por otro lado, la afirmación realizada en la STC 114/1984 —«[l]a grabación en sí [...] sólo podría constituir un ilícito sobre la base del reconocimiento de un hipotético “derecho a la voz”»— debe entenderse como correcta en el tiempo en el que fue dictada, cuando las relaciones comunicativas eran generalmente mantenidas a través de los medios que expresamente se citan en el art. 18.3 CE: correspondencia y comunicaciones telegráficas y telefónicas.

Sin embargo, el actual estado de las tecnologías permite mantener comunicaciones bidireccionales simultáneas en las que el contenido se traslada no solo a través de la voz, sino también de la imagen dinámica (videoconferencias o videollamadas)⁵⁴.

Resulta también patente que el destinatario de una videollamada dispone de artificios técnicos para registrar, en el sentido de captar técnicamente, la imagen física de su interlocutor y, en este caso, la Ley considera intromisión ilegítima la mera captación no consentida⁵⁵.

Por ello, el art. 2.2 LOPDH exige que el consentimiento del titular del derecho sea expreso, si bien en ocasiones se ha admitido como válido un consentimiento tácito inferido de los propios actos del titular, a los que la ley se refiere como delimitadores del alcance del derecho⁵⁶.

⁵⁴ O incluso solo mediante la imagen. Tal sería el caso de una videollamada entre personas con discapacidad auditiva mantenida a través de lengua de signos.

⁵⁵ Art. 7.5 LOPDH: «La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos». La gran mayoría de los dispositivos que permiten mantener este tipo de comunicaciones cuenta con una utilidad (o, en caso contrario, es fácilmente instalable) que permite *capturar* la pantalla, registrando por la tanto la imagen proyectada tanto en forma estática como dinámica.

⁵⁶ Art. 2.1 LOPH: «La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia». Así, por ejemplo, se ha entendido como consentimiento válido para la captación de imágenes —aunque no para su publicación— el hecho de encontrarse la fotografiada «en una clara posición de posar»; *vid.* STS, Sala de lo Civil, de 3 de noviembre de 1988 (FJ. 2). Sobre el consentimiento en el caso del derecho a la propia imagen, puede verse PASCUAL MEDRANO, A., *El Derecho Fundamental a la Propia Imagen...*, *op.cit.*, págs. 89 y ss.

Obviamente, la decisión de mantener una comunicación a través de un medio técnico de este tipo supone un consentimiento implícito de cada interlocutor de que el resto *capte* a través de sus sentidos su imagen física. Pero no parece tan claro que aquel consentimiento pueda abarcar su captación a través de un artificio técnico, es decir, el registro o grabación de una copia en un soporte, que es precisamente lo que la ley considera intromisión ilegítima —«por fotografía, filme, o cualquier otro procedimiento»—.

Distinto será el caso de que el contenido material de la comunicación — el mensaje transmitido— coincida precisamente con el objeto protegido por el derecho a la propia imagen. En el caso de enviar una fotografía o un video donde aparece la imagen física o una nota de voz —audios de *WhatsApp*, por ejemplo— su «captación» no podrá considerarse, en atención a los propios actos de su titular, como intromisión ilegítima, aunque tal consentimiento tácito no habilitará una ulterior difusión.

Es necesario realizar todavía una consideración respecto al uso del contenido comunicativo por los propios comunicantes. Del mismo modo que un comunicante puede grabar una conversación en la que participe con el fin de aportarla como prueba, nuestra jurisprudencia ha considerado que no supone vulneración alguna del derecho fundamental al secreto de las comunicaciones el hecho de que uno de los comunicantes permita el acceso a su contenido a un tercero, bien sea mostrándole la pantalla del terminal, bien dejándole escuchar a través del altavoz⁵⁷.

⁵⁷ Así se entiende en la STC 56/2003, de 24 de marzo (FJ. 3), cuando dice que «[...] en el presente caso, no existe vulneración del derecho al secreto de las comunicaciones. Es, precisamente, uno de los interlocutores en la comunicación telefónica (el denunciante del chantaje al que se encontraba sometido) quien autorizó expresamente a la Guardia Civil a que registrara sus conversaciones para poder determinar así el número desde el que le llamaban». Del mismo, la STC 114/1984, de 29 de noviembre (FJ. 7), señala: «Quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones».

No obstante, en la doctrina y jurisprudencia italiana parece haberse asentado la diferenciación entre dos supuestos: si el comunicante aprehende el contenido por propia voluntad no existe vulneración de secreto, sino simplemente una forma de «documentación del diálogo». Por el contrario, si el interlocutor actúa como *longa manus* de las autoridades encargadas de la persecución penal, se equipara a una intervención de terceros y requiere, por tanto, intervención judicial⁵⁸.

También el TEDH ha considerado contrario al art. 8 del Convenio, en tanto que injerencia en el respeto de la correspondencia, la grabación practicada por uno de los interlocutores, pero por sugerencia o con apoyo técnico de la policía, al constituir su participación «una contribución crucial a la ejecución del plan» y una vía para evadir las garantías dispuestas por el ordenamiento⁵⁹.

En nuestro ordenamiento existe, con todo, un caso en el que uno de los intervinientes en la comunicación requiere autorización judicial para grabar conversaciones en las que participe: cuando se trate de un agente de los fuerzas y cuerpos de seguridad del Estado que actúa como *agente encubierto informático*.

La Ley Orgánica 13/2015, de 5 de octubre, introdujo esta figura en la Ley de Enjuiciamiento Criminal (art. 286 bis.6) a través de la cual se permite autorizar a funcionarios de la Policía Judicial para, bajo identidad falsa,

⁵⁸ «La jurisprudencia [...] ha considerado, en cambio, la inutilidad de las grabaciones de las conversaciones realizadas, en ausencia de la autorización del juez, por uno de los interlocutores equipados con herramientas de recolección preparadas por la policía judicial, por la razón de que, de esta manera, habría una elusión subrepticia de las reglas que imponen recurrir a instrumentos reglados para invadir el bien protegido constitucionalmente del secreto de las comunicaciones», cfr. Corte de Casación penal, sección II, Sentencia núm. 19158 de 20 de marzo de 2015. Así mismo, *vid.* Setenza n. 320 del 2009 de la Corte Constitucional y, en la doctrina, USAI, S., «Registrazione di conversazione tra privati...», *op.cit.*, págs. 14-15 y GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal*, La Ley, Madrid, 2007, pág. 203.

⁵⁹ SSTEDH de 8 de abril de 2003 (asunto *M.M. c. Países Bajos*; § 37 a 42), y 23 de noviembre de 1993 (asunto *A. c. Francia*, § 36 a 37).

participar en comunicaciones mantenidas a través de canales cerrados de comunicación con el fin de llevar a cabo averiguaciones de hechos delictivos⁶⁰.

Descartado, por tanto, y con las salvedades antedichas, que el secreto rijan entre comunicantes, su protección se dirige a quienes son ajenos a la relación comunicacional.

La garantía de secreto prevista en el art. 18.3 CE impone, en este sentido, un deber de no desvelar el contenido ni los elementos del proceso comunicativo⁶¹. Un deber orientado a procurar la impenetrabilidad de las comunicaciones objeto del secreto con vocación de universalidad: «el derecho posee eficacia *erga omnes*»⁶². El derecho fundamental se dirige, según ha manifestado el Tribunal Constitucional, a evitar la ruptura del secreto, provenga ésta de los poderes públicos o de sujetos particulares⁶³.

D. El deber de confidencialidad del prestador del servicio

El círculo limitado de personas para quienes el conocimiento no se mantiene oculto y entre los que, por tanto, no rige el secreto, no se circunscribe en este caso únicamente a los interlocutores de la comunicación.

⁶⁰ «[...] a la hora de intervenir por los funcionarios policiales una conversación telefónica entre el agente encubierto ya infiltrado y un miembro de la organización criminal, resulta necesaria autorización judicial. La grabación de cualquier conversación telefónica y telemática que tenga lugar entre el agente encubierto y cualquier investigado, debe llevarse a cabo de conformidad con las previsiones del artículo 588 ter a) y ss. y ello por cuanto se ven afectados los derechos tanto del propio agente encubierto como de los otros intervinientes»; GÓMEZ DE LIAÑO FONSECA-HERRERO, M., «El uso de dispositivos electrónicos de captación de comunicaciones en operaciones de infiltración policial», DÍAZ MARTÍNEZ, M. y LÓPEZ-BARAJAS PEREA, I. (Coords.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant Lo Blanch, Valencia, 2018, pág. 218.

⁶¹ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 50.

⁶² El secreto de las comunicaciones «ilumina sobre la identidad del sujeto genérico sobre el que pesa el deber impuesto por la norma constitucional»; STC 114/1984, de 29 de noviembre (FJ. 7).

⁶³ Sobre la eficacia del derecho en las relaciones entre particulares *vid. infra* Capítulo V, apdo. III.3.

También debe entrar en esta categoría, aunque de distinto modo según veremos, el prestador del servicio soporte de la comunicación.

El prestador tiene la consideración de «tercero ajeno a la comunicación», por cuanto no emite, ni a él se dirigen, las expresiones de sentido en cuyo intercambio la comunicación consista⁶⁴. No obstante, para proporcionar su necesaria intermediación técnica, requiere del acceso a determinados elementos de la comunicación que, para el resto, permanecen sujetos a secreto.

Así sucede con aquellos datos que el prestador necesita conocer para hacer posible la comunicación y, en su caso, para facturarla. La existencia de la comunicación, desde luego, pero también de otros datos externos que permitan su activación técnica —identidad de los comunicantes (o de los titulares de la «línea»), fecha, hora de inicio y fin y, por tanto, duración, etc.— y, en ocasiones, el propio mensaje transmitido⁶⁵.

Por tanto, frente al prestador del servicio de comunicaciones, será oponible el secreto en todo aquello que no resulte técnicamente preciso para hacer posible la comunicación y el correspondiente abono de la prestación proporcionada; en iguales condiciones que para cualquier otro tercero ajeno.

Pero además, para garantizar completamente la inaccesibilidad de las comunicaciones, el ordenamiento activa respecto del prestador del servicio el mecanismo preciso, como vimos, para impedir que el conocimiento rebase el círculo reducido de personas que lo poseen, quedando así sujeto a un deber de confidencialidad⁶⁶.

⁶⁴ «[...] su específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son possibilitadas mediante la intermediación técnica de un *tercero ajeno a la comunicación*»; STC 123/2002, de 20 de mayo (FJ. 5).

⁶⁵ Típicamente las comunicaciones telegráficas, pero también otras comunicaciones que requieren constancia de su contenido como el burofax o el servicio de telegrama online.

⁶⁶ «Effective protection of communications confidentiality is only possible if the law limits what communication providers can do with our communications and requires such providers to protect our communications against unlawful access by third parties», *vid.* ZUIDERVEEN

Un deber que se deriva de la propia norma iusfundamental en la medida en que se trata de un elemento indispensable para asegurar la eficacia del secreto que el derecho garantiza⁶⁷.

Con todo, el deber de confidencialidad se reitera específicamente en las normas jurídicas que regulan los servicios de comunicaciones disponiendo, por un lado, la prohibición de revelar datos relativos a las comunicaciones tratadas y tipificando, por otro, un catálogo de infracciones y sanciones en caso de contravención⁶⁸.

Secreto como prohibición de descubrir la comunicación protegida y confidencialidad como prohibición de disposición de los habilitados para proporcionarla son los dos institutos jurídicos de que el ordenamiento dispone para asegurar el derecho al secreto de las comunicaciones.

II.2. La libertad de las comunicaciones

Como ya advertimos al comenzar este capítulo, el secreto es una exigencia normativa que posee carácter teleológico. El ordenamiento no tutela el secreto *per se*, sino que califica como tal un elenco de actividades comunicativas para, a su través, proteger un bien jurídicamente relevante.

En este sentido, y por lo que se refiere al secreto que acabamos de delimitar, ya la STC 114/1984, de 29 de noviembre, afirmó que «[e]l bien

BORGESIU, F.J., y STEENBRUGGEN, W., «The right to communications confidentiality...», *op.cit.*, pág. 303.

⁶⁷ «[...] no puede negarse que el reconocimiento de tal derecho está enlazado de forma coesencial con la garantía consistente en el deber, a cargo de todos aquellos que por motivos profesionales conocen el contenido y los datos externos de la comunicación, de mantener la más rigurosa reserva sobre los elementos mencionados»; Sentencia 81/1993 de la Corte Constitucional italiana.

⁶⁸ Así, arts. 5, 59.a) y 62.1 de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal; art. 6 del Real Decreto 1829/1999, de 3 de diciembre, por el que se aprueba el Reglamento que desarrolla la precitada ley; arts. 39.1, 76.10 y 79.1.a) y b) de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones; y arts. 91 a 93 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

constitucionalmente protegido es así —a través de la imposición a todos del “secreto”— la libertad de las comunicaciones».

Es preciso analizar, por tanto, si la norma iusfundamental protege únicamente la ocultación de la comunicación, dirigiéndose en exclusiva a garantizar la inaccesibilidad del proceso comunicativo o si, por el contrario, el reconocimiento de la libertad como objeto mediato del derecho aporta *algo más* a su contenido.

A estos efectos, la afirmación de un derecho a la libertad de las comunicaciones tendría como objetivo, según ha manifestado una parte de la doctrina, conceder a su titular facultades para hacer frente a determinadas acciones dirigidas a comprometer el normal desarrollo del proceso comunicativo: su detención, destrucción, alteración, retención, etc.⁶⁹.

A. Libertad de las comunicaciones expresamente garantizada

La Constitución española de 1978 solo reconoce expresamente en su art. 18.3 el secreto de las comunicaciones, lo que constituye casi excepción en nuestra tradición constitucional y legislativa donde, por el contrario, la regla general había sido la afirmación de ambas cualidades o, más bien, la expresa prohibición de las acciones dirigidas a perturbar tanto la libertad como el secreto de las comunicaciones.

Como tímidamente advertimos en el capítulo primero, las constituciones decimonónicas que incluyeron entre sus declaraciones de derechos algún tipo de protección de las comunicaciones (1869 y 1876) prohibían, ambas en su

⁶⁹ SERRANO ALBERCA, M., «Artículo 18», GARRIDO FALLA, F. (Dir.), *Comentarios a la Constitución*, Civitas, Madrid, 1985, pág. 373. La doctrina italiana, cuya Constitución declara la inviolabilidad de ambas categorías —libertad y secreto—, ha definido la libertad de las comunicaciones como «[e]l derecho a comunicarse y mantener correspondencia con otros sujetos, sin ninguna interrupción o suspensión del curso "normal" de una correspondencia o comunicación», *vid.* ITALIA, V., *Libertà e segretezza della corrispondenza...*, *op.cit.*, pág. 63.

artículo 7, tanto la detención —libertad— como la apertura —secreto— de las mismas.

Por su parte, la Constitución republicana de 1931 garantizaba en su artículo 32 la *inviolabilidad* de la correspondencia, término que se ha entendido delimitador de un ámbito más amplio que comprendería tanto la libertad como el secreto de la comunicación⁷⁰.

El *Fuero de los Españoles* de 1945, que se intitula a sí mismo como el «texto fundamental definidor de los derechos y deberes [...] y amparador de sus garantías», disponía en su art. 13: «Dentro del territorio nacional el Estado garantiza la libertad y el secreto de la correspondencia».

Tampoco faltaron intentos durante el proceso constituyente de 1977-1978 de introducir expresamente la *libertad* en la redacción del vigente art. 18.3 CE.

Así, durante la tramitación del proyecto en el Congreso, la enmienda núm. 470, presentada por el Grupo Parlamentario Mixto, propuso que la norma que nos ocupa garantizase «la libertad y el secreto de las comunicaciones», indicando simplemente en la motivación que con esa redacción se garantizaban con mayor precisión los derechos declarados. En Comisión no se le prestó atención, aprobándose el texto en el Congreso con la sola garantía expresa del secreto.

Mejor suerte correría la propuesta que en similar sentido impulsó en el Senado el Grupo Parlamentario Agrupación Independiente. Su enmienda núm. 663 se justificaba en los siguientes términos:

«La enmienda se propone garantizar no solo el secreto sino también la libertad de las comunicaciones, pues que se garantice el secreto no implica que se garantice la libertad».

⁷⁰ SERRANO ALBERCA, M., «Artículo 18», *op.cit.*, pág. 373. En el mismo sentido, SEMPERE RODRÍGUEZ, C., «Artículo 18: Derecho al honor, a la intimidad y a la propia imagen», ALZAGA VILLAAMIL, O (Dir.), *Comentarios a la Constitución Española de 1978*, Tomo II, Edersa, Madrid, 1996, pág. 441.

Sometida a votación en la Comisión de Constitución, la enmienda fue aprobada con un solo voto a favor y veintidós abstenciones⁷¹, si bien, la referencia a la *libertad* desaparece finalmente en los trabajos de la Comisión Mixta por razones que desconocemos al ser secretas sus deliberaciones⁷².

Con todo, la ausencia de referencia expresa a la libertad de las comunicaciones en el art. 18.3 CE no ha impedido su reconocimiento expreso en normas infraconstitucionales, incluso formalmente previas a la entrada en vigor de la Constitución.

Tal fue el caso de la Ley 62/1978, de 26 de diciembre, de Protección Jurisdiccional de los Derechos Fundamentales de la Persona que, al establecer su ámbito de aplicación en el art. 1.2, dispone:

«Quedan comprendidas en el ámbito de aplicación de esta Ley, sin perjuicio de lo establecido en su disposición final, las libertades de expresión, reunión y asociación, *la libertad y secreto de la correspondencia*, la libertad religiosa y la de residencia, la garantía de la inviolabilidad del domicilio, la protección jurídica frente a las detenciones ilegales y, en general, frente a las sanciones impuestas en materia de orden público»⁷³.

Por su parte, tanto la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal, como el Real Decreto 1829/1999, de 3 de diciembre, que aprueba el reglamento que la desarrolla, distinguen entre secreto e inviolabilidad.

⁷¹ Azcárate Florez, defensor de la enmienda, agradeció expresamente al senador Unzueta, único votante a favor de la misma, por ser en palabras de aquél el «único entusiasta de la libertad bien garantizada». Diario de Sesiones del Senado, Comisión de Constitución, núm. 43, de 24 de agosto de 1978, pág. 1845.

⁷² Una de las posibles causas pudiera ser, en términos de mera conjetura y ante la discrepancia con el texto aprobado en el Congreso, la exigua mayoría con la que resultó aprobada la enmienda en el Senado.

⁷³ El Real Decreto 342/1979, de 20 de febrero, legislativo sobre ampliación del ámbito de la Ley 62/1978, de 26 de diciembre, incorporó «las comunicaciones telefónicas y telegráficas», pero solo en términos de secreto y no de libertad. Probablemente porque secreto y libertad se vinculan inexorablemente solo en el caso de las comunicaciones postales, única modalidad para cuya apertura se requiere su previa detención física.

Mientras que bajo la rúbrica de *secreto* (art. 5 de la Ley y 6 del Reglamento) se garantiza el deber de reserva o confidencialidad de los prestadores en el sentido que expusimos, la *inviolabilidad* (art. 6 de la Ley y 7 del Reglamento) sugiere unos contornos más amplios, ya que viene referida tanto al secreto —entendido como el acceso al conocimiento oculto a los operadores mediante la «apertura» del envío postal— como a la libertad, al disponer:

«Los operadores postales deberán cumplir con el deber de fidelidad en la custodia y gestión de los envíos postales. Se considerará incumplimiento de dicho deber la detención contraria a derecho, el intencionado curso anormal, la apertura ilegal, la sustracción, la destrucción, la retención indebida y la ocultación de los citados envíos postales»⁷⁴.

Por lo demás, la omisión de la referencia expresa a la libertad de comunicaciones en el texto constitucional de 1978, se alinea con la tónica general presente en las constituciones de nuestro entorno. En la Unión Europea, solo las Constituciones de Italia (art. 15), Polonia (art. 49) y Bulgaria (art. 34) garantizan expresamente la libertad junto con el secreto de las comunicaciones⁷⁵.

B. Delimitación de la libertad de las comunicaciones

El hecho de que no se garantice expresamente la libertad de las comunicaciones en el art. 18.3 CE no ha servido de obstáculo para que el Tribunal Constitucional considerara que la misma formaba parte del objeto del derecho fundamental al secreto de las comunicaciones.

⁷⁴ Art. 6.1 de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal. En similares términos se expresa el art. 7 del Reglamento, aunque otorga a la lista de conductas previstas en la Ley carácter ejemplificativo al señalar que se considerará también *violación* de los envíos postales «cualquier acto de infidelidad en su custodia».

⁷⁵ La Constitución de la República de Chipre reconoce, en su art. 17, el derecho «al respeto y al secreto» de la correspondencia.

Así, en la primera sentencia en la que analiza con carácter general este derecho, la tantas veces citada STC 114/1984, de 29 de noviembre, afirma:

«Rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas. El bien constitucionalmente protegido es así —a través de la imposición a todos del “secreto”— la libertad de las comunicaciones».

Veamos, por tanto, cual es el alcance de tal reconocimiento.

B.1. Libertad de las comunicaciones como derecho al medio o servicio de comunicaciones

En una gradación de las supuestas facultades que podría otorgar a su titular un derecho a la libertad de comunicarse, la más alta cota estaría sin duda ocupada por la obligación estatal de prestar el servicio y los medios que lo hagan posible. Posibilidad que debemos rechazar de plano.

Ni del fundamento ni de la formulación del art. 18.3 CE es posible inferir un derecho tal. Nos hallamos, como dijimos, ante una prohibición constitucional que, reflejamente, puede definir un ámbito de libertad, pero en ningún caso establecer un derecho prestacional.

Esta posibilidad ha sido rechazada por la doctrina, incluso para aquellos sistemas constitucionales en que se reconoce expresamente la libertad de las comunicaciones⁷⁶.

⁷⁶ «[...] el derecho a la inviolabilidad de la correspondencia no es parte de los llamados "derechos sociales", sino que forma parte de los derechos de libertad clásicos [...]. No se concreta, por lo tanto, en la exigencia de una prestación del servicio por parte de individuos o por el Estado». ITALIA, V., *Libertà e segretezza della corrispondenza...*, *op.cit.*, pág. 54. Para el caso español la respuesta es unánime. Cfr., entre otros, JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 51; BELDA PÉREZ-PEDRERO, E., «El derecho al secreto de las comunicaciones», *op.cit.*, pág. 176 y RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, págs. XVIII-XIX.

B.2. Libertad de las comunicaciones como libertad de acción

Descartada su naturaleza prestacional se ha sostenido también que el derecho al secreto de las comunicaciones, *via* la libertad que persigue, «resultará lesionado en todos los casos en los que, disponiendo su titular del medio para comunicarse, la comunicación se impida»⁷⁷.

La libertad de las comunicaciones se entendería, en este sentido, como un derecho de su titular a entablar comunicaciones.

Del mismo modo, una parte de la doctrina ha entendido que «la protección constitucional del secreto de las comunicaciones atiende a la llamada libertad de las comunicaciones, aquel derecho que tenemos todo a expresarnos libremente e interrelacionarnos con todo aquello que abarca el entorno social»⁷⁸.

El TEDH se ha pronunciado en similares términos cuando, al enjuiciar la conformidad de la interceptación de comunicaciones telefónicas con el art. 8 CEDH, ha afirmado que el citado precepto «comprende el derecho a establecer y desarrollar relaciones con otros seres humanos»⁷⁹.

Consideramos, no obstante, que la facultad de entablar comunicaciones se hallaría protegida, no ya por el derecho fundamental al secreto de las comunicaciones, sino más propiamente por el derecho a la libertad de expresión, entendido como «el derecho de todos a manifestar y comunicar sin trabas el propio pensamiento»⁸⁰.

⁷⁷ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 51. También, en este sentido, MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 47.

⁷⁸ RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, pág. 31.

⁷⁹ STEDH de 16 de febrero de 2000 (asunto *Amann c. Suiza*, §65).

⁸⁰ SOLOZÁBAL ECHEVARRÍA, «La libertad de expresión desde la teoría de los derechos fundamentales», *Revista Española de Derecho Constitucional*, 32, 1991, pág. 73. La imposibilidad de entablar una comunicación también se ha conectado con la libertad de expresión por la doctrina penalista, afirmándose que tal conducta «quebrantaría la libertad de la comunicación interpersonal a distancia, impidiendo o intentando impedir la positiva facultad de interrelación que corresponde a todo sujeto en la sociedad, como un aspecto de la libertad

El art. 20.1.a) CE reconoce, como afirma la doctrina, un derecho de comunicación del individuo con los demás mediante cualquier procedimiento⁸¹. La comunicación del individuo con sus semejantes, generadora del intercambio de pensamientos y necesaria para la conformación de la opinión, se puede producir tanto a través de los medios de comunicación social como mediante la transmisión de expresiones de sentido entre sujetos determinados.

Esta vinculación entre libertad de las comunicaciones así entendida y libertad de expresión se ha puesto de manifiesto en aquellos sistemas donde ambas se reconocen conjuntamente. Así, se ha dicho que «la expresión del pensamiento y la necesidad de que este pensamiento llegue libremente a otro sujeto son dos fenómenos idénticos, tanto respecto a "corresponder", como respecto a "manifestar"»; y que, por tanto, en cuanto al aspecto de la libertad garantizada en el art. 15 de la Constitución italiana —relativo a las comunicaciones— «no puede negarse su afinidad estructural y su dependencia con el derecho ex art. 21 de la Constitución» —relativo a la libertad de expresión—⁸².

La diferencia entre *comunicar* y *manifestar* el propio pensamiento se centra, como ya advertimos, en la determinación de los destinatarios: «mientras que, en un caso, se pretende que el pensamiento se exponga libremente al conocimiento de una generalidad de sujetos, en el otro, se pretende llevarlo, también libremente, a conocimiento de un sujeto determinado»⁸³.

de expresión»; cfr. OLMO FERNÁNDEZ-DELGADO, L., *El descubrimiento y revelación de secretos...*, *op.cit.*, págs. 80-81.

⁸¹ «Se garantiza el derecho a hacerse oír, lo que implica que el Estado no separa a quien emite la opinión de su auditorio; pero no se le garantiza al comunicante el derecho a ser oído por todo el mundo o por determinadas personas». *Vid.* SOLOZÁBAL ECHEVARRÍA, «Aspectos constitucionales de la libertad de expresión y el derecho a la información», *Revista Española de Derecho Constitucional*, 23, 1988, págs. 146-147.

⁸² ITALIA, V., *Libertà e segretezza della corrispondenza...*, *op.cit.*, pág. 45 y ss.

⁸³ *Ibid*, pág. 62.

La distinción entre ambos modos de transmitir expresiones de sentido se articula, por tanto, en torno a su cognoscibilidad y, por ello, incide en la garantía de su secreto. Así, la naturaleza *privada* del pensamiento comunicado —a través de un medio que permite la determinación de los destinatarios— determinará su inclusión en el objeto del art. 18.3 CE, pero sin que por ello se derive del mismo un derecho generalmente reconocido a comunicarse con los demás.

Los autores que han considerado incluido en el art. 18.3 CE un derecho a entablar comunicaciones han justificado tal interpretación, *vía* 10.2 CE, en la doctrina emanada del TEDH en el asunto *Golder c. Reino Unido*⁸⁴.

Cierto es que en el citado asunto el TEDH afirmó que «[u]n obstáculo en la posibilidad misma de iniciar correspondencia representa la forma más radical de “interferencia” (párrafo 2 del artículo 8) en el ejercicio del “derecho al respeto a la correspondencia”»⁸⁵. Pero también lo es que tal reconocimiento solo se ha realizado cuando se trata de las comunicaciones a entablar por un preso con su abogado, y que las razones que se valoran para entender vulnerado el derecho del demandante parecen más encaminadas a salvaguardar el derecho de defensa que una pretendida libertad de las comunicaciones⁸⁶.

En ocasiones se ha apelado a la libertad de las comunicaciones en otros ámbitos en los que, en sentido similar al caso aludido, existen trabas a la posibilidad de comunicarse derivadas de una relación en la que se enmarca el sujeto, como sucede en el caso de las relaciones laborales.

⁸⁴ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 52.

⁸⁵ STEDH de 21 de febrero de 1975 (asunto *Golder c. Reino Unido*, §43).

⁸⁶ En similar sentido, BELDA PÉREZ-PEDRERO, E., «El derecho al secreto de las comunicaciones», *op.cit.*, pág. 177. Por la misma razón, las referencias a esta sentencia del TEDH solo aparecen en la jurisprudencia de nuestro Tribunal Constitucional en asuntos en los que se valora la conformidad de suspensiones de las comunicaciones de internos en centro penitenciarios (así, *v.gr.*, STC 15/2011, de 28 de febrero, FJ. 5).

Así, el Voto Particular que emite el magistrado Valdés Dal-Ré a la STC 241/2012, de 17 de diciembre, tras recordar que, desde la STC 114/1984, la libertad de las comunicaciones, y no sólo su secreto, integra el título de cobertura que desencadena la tutela constitucional del 18.3 CE, considera que, desde esa perspectiva, las órdenes del empresario limitativas del uso de herramientas que permitan la comunicación, aunque sean de su titularidad, pueden ser contrarias al derecho fundamental al secreto de las comunicaciones.

Consideramos, no obstante, que cuando se limita el derecho de una persona a comunicarse con los demás, ilegítimamente o no (como sucede en el caso de la pena de prohibición de comunicarse con la víctima del delito u otras personas —art. 39.h) CP—, la prisión provisional incomunicada —art. 509 LECrim—, o el régimen especial de los internos en centros penitenciarios —art. 51 LOGP—), tales limitaciones operan sobre el ejercicio del derecho a la libertad de expresión; sin afección por tanto del derecho al secreto de las comunicaciones.

Aceptar lo anterior supondría desnaturalizar el objeto del derecho fundamental previsto en el art. 18.3 CE mediante una dilatación de su delimitación constitucional, con el riesgo de debilitación de su eficacia protectora y garantista⁸⁷.

B.3. Libertad de las comunicaciones como prohibición de alterar su curso normal

La doctrina italiana, país cuya constitución declara expresamente como inviolable la libertad de las comunicaciones en su art. 15, la ha definido como «el derecho a comunicarse y mantener correspondencia con otros sujetos, sin

⁸⁷ Sobre esta cuestión, *vid.* CHUECA RODRÍGUEZ, R., «Debilidades estructurales del derecho fundamental», CHUECA RODRÍGUEZ, R. (Dir.), *Las fronteras de los derechos fundamentales en la constitución normativa*, Centro de Estudios Políticos y Constitucionales, Madrid, 2019, págs. 23-52.

ninguna interrupción o suspensión del curso normal de una correspondencia o comunicación»⁸⁸.

Esta parece también la connotación que quiso dar nuestro Tribunal Constitucional al reconocimiento de la libertad de las comunicaciones como bien constitucionalmente protegido en el art. 18.3 CE, al considerar que la vinculación entre secreto y libertad implica que el derecho al secreto de las comunicaciones pueda ser vulnerado por la mera detención, sin acceso a contenido, del proceso comunicativo. Esta es la interpretación más verosímil de la afirmación contenida en la STC 114/1984, de 29 de noviembre (FJ. 7):

«[...] el derecho puede conculcarse [...] por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje —con conocimiento o no del mismo— [...])».

No obstante, esta temprana aseveración de nuestro Tribunal Constitucional, avalada por una parte de la doctrina, suscita algunas consideraciones⁸⁹.

La interpretación que, como hemos visto, se ha realizado del secreto de las comunicaciones en el art. 18.3 CE hace innecesario acudir a una supuesta libertad de las mismas para amparar detenciones arbitrarias.

Para llevar a cabo una acción dirigida a suspender el curso normal de una comunicación —su detención, destrucción, retención...— es necesario el conocimiento de su existencia. Sin embargo, reconocido ya que el secreto se predica en el art. 18.3 CE del proceso comunicativo íntegro y no solo del mensaje, la existencia misma de la comunicación formará parte del ámbito objetivo protegido por el secreto. De ahí que su desvelamiento, como

⁸⁸ ITALIA, V., *Libertà e segretezza della corrispondenza...*, *op.cit.*, pág. 63.

⁸⁹ Afirma JIMÉNEZ CAMPO que «la libertad para comunicarse impone, por necesidad, la libertad misma de la comunicación, esto es, y al margen ya de la hipótesis del quebrantamiento del secreto, la no interceptación de su regular curso». JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 51.

precondición para incidir en su normal curso, constituirá ya una vulneración de aquel⁹⁰.

Por ello, la expresa prohibición de las conductas vulneradoras de la libertad de las comunicaciones, entendida en el sentido arriba expuesto, es solo necesaria frente a aquellos para quienes la existencia misma de la comunicación nunca puede ser secreta: los prestadores del servicio. Y ello explica que la única norma vigente en nuestro ordenamiento que se expresa en este sentido sea el referido art. 6 de la Ley del Servicio Postal, actuando por tanto como una suerte de régimen de organización interna del servicio.

Con todo, es cierto que los poderes públicos también podrán conocer la existencia del proceso comunicativo, pero una vez habilitados en cumplimiento de los requisitos que el propio derecho dispone para su limitación.

Alzado legítimamente el secreto sobre la existencia de la comunicación no es posible, sin embargo, ordenar una medida cuya finalidad sea la mera suspensión de su curso. No ya porque con tal actuación se vulnere un pretendido derecho a la libertad de las comunicaciones, sino porque tal medida desbordará la justificación que legitimó su habilitación para alzar el secreto. Si la intervención pública en el objeto de este derecho se justifica en la salvaguarda de otro bien jurídico, como es la investigación de hechos delictivos, la mera suspensión del proceso comunicativo, sin la finalidad de acceder a su contenido, carecerá precisamente de la *ratio* justificadora que la convertía en legítima⁹¹.

⁹⁰ Repárese en que, en los sistemas como el italiano en que se garantizan tanto la libertad como el secreto de las comunicaciones, éste último ha sido solo entendido como una garantía frente al descubrimiento de su contenido, siendo definido como «el derecho a que sujetos diferentes del destinatario no tomen conocimiento del contenido de una correspondencia o comunicación» *Vid.* ITALIA, V., *Libertà e segretezza della corrispondenza...*, *op.cit.*, pág. 91.

⁹¹ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 52. Esta conducta, que ha sido denominada por la doctrina penalista como *interceptación de obstrucción*, frente a la *interceptación de indiscreción* en la que se accede al contenido, está castigada penalmente en el art. 536.1 CP: «La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las

De hecho, cuando la Ley de Enjuiciamiento Criminal dispone, en su art. 579.1, que «[e]l juez podrá acordar la *detención* de la correspondencia», lo hace únicamente en cuanto que acción necesaria para su posterior apertura⁹². La orden judicial se dirige al prestador del servicio y, con ello, le exime del deber de inviolabilidad general a que se encuentra sometido.

B.4 Libertad de las comunicaciones como libertad para compartir expresiones de sentido exclusivamente con sujetos determinados

Las anteriores consideraciones nos habilitan para la siguiente conclusión: la libertad de las comunicaciones como bien jurídico tutelado por el art. 18.3 CE es, ni más ni menos, que la libertad que a los comunicantes les asegura saberse protegidos por el secreto.

Privado el ciudadano del aseguramiento material que aquel derecho le proporciona, no dispondría de la libertad precisa para entablar determinados procesos comunicativos ni compartir libremente sus pensamientos. La libertad de las comunicaciones es, en este sentido, la libertad para compartir expresiones de sentido con sujetos determinados con exclusión del resto. Una libertad que el secreto garantiza y que de él cabalmente se deriva⁹³.

Este es el sentido que debe darse a las palabras del Tribunal Constitucional cuando afirma que con la garantía de secreto «se pretende que todas las comunicaciones [...] puedan realizarse con libertad»⁹⁴.

telecomunicaciones [...] con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años». *Vid.* OLMO FERNÁNDEZ-DELGADO, L., *El descubrimiento y revelación de secretos...*, *op.cit.*, págs. 80-81.

⁹² Por ello, el art. 581 LECrim ordena al empleado responsable de la detención de la correspondencia su inmediato envío al Juez, quien practicará su apertura conforme a los arts. 584 y ss.

⁹³ RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, pág. XIX.

⁹⁴ STC 170/2013, de 7 de octubre (FJ.4.a).

El secreto, como dijimos, no se tutela por tal, sino como condición de libertad que se alza contra el riesgo de intromisión pues, como acertadamente se ha dicho, «no [existe] libertad allá donde no hay expectativa cierta de inmunidad frente a indagaciones ajenas»⁹⁵.

El secreto garantizado en el art. 18.3 CE se comporta así como otros tipos de secreto previstos en el ordenamiento, vale decir, como precondition de aseguramiento de libertad, cuyo ejemplo más evidente quizá sea, por la expresa previsión de su libertad, el secreto del sufragio⁹⁶.

⁹⁵ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 51.

⁹⁶ La delimitación que la doctrina ha realizado sobre el carácter secreto del sufragio es pues trasladable, *mutatis mutandis*, al secreto de las comunicaciones. En este sentido se ha dicho que «[s]e trata de una garantía con la que se pretende asegurar que será una expresión libre de la voluntad del elector; quien podría sentirse coartado en el supuesto de que fuese posible conocer, sin su consentimiento, el sentido de su voto», *vid.* PRESNO LINERA, M.A., *El derecho de voto*, *op.cit.*, págs. 213-214.

III. EL SECRETO TECNOLÓGICAMENTE GARANTIZADO

El derecho fundamental al secreto de las comunicaciones se cimienta sustancialmente sobre dos prohibiciones. Por un lado, la de descubrir el proceso comunicativo blindado con el secreto. Por otro, la de revelar aquello conocido bajo condición de confidencialidad.

Estas dos técnicas resultan en principio suficientes para evitar potenciales intromisiones en los sistemas comunicativos tradicionales y además se adecúan a la estructura que la norma iusfundamental dispone, al garantizar el secreto y, a su vez, permitir acceder al proceso comunicativo atendiendo a las garantías previstas, bien levantando el secreto, bien relevando al obligado de su deber de confidencialidad⁹⁷.

No obstante, con el nacimiento de Internet en los años 70 del siglo pasado y su posterior desarrollo exponencial, comienzan a tejerse complejas relaciones institucionales, académicas y económicas de carácter global en las que los flujos de información se transmiten en línea, demandando una creciente garantía de protección de las transacciones informáticas de datos. Del mismo modo, la red ha transformado las comunicaciones, cada vez más sencillas, veloces y accesibles ya a la mayoría de la población terráquea. De ahí su universalización y creciente incidencia en la transformación de las relaciones sociales y aun de los patrones sociales y valorativos. Las comunicaciones mediante soporte informático forman ya parte del patrimonio universal de comportamiento de los seres humanos⁹⁸.

Pero a su vez, las amplias funcionalidades comunicativas de la red ofrecen crecientes posibilidades de interceptar procesos comunicativos y, por ende, el grado de exposición a acciones de vigilancia masiva. Redes como

⁹⁷ DE ASÍS ROIG, A.E., «Artículo 36», GARCÍA DE ENTERRÍA, E. y DE LA QUADRA-SALCEDO, T. (Coords.), *Comentarios a la Ley General de Telecomunicaciones. Ley 32/2003, de 3 de noviembre*, Civitas, Madrid, 2004, págs. 570-571

⁹⁸ TEJERINA RODRÍGUEZ, O., *Seguridad del Estado y privacidad*, Editorial Reus, Madrid, 2014, pág. 179.

ECHELON (seguramente ya obsoleta) o más recientes artilugios, como el programa *PRISM*, acreditan la dimensión de los problemas que debemos, y deberemos, afrontar⁹⁹.

En esta situación las organizaciones públicas y privadas, y cada vez más los ciudadanos, comienzan a buscar protección adicional para mantener reservado el contenido de sus comunicaciones más allá de la garantía jurídica dispensada hasta ahora por el derecho al secreto de las comunicaciones u otros análogos.

Ello, junto con la posibilidad de adquirir herramientas de encriptación de comunicaciones a bajo coste, ha derivado en una potenciación del uso del cifrado de comunicaciones electrónicas que, si bien es una técnica utilizada desde el inicio de las comunicaciones, se desgaja de su tradicional uso militar o político hasta generalizarse también entre particulares¹⁰⁰.

⁹⁹ *ECHELON* era una red de vigilancia masiva de comunicaciones a nivel mundial en el que participaban EE.UU., Reino Unido, Canadá, Australia y Nueva Zelanda, interceptando indiscriminadamente enormes cantidades de comunicaciones mediante el sistema *Carnivore* y seleccionando después la información de su interés mediante la búsqueda entrecruzada de palabras clave. Su existencia fue confirmada por el Parlamento Europeo, no descartando la existencia de sistemas similares en manos de otros Estados. *Vid.* Informe del Parlamento Europeo sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación *ECHELON*), de 11 de julio de 2001, apdo. 13.1. También GONZÁLEZ NAVARRO, B.A., «Criptología y libertades públicas», *Cuadernos de Derecho Judicial. Internet y derecho penal*, 10, 2001, págs. 160 y ss. Por su parte, *PRISM* es un programa de vigilancia masiva de comunicaciones telemáticas utilizado por la Agencia de Seguridad Nacional de EE.UU., cuya existencia fue revelada por su Edward Snowden en junio de 2013. Cfr. SALAMANCA AGUADO, E., «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones», *Revista del Instituto Español de Estudios Estratégicos*, 4, 2014, págs. 1-26; y VIDAL, G. y MORENO, J.L., «Cryptography and Communications Privacy: An Introduction», ALHAJJ, R. y ROKNE, J. (Eds.), *Encyclopedia of Social Network Analysis and Mining*, Springer, Nueva York, 2018, págs. 526-527.

¹⁰⁰ Se ha recomendado desde diversas instancias la utilización de programas de encriptación, afirmándose que «[e]n las redes abiertas, el cifrado de datos suele ser la única forma eficaz y rentable de proteger la confidencialidad de los datos y las comunicaciones»; cfr. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, 8 de octubre de 1997, «Garantizar la seguridad y la confianza en la comunicación electrónica. Hacia un marco europeo para la firma digital y el cifrado». Igualmente, el informe del Parlamento UE sobre la red *ECHELON* recomienda el uso de la criptografía como medida de autoprotección frente a sistemas de vigilancia masiva de comunicaciones: «También se debe instar a las personas a que codifiquen urgentemente el correo electrónico, ya que un mensaje sin codificar es como una carta sin sobre. En Internet hay sistemas relativamente fáciles de utilizar que están a disposición de los particulares,

En la actualidad el cifrado de comunicaciones interpersonales está completamente generalizado y accesible. Millones de personas intercambian diariamente millones de mensajes encriptados sin ser, en muchos casos, conscientes de ello. La incorporación por defecto de técnicas de cifrado extremo a extremo a plataformas comunicativas de uso generalizado — *WhatsApp*, *Skype* o *Telegram*— supone que una buena parte de las comunicaciones intercambiadas cada día resulten ilegibles por terceros ajenos mientras transitan por la red¹⁰¹.

La criptografía mantiene con el derecho al secreto de las comunicaciones una relación inevitablemente ambivalente, pues si bien refuerza materialmente el secreto comunicacional, obstaculiza su legítima desactivación mediante resolución judicial. Mengua así sensiblemente la capacidad de los poderes públicos de alcanzar los objetivos legítimos vinculados al levantamiento judicial del secreto —típicamente, la investigación de delitos— pues, interceptada una comunicación encriptada, solo se obtendrán datos codificados sin sentido aparente carentes de utilidad para la investigación¹⁰².

Por ello, el uso extendido de la criptografía ha suscitado la preocupación de los Estados en tanto que esta tecnología disminuye su eficacia en la prevención e investigación criminal¹⁰³. Surgen así diferentes

algunos de ellos gratuitos»; cfr. Informe del Parlamento Europeo sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON), de 11 de julio de 2001, apdo. 13.1.

¹⁰¹ «[E]l cifrado ya no se limita a los ordenadores de mesa, sino que está cada vez más disponible en los dispositivos móviles, y muchas plataformas de comunicación disponibles comercialmente cuentan en la actualidad con cifrado por defecto (cada vez más mediante el cifrado de extremo a extremo, que lleva a situaciones en las que los servicios no son interceptables)». Informe 14711/16 de la Presidencia del Consejo de la Unión Europea, 23 de noviembre de 2016, «Cifrado: retos para la justicia penal en relación con el uso del cifrado. Medidas futuras», pág. 2.

¹⁰² GONZÁLEZ NAVARRO, A., «Medios tecnológicos de investigación en el proceso penal alemán: una visión comparada», DÍAZ MARTÍNEZ, M. y LÓPEZ-BARAJAS PEREA, I. (Coords.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant Lo Blanch, Valencia, 2018, pág. 249.

¹⁰³ RIVEST, R.L., «The Case against Regulating Encryption Technology», *Scientific American*, 279, 1998, pág. 116.

propuestas de regulación del uso del cifrado de comunicaciones que se han entendido invasivas —o potencialmente invasivas— del derecho al secreto de las comunicaciones o, más generalmente, de un derecho a la privacidad.

Trataremos de explicar en qué consiste el cifrado de comunicaciones y cómo interacciona con el derecho fundamental considerado, especialmente en lo que respecta a la posibilidad de su limitación.

III.1. El cifrado de comunicaciones

La protección de las comunicaciones frente a posibles interceptaciones —históricamente de enemigos militares o estatales— ha sido una necesidad presente desde la formación de estructuras sociales con una cierta complejidad.

Mucho antes de que se dispensara protección jurídica a las comunicaciones interpersonales, estas se dotaban de diversos sistemas de protección material destinados a evitar su conocimiento. Así, bien mediante la ocultación del mensaje —esteganografía— o bien mediante su codificación —criptografía— se trataban de impedir que ajenos al destinatario conociesen lo transmitido¹⁰⁴.

Ambas técnicas han sido utilizadas desde la antigüedad. La ocultación de la existencia misma del mensaje —la esteganografía— fue utilizada ya en las guerras médicas —escribiendo el mensaje en una tabla de madera y ocultándolo con cera, o directamente en el cuero cabelludo del mensajero enviándolo una vez que le creciese el pelo— y cobró gran importancia durante la Segunda Guerra Mundial mediante la técnica del «micropunto», consistente

¹⁰⁴ Vid. PÉREZ PEREIRA, M., «La evolución de los sistemas de cifrado», *Revista de la Contratación Electrónica*, 75, 2006, pág. 94 y GONZÁLEZ NAVARRO, B.A., «Criptología y libertades públicas», *op.cit.*, pág. 148.

en reducir un texto hasta un tamaño inferior al milímetro y ocultarlo en un signo de puntuación de un texto aparentemente insustancial¹⁰⁵.

No obstante, esta técnica utilizada por sí sola no proporciona una seguridad total, pues, descubierto el mensaje oculto, nada impide que se conozca el contenido comunicado. Por ello, se desarrolla la técnica de la criptografía que, en vez de ocultar el mensaje, pretende ocultar su sentido mediante la codificación del texto transmitido.

Las técnicas criptográficas hacen posible que un texto —texto claro— se convierta en un criptograma —texto cifrado— mediante la aplicación de una serie de operaciones —algoritmo de cifrado—. El elemento más importante es la clave criptográfica, esto es, la información que aplicada al algoritmo permite al emisor cifrar el texto claro y al destinatario descifrar el criptograma¹⁰⁶.

En la criptografía clásica se empleaban criptosistemas simétricos o de clave privada, en los que la misma clave es utilizada tanto para cifrar como para descifrar el mensaje. Por tanto, todos los comunicantes deben conocer la clave, lo que supone un riesgo añadido de posibles interceptaciones de la clave en el momento de su distribución entre comunicantes, haciendo en ese caso inútil el criptosistema¹⁰⁷.

Estos sistemas de cifrado pueden ser de trasposición o de sustitución. En los primeros se altera el orden de las letras, es decir, cada letra cambia su posición, pero mantiene su identidad. Por su parte, en el cifrado de sustitución

¹⁰⁵ SINGH, S., *Los códigos secretos. El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era de Internet*, Editorial Debate, Barcelona, 2000, pág. 20.

¹⁰⁶ DE ASÍS ROIG, A.E., «Artículo 36», *op.cit.*, pág. 561.

¹⁰⁷ MELGAR MARTÍNEZ, L., «4Cs: Ciberseguridad, Confidencialidad, Criptografía y Computación cuántica», *Diario La Ley*, 10, 2017, pág. 4. «Si dos personas quieren intercambiar un mensaje secreto, el emisor debe codificarlo. Para codificar el mensaje secreto, el emisor debe usar una clave, que es en sí misma un secreto, de modo que entonces hay el problema de transmitir la clave secreta al receptor para transmitir el mensaje secreto. En resumen, antes de que dos personas puedan intercambiar un secreto (mensaje codificado) deben ya compartir un secreto (la clave)». SINGH, S., *Los códigos secretos...*, *op.cit.*, pág. 258.

las letras cambian su identidad —por otra letra, par de letras o un símbolo—, pero mantienen su posición en el texto¹⁰⁸.

La evolución de la criptología estuvo marcada, primero, por su mecanización —cuyo ejemplo más notorio fue la máquina *Enigma*— y, posteriormente y con mayor incidencia, por el desarrollo de la informática, lo que supuso nuevos avances en la criptografía clásica permitiendo la generación de claves más seguras y la estandarización de algoritmos —como *DES (Data Encryption Standard)*, desarrollado en 1976 y mundialmente utilizado o *AES (Advanced Encryption Standard)* que reemplazó al anterior en 2001—. Pero el problema de distribuir las claves entre comunicantes seguía presente¹⁰⁹.

La solución llegó mediante la generación de criptosistemas asimétricos o de clave pública, En ellos, la clave de codificación y la de descodificación son distintas, esto es, conociendo la clave de codificación se puede cifrar el mensaje, pero, a diferencia de los sistemas simétricos, no descifrarlo.

De este modo, cada comunicante posee dos claves criptográficas que están relacionadas entre sí, una clave pública, conocida por todos, y una clave privada que solo conoce cada uno de ellos. El emisor utiliza la clave pública del destinatario para codificar el mensaje y éste lo descifra con su clave privada¹¹⁰.

¹⁰⁸ Un ejemplo clásico de sistema de trasposición es la *escitala* espartana, consistente en enrollar una tira de pergamino en un bastón y escribir el mensaje longitudinalmente, por lo que, al desenrollar el pergamino, el texto se desprendía de su sentido original convirtiéndose en una serie de letras sin sentido aparente. El destinatario podía descifrar el criptograma enrollando de nuevo el pergamino en un bastón del mismo diámetro, que actuaba, por tanto, como clave criptográfica. Por su parte, encontramos un ejemplo de sistema de sustitución en la denominada cifra César, consistente en sustituir una letra por aquella que ocupa tres posiciones más en el alfabeto (sustituyendo la A por la D, la B por la E, etc.). Vid. SINGH, S., *Los códigos secretos...*, *op.cit.*, págs. 21 y ss. y PÉREZ PEREIRA, M., «La evolución de los sistemas de cifrado», *op.cit.*, pág. 96.

¹⁰⁹ SINGH, S., *Los códigos secretos...*, *op.cit.*, págs. 252.

¹¹⁰ MELGAR MARTÍNEZ, L., «4Cs: Ciberseguridad, Confidencialidad...», *op.cit.*, pág. 4. La relación entre las dos claves se asemeja a la que mantienen un candado y su llave. Conocer cómo cerrar el candado (clave pública) no te permite sin embargo abrirlo, sino que necesitarás tener la llave (clave privada). SINGH, S., *Los códigos secretos...*, *op.cit.*, págs. 271.

Eliminada la posibilidad de comprometer el sistema criptográfico mediante la interceptación de la clave, la seguridad de los criptosistemas de clave pública se funda en la extraordinaria dificultad matemática, basada en la factorización de números muy grandes, de descubrir en un periodo de tiempo razonable la clave privada a partir de la clave pública conocida¹¹¹.

Sin embargo, la dificultad actual para descifrar claves quizá pueda superarse en un futuro próximo a través de la aplicación computacional de la física cuántica, basada en la teoría de la superposición de estados, comúnmente explicada con la paradoja del gato de Schrödinger¹¹².

Al mismo tiempo, las propiedades de la física cuántica pueden tener importantes aplicaciones en procesos de comunicación que están ya siendo desarrollados. Nos referimos a los principios de entrelazamiento de partículas o teleportación y de indeterminación.

Según el primero, dos partículas entrelazadas están intrínsecamente conectadas, de modo que, con independencia de la distancia que las separe, cualquier acción realizada sobre una de ellas supone un cambio igual en la otra, teleportando así el estado del *qbit* de emisor a receptor¹¹³.

Por su parte, el principio de indeterminación permite detectar cualquier interferencia en el proceso de comunicación, en la medida en que destruye la

¹¹¹ PÉREZ PEREIRA, M., «La evolución de los sistemas de cifrado», *op.cit.*, pág. 98.

¹¹² Mientras que en la computación clásica los *bits* pueden existir en el estado 0 o en el 1, en la computación cuántica los *qbits* o *bits cuánticos* pueden adoptar el estado 0, el estado 1 o los estados 0 y 1 a la vez, del mismo modo que en la conocida paradoja el gato está vivo y muerto al mismo tiempo. Esta superposición permite desarrollar varios procesos de forma simultánea en un ordenador, aumentando exponencialmente la capacidad computacional y, con ello, la posibilidad de criptoanalizar claves factorizadas en unos minutos. MORALES LUNA, G., «Computabilidad y computación cuántica: revisión de modelos alternativos de computación», *Ingeniería Industrial*, 2, 2011, pág. 53. El riesgo que ello supone para los sistemas de cifrado asimétrico generalmente utilizados, como en el comercio electrónico por Internet, ha despertado la necesidad de desarrollar *criptografía poscuántica*, aquella «que busca protocolos convencionales seguros (no cuánticos) ante un ordenador cuántico». RIVERA, A., «Computación cuántica: nuevas reglas del juego para los ordenadores», *Alfa. Revista de seguridad nuclear y protección radiológica*, 27, 2015, pág. 37.

¹¹³ *Vid.* CLEMENTE GALLARDO, J., «Computación y comunicación cuánticas», *Matemática. Revista digital de divulgación matemática*, 4-5, 2007, pág. 6 y MELGAR MARTÍNEZ, L., «4Cs: Ciberseguridad, Confidencialidad...», *op.cit.*, pág. 5.

superposición de estados. El mero intento de medir el estado de un *qbit* transmitido modifica su estado, por lo que un tercero no podría interceptar una comunicación sin ser detectado por los comunicantes¹¹⁴.

Estas tecnologías, que aparenta ciencia ficción para quienes somos profanos, suponen en cualquier caso nuevos retos jurídicos, particularmente para el derecho que analizamos. Tanto los actuales sistemas criptográficos como la previsible criptografía cuántica protegen tecnológicamente el secreto de la comunicación durante su tránsito, incidiendo así en el mismo ámbito de eficacia temporal del derecho al secreto de las comunicaciones y haciendo inútil su apertura para la investigación penal. Lo que exige buscar soluciones ponderadas en un nuevo caso de tensión entre libertad y seguridad.

III.2. Incidencia del cifrado en el derecho fundamental al secreto de las comunicaciones

La prohibición de intervenir comunicaciones junto con la imposición de un deber de confidencialidad a los operadores que las intermedian se han mostrado suficientes para garantizar el secreto de las comunicaciones tradicionales, a la vez que idóneas para alzarlo atendiendo a las garantías legalmente establecidas.

Sin embargo, la aplicación por defecto de técnicas de cifrado a comunicaciones electrónicas de uso generalizado, en la medida en que operan sobre su mismo ámbito temporal, inciden en el derecho fundamental al secreto de las comunicaciones en un doble sentido.

El cifrado se presenta como una garantía técnica de inaccesibilidad al contenido comunicado y, en este sentido, refuerza el secreto normativamente dispuesto¹¹⁵. Pero, a su vez, diluye la posibilidad de desvelar el contenido

¹¹⁴ RIVERA, A., «Computación cuántica...», *op.cit.*, pág. 38 y MELGAR MARTÍNEZ, L., «4Cs: Ciberseguridad, Confidencialidad...», *op.cit.*, pág. 5.

¹¹⁵ La Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que introdujo por primera vez con carácter general disposiciones relativas al uso del cifrado en las telecomunicaciones,

también en aquellos casos en que la ruptura del secreto sea constitucionalmente legítima, convirtiendo un secreto jurídicamente relativo en tecnológicamente exorbitante para el instituto jurídico iusfundamental que analizamos¹¹⁶.

Por ello, la generalización del uso de sistemas criptográficos provocó la reacción de los Estados que, al ver limitada su capacidad legítima de interceptar comunicaciones y, por tanto, sus funciones de mantenimiento de la seguridad pública y persecución delictiva, propusieron establecer restricciones al uso del cifrado¹¹⁷.

Las eventuales soluciones en este frágil binomio libertad-seguridad abarcarían desde la absoluta prohibición del uso de criptografía hasta su total libertad, pasando por soluciones intermedias como el depósito de claves de cifrado. Es por tanto necesario determinar en qué medida el reconocimiento de un derecho fundamental al secreto de las comunicaciones puede influir en los posibles modos de regular el uso de técnicas de cifrado. Lo que exige responder a determinadas preguntas. ¿El derecho a cifrar comunicaciones forma parte del contenido del derecho fundamental? ¿Debe el Estado tener asegurada la posibilidad de interceptar comunicaciones encriptadas?

El contenido esencial del derecho fundamental al secreto de las comunicaciones, aquello que se impone a la voluntad del legislador, se identifica con la prohibición constitucional de desvelar la comunicación, a la vez que eximir de dicha prohibición, en los presupuestos legalmente

dispone en su Exposición de Motivos, que su objetivo es «garantizar técnicamente los derechos fundamentales constitucionalmente reconocidos».

¹¹⁶ De apostar por la absoluta permisibilidad de uso de un cifrado fuerte, en principio, «la protección del secreto de las comunicaciones sería absoluta, pero la imposibilidad de realizar interceptaciones o un control por parte de las autoridades públicas también». TINTO GIMBERNAT, M., «El secreto de las comunicaciones electrónicas...», *op.cit.*, pág. 255.

¹¹⁷ RIVEST, R.L., «The Case against...», *op.cit.*, pág. 116. No obstante, la búsqueda de soluciones que permitiesen acceder al contenido de comunicaciones cifradas no son en absoluto novedosas. En España, ya la Orden de 2 de junio de 1933, sobre Telegramas convenidos y cifrados, si bien permitía el envío de telegramas con texto cifrado, era condición indispensable facilitar al operador, junto con el contenido cifrado, la reproducción en claro de su contenido. *Vid.* DE ASÍS ROIG, A.E., «Artículo 36», *op.cit.*, pág. 571.

dispuestos y con la debida autorización judicial que exprese motivadamente la superación del juicio de idoneidad, necesidad y proporcionalidad.

La criptografía, sin embargo, guarda con el derecho fundamental una relación de instrumentalidad en la que claramente puede diferenciarse derecho protegido y artificio tecnológico para su preservación, pero en ningún caso el uso de la criptografía forma parte del contenido esencial del derecho fundamental al secreto de las comunicaciones¹¹⁸. Por tanto, y pese a determinadas afirmaciones, no puede identificarse en el art. 18.3 CE un derecho constitucionalmente garantizado a la utilización de sistemas de cifrado de comunicaciones —al modo como tampoco del 18.2 puede extraerse un derecho a utilizar puertas blindadas—¹¹⁹.

La decisión sobre el modo de regular la criptografía es, por tanto, de carácter político o de oportunidad. Sin embargo, no se trata de una decisión incondicionada pues, en la medida en que el uso de la criptografía puede incidir, como garantía material de carácter tecnológico, en la efectividad del derecho fundamental al secreto de las comunicaciones —y en la de otros— deberá tener en cuenta el sistema iusfundamental que la Constitución configura.

Los derechos fundamentales, como reconoció ya en sus primeras resoluciones el Tribunal Constitucional, además de declarar derechos subjetivos, poseen una dimensión objetiva que se proyecta sobre el

¹¹⁸ DE ASÍS ROIG, A.E., «Artículo 36», *op.cit.*, págs. 570-571.

¹¹⁹ Debemos rechazar, por ello, ciertas afirmaciones que consideran, por ejemplo, que «[l]as restricciones al derecho de uso de la criptografía atacan a la misma línea de flotación del derecho fundamental que está garantizando», cfr. GONZÁLEZ NAVARRO, B.A., «Criptología y libertades públicas», *op.cit.*, pág. 203. En similar sentido, se ha afirmado que «restringir legislativamente el uso de criptografía supondría convertir la excepción en norma» y que «[e]n una situación de normalidad democrática, es un derecho fundamental utilizar aquellas herramientas que permitan asegurar el secreto de las comunicaciones»; SÁNCHEZ ALMEIDA, C., «España: La Criptografía como derecho», *Revista Electrónica de Derecho Informático*, 23, 2000, pág. 2.

ordenamiento jurídico (son, en palabras del art. 10.1 CE, «fundamento del orden político y de la paz social»)¹²⁰.

En su dimensión objetiva los derechos fundamentales se comportan como directrices constitucionales y reglas de actuación legislativa, como «la expresión jurídica de un sistema de valores que, por decisión del constituyente, ha de informar el conjunto de la organización jurídica y política» y, en consecuencia, los poderes públicos están obligados a contribuir a su efectividad¹²¹.

Por ello, en la medida en que el art. 18 CE enuncia una serie de derechos tendentes a garantizar espacios de inmunidad en la vida privada del individuo y a cuya efectividad puede contribuir el uso de técnicas de cifrado —secreto de las comunicaciones, pero también intimidad y protección de datos respecto de la aplicación del cifrado a otras transacciones que no son comunicaciones en el sentido del 18.3 CE—, consideramos que su total prohibición no es una opción atendible¹²².

A la hora de inclinar la balanza en la tensión libertad-seguridad deben ponderarse además otras razones que invitan a rechazar la posibilidad de prohibir totalmente el uso de criptografía. Existen, como veremos, opciones de

¹²⁰ «En primer lugar, los derechos fundamentales son derechos subjetivos, derechos de los individuos no sólo en cuanto derechos de los ciudadanos en sentido estricto, sino en cuanto garantizan un status jurídico o la libertad en un ámbito de la existencia. Pero al propio tiempo, son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado social de Derecho o el Estado social y democrático de Derecho, según la fórmula de nuestra Constitución (art. 1.1)», *vid.* STC 25/1981, de 14 de julio (FJ. 5).

¹²¹ STC 53/1985, de 11 de abril (FJ. 4).

¹²² Como reflejo de la dimensión objetiva de los derechos fundamentales, la obligación de su protección por parte del Estado se concreta en la fijación de una obligación de prohibición, una obligación de garantía y una obligación de prevención. En lo que aquí nos interesa, esta última obligación de prevención «implica la adopción y exigencia de condiciones y requisitos en relación a conductas para permitir el disfrute pleno del derecho antes de que se produzca lesiones o perjuicios». La criptografía satisface, sin duda, esa capacidad instrumental para proteger el derecho de forma anticipada a su vulneración. Cfr. GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva de los derechos fundamentales: el art. 10.1 CE*, Bosch, Barcelona, 2011, págs. 89-90.

regulación menos gravosas e igualmente eficaces para la finalidad pretendida. Pero además se debe tener en cuenta que, si bien puede ser utilizado en ocasiones para obstaculizar la investigación criminal, el cifrado de comunicaciones tiene sobre todo una gran capacidad para evitar la comisión de determinados delitos, como el fraude en operaciones bancarias a través de la red o el espionaje industrial¹²³.

La solución pasa, por tanto, por adoptar un sistema que permita el uso de técnicas de cifrado y, al mismo tiempo, garantice el normal desarrollo de las actividades estatales dirigidas a salvaguardar la seguridad.

Este es el sentido de los sistemas de depósito y recuperación de claves, esto es, la imposición a usuarios y fabricantes de tecnología de encriptación de la obligación de depositar en ciertos organismos de confianza (*Trusted Third Partys*, TTP's) las claves, siendo entregadas a las autoridades cuando sea necesario acceder a la información cifrada¹²⁴.

El depósito de claves —*key escrow*— consiste en la entrega a un TTP de una copia de cualquier clave de cifrado generada, como encargado de su custodia y cesión a las autoridades en los casos establecidos. Por su parte, en los sistemas de recuperación de claves —*key recovery*— es el propio sistema de cifrado el que permite a los organismos de confianza reconstruir la clave a petición de la autoridad legitimada para ello. En ambos casos se consigue la finalidad pretendida, reforzando el secreto de las comunicaciones a través de la garantía técnica de cifrado y permitiendo a su vez el acceso a los contenidos transmitidos en una eventual investigación penal. Sin embargo,

¹²³ Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, 8 de octubre de 1997, «Garantizar la seguridad y la confianza en la comunicación electrónica. Hacia un marco europeo para la firma digital y el cifrado». Se ha comparado el uso de la criptografía con el uso de los guantes. Si bien los guantes pueden ser utilizados para cometer robos, obstaculizando el análisis de huellas dactilares por parte de las autoridades encargadas de la investigación penal, en la mayoría de las ocasiones se utilizan para proteger las manos de lesiones o del frío. RIVEST, R.L., «The Case against...», *op.cit.*, pág. 116.

¹²⁴ TINTO GIMBERNAT, M., «El secreto de las comunicaciones electrónicas...», *op.cit.*, pág. 256.

una vez que la clave ha sido entregada o reconstruida, todas las comunicaciones encriptadas con dicha clave son potencialmente descifrables¹²⁵.

Esta es la posibilidad por la que parece optar el legislador español desde la Ley 11/1998, de 24 de abril, General de Telecomunicaciones. Su art. 52, bajo la rúbrica *Cifrado en las redes y servicios de telecomunicaciones*, establecía, en su apartado primero, la posibilidad de proteger mediante procedimiento de cifrado cualquier información transmitida por redes de telecomunicaciones. No obstante, el apartado segundo del mismo artículo establecía lo siguiente:

«El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, *se podrá imponer la obligación de notificar bien a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado*, a efectos de su control de acuerdo con la normativa vigente. Esta obligación afectará a los fabricantes que incorporen el cifrado en sus equipos o aparatos, a los operadores que lo incluyan en las redes o dentro de los servicios que ofrezcan y, en su caso, a los usuarios que lo empleen».

Sin apenas variaciones, sus términos pasaron al artículo 36 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y, posteriormente, al hoy vigente artículo 43 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. Sin embargo, pese a la posibilidad legalmente permitida de establecer un sistema de depósito de claves de cifrado, más de once años después aún no se ha llevado a la práctica¹²⁶.

¹²⁵ Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, 8 de octubre de 1997, «Garantizar la seguridad y la confianza en la comunicación electrónica. Hacia un marco europeo para la firma digital y el cifrado», anexo III, pág. IX.

¹²⁶ El sistema de depósito de claves no es desconocido para el ordenamiento jurídico español. El artículo 715 del Reglamento para el Régimen y Servicio Interior del Cuerpo de Telecomunicación de 1900, en redacción modificada por la Orden de 4 de diciembre de 1945, establecía: «Los telegramas pueden redactarse en lenguaje claro o en lenguaje secreto [...]».

Con todo, la solución del depósito no ha estado tampoco exenta de críticas, centradas principalmente en la facilidad para eludir estos sistemas por quienes necesitan mantener sus comunicaciones cifradas para delinquir — modificando el *software* de cifrado o adquiriendo sistemas alternativos— y en la posibilidad de que las puertas traseras habilitadas con las claves depositadas se conviertan en objetivos para los delincuentes¹²⁷. Pero, sobre todo, por la incidencia que un sistema de este tipo puede generar en la confianza de los ciudadanos, creando una atmósfera de sospecha constante¹²⁸.

Pese a ello, a nuestro juicio, los sistemas de depósito y recuperación de claves resultan *a priori* perfectamente compatibles con el derecho fundamental al secreto de las comunicaciones, si bien este exige también la existencia de mecanismos que aseguren que los poderes públicos solo podrán acceder a las claves de descifrado atendiendo a las mismas garantías previstas para la intervención de comunicaciones no cifradas, o incluso exigiendo un plus de motivación respecto a la necesidad de intervenir comunicaciones cifradas respecto a las transmitidas sin protección.

Es preciso en todo caso prever un sistema que permita a las autoridades encargadas de la persecución penal acceder al contenido de comunicaciones encriptadas pues, de lo contrario, el carácter absoluto del secreto haría inútil

El lenguaje secreto puede ser convenido, cifrado y de letras que tengan significación secreta, [...] debiendo presentar los expedidores [...] cuando se les pida, las claves o vocabularios que usen». Vid. DE ASÍS ROIG, A.E., «Artículo 36», *op.cit.*, pág. 582.

¹²⁷ «Pretender afianzar la lucha contra el crimen mediante la imposición de normas jurídicas en la utilización del cifrado, cuando el adversario se caracteriza precisamente por su desprecio hacia ellas, resulta al menos ilusorio»; cfr. GONZÁLEZ NAVARRO, B.A., «Criptología y libertades públicas», *op.cit.*, pág. 208.

¹²⁸ Siguiendo la analogía entre el uso de guantes y el de tecnologías de cifrado, se ha comparado la obligación de depósito de claves con una hipotética obligación de coser copias de látex de las huellas dactilares en la punta de los dedos de los guantes. RIVEST, R.L., «The Case against...», *op.cit.*, pág. 117. Vid., igualmente, GALINDO AYUDA, F., «La conveniencia de una regulación española del cifrado de las comunicaciones electrónicas», *Diario La Ley*, 4708, 1999, pág. 1.

definir la posibilidad de limitar el derecho y, a su través, innecesaria su protección jurídica¹²⁹.

No obstante, consideramos más apropiado establecer soluciones singulares, técnicamente posibles, que prevén el acceso a contenidos de comunicaciones encriptadas caso por caso y sin establecer una regulación general que incida en los elementos internos de los sistemas de cifrado.

Se trataría en definitiva de aplicar técnicas de descifrado sobre las comunicaciones concretas ya intervenidas; o de buscar fórmulas alternativas que permitan acceder al contenido de las comunicaciones en los momentos en que no está protegido por el sistema de cifrado.

III.3. Intervención de comunicaciones cifradas

Descartada la absoluta prohibición del uso de técnicas de cifrado y considerando innecesaria una regulación general sobre las claves, se trata ahora de hallar técnicas que permitan a los poderes públicos acceder al contenido de comunicaciones encriptadas respetando las garantías iusfundamentales.

Existen, a grandes rasgos, dos posibilidades. Por un lado, operar sobre las comunicaciones en tránsito y despojarlas del cifrado mediante el recurso a técnicas diversas; por otro, cuando esto no sea posible o altamente ineficiente, accediendo en aquellas fases del proceso comunicativo en que el cifrado no sea operativo.

¹²⁹ En similar sentido, *vid.* RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, págs. 129-131.

A. Interceptación del contenido comunicacional mediante ataques de suplantación

Una primera posibilidad consistirá en que el sujeto que ejecute la intervención conozca las claves de cifrado utilizada por los comunicantes, lo que puede tener lugar, más allá de los casos de depósito y recuperación de claves, llevando a cabo, con éxito, un ataque de suplantación.

Un ataque de suplantación, de intermediario o *man-in-the-middle attack* consiste en conseguir que el emisor se comunique con el intermediario haciéndole creer que se está comunicando con el receptor, de modo que el intermediario, una vez accedido el contenido comunicado, lo retransmita al verdadero destinatario sin rastro de la intervención suplantadora.

En el caso de comunicaciones cifradas con clave asimétrica, una vez suplantada la identidad del destinatario por el intermediario, el emisor cifra el contenido de la comunicación utilizando la clave pública del intermediario, que éste puede descifrar utilizando su clave privada. A continuación, el intermediario transmite la información al destinatario verdadero cifrándola con su clave pública, para que éste la descifre con su clave privada y concluya el proceso comunicativo¹³⁰.

De este modo, el intermediario obtiene la información transmitida mientras que los interlocutores permanecen en la confianza de haber mantenido una comunicación reservada.

No obstante, esta forma de intervenir comunicaciones cifradas se tornará ineficaz en caso de que los interlocutores dispongan de claves públicas certificadas por terceros, pues, cuando el emisor solicite al organismo

¹³⁰ MORENO FONTELA, J.L., «Servicios cifrados de extremo a extremo e investigación penal bajo derecho español», VALLS PRIETO, J. (Coord.), *Retos jurídicos por la sociedad digital*, Aranzadi, Cizur Menor, 2018, pág. 281.

certificador la clave pública del destinatario recibirá la clave del intermediario, siendo descubierta la suplantación¹³¹.

B. Remoción de las técnicas de cifrado con auxilio de terceros

Para la remoción de las técnicas de cifrado la autoridad puede recabar el auxilio de determinados sujetos.

Por un lado, el art. 39.11 LGT —reproducido en el art. 96 RLGT— dispone el deber de proporcionar a las autoridades, en determinadas circunstancias, las comunicaciones intervenidas en formato inteligible:

«En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles».

Pese a que algunos autores han considerado que se trata de una obligación de resultado¹³², la misma resulta condicionada por los términos en que se expresa la norma, que solo se impone cuando sean los propios sujetos obligados quienes apliquen el cifrado a las comunicaciones y, en todo caso, siempre que el mismo sea reversible¹³³.

Por otro lado, el art. 588 ter.e LECrim impone un deber de prestar a las autoridades —Juez, Ministerio Fiscal y agentes de la Policía Judicial— «la

¹³¹ Con todo, el deber de colaboración que, como veremos, prevé la actual regulación de la intervención de las comunicaciones, puede permitir al juez requerir a la autoridad de certificación la expedición de certificados falsos que avalen la suplantación; *vid.* MORENO FONTELA, J.L., «Servicios cifrados...», *op.cit.*, pág. 281.

¹³² «[...] en todo caso el operador de telecomunicaciones incumpliría sus obligaciones siempre que no ejecutase las interceptaciones de manera que se acceda o transmita la información libre de los efectos de las diferentes técnicas criptográficas»; *cfr.* MORENO FONTELA, J.L., «Servicios cifrados...», *op.cit.*, pág. 286.

¹³³ RODRÍGUEZ LAINZ, J.L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», *Diario La Ley*, 8896, 2017, págs. 1-2.

asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones».

Este deber de colaboración es más amplio que el previsto en la LGT, extendiéndose también a particulares, ajenos a la explotación de recursos públicos¹³⁴.

Así, el art. 588 ter.e LECrim se dirige, en primer lugar, a los obligados por la LGT, esto es, a los prestadores de servicios de telecomunicaciones y de acceso a redes de telecomunicaciones. Pero la obligación se extiende también tanto a los prestadores de servicios de la sociedad de la información, como a «toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual», donde debe entenderse incluido tanto el responsable de una red informática privada como el propietario de un dispositivo utilizado por el investigado para comunicarse¹³⁵.

Pero tampoco el recurso a la asistencia técnica de terceros es un método totalmente satisfactorio para el descifrado de comunicaciones.

Por un lado, los sistemas comunicativos implementan crecientemente sistemas de cifrado extremo a extremo en que las claves se almacenan únicamente en los propios dispositivos de los comunicantes, no siendo conocido el contenido intercambiado por los operadores del servicio¹³⁶.

Por otro, la indeterminación de la regulación del deber de colaboración y la colisión de intereses que puede producirse en algunos casos, puede conllevar que determinados expertos se nieguen legítimamente a prestar la asistencia técnica requerida¹³⁷.

¹³⁴ Circular de la Fiscalía General del Estado, 2/2019, sobre interceptación de comunicaciones telefónicas y telemáticas, apdo. 7, pág. 24.

¹³⁵ *Ibidem*.

¹³⁶ MORENO FONTELA, J.L., «Servicios cifrados...», *op.cit.*, pág. 291; y VIDAL, G. y MORENO, J.L., «Cryptography and Communications Privacy...», *op.cit.*, pág. 528.

¹³⁷ Aunque referido a encriptación de datos almacenados en un dispositivo, así sucedió durante la investigación por parte del FBI del atentado de San Bernardino. Frente a la solicitud

C. Descifrado mediante técnicas de criptoanálisis

Finalmente, una última vía para acceder al contenido de comunicaciones encriptadas consiste en la intervención del mensaje cifrado y su conversión a texto descifrado aplicando técnicas de criptoanálisis.

El criptoanálisis es la ciencia matemática que se ocupa del análisis de los sistemas criptográficos con el objetivo de romper o eludir la protección que el sistema proporciona¹³⁸.

Si bien la ruptura de sistemas de cifrado con claves matemáticamente fuertes puede resultar en ocasiones ineficiente por su alto coste de tiempo o recursos, la incorporación de este tipo de funcionalidades a herramientas de interceptación de comunicaciones es cada vez más habitual¹³⁹.

Esta parece ser la solución adoptada en el caso español, incorporando en el año 2018 una actualización de la plataforma SITEL que permite la intervención de comunicaciones mantenidas a través de sistemas de intercambio de mensajería instantánea que incorporan cifrado de extremo a extremo¹⁴⁰.

D. Registro remoto de dispositivos como técnica de intervención de comunicaciones

Otra opción para sortear el cifrado de las comunicaciones pasa por llevar a cabo la intervención en aquellos momentos del proceso comunicativo en que las técnicas de encriptación no tienen incidencia en el contenido

judicial de asistencia a *Apple* para que habilitase una *puerta trasera* que permitiese acceder a los datos del dispositivo, la empresa se negó alegando la puesta en peligro de la privacidad del resto de los usuarios de sus dispositivos. Sobre este asunto, *vid.* ETZIONI, A., «Apple: Good Business, Poor Citizen?», *Journal of Business Ethics*, 151, 2018, págs. 1-11.

¹³⁸ VIDAL, G. y MORENO, J.L., «Cryptography and Communications Privacy...», *op.cit.*, pág. 513.

¹³⁹ RODRÍGUEZ LAINZ, J.L., «Intervención judicial de comunicaciones...», *op.cit.*, pág. 2.

¹⁴⁰ «Interior gasta 6,2 millones en mejorar su sistema de escuchas», noticia publicada en el diario *El País* en fecha 13 de noviembre de 2018 (disponible en: <https://cutt.ly/pr1nNXc>).

comunicado, lo que sucede bien accediendo a las albergadas en el dispositivo del emisor, bien a las recibidas y descifradas en el del destinatario.

En este sentido, los sistemas comunicativos que incorporan cifrado extremo a extremo conservan por defecto los contenidos comunicados y ya descifrados en el dispositivo, salvo que se proceda a su borrado por parte de los interlocutores.

Por ello, es posible acceder a los contenidos intercambiados sin interceptación de la señal soportada por la red pública de comunicaciones, accediendo a la fuente de origen o de destino: ya sea antes de que la encriptación se produzca —en el sistema del emisor—, ya después de que la comunicación cifrada se convierta a texto claro —en el dispositivo receptor—

141.

El acceso a los contenidos almacenados se puede llevar a cabo mediante el registro físico del dispositivo o mediante su registro remoto.

En el primer caso (arts. 588 sexies.a y ss. LECrim), el registro se practica sobre el contenido albergado en el dispositivo o sistema estáticamente considerado y los archivos que contengan en el momento de su práctica. En este caso, el acceso se producirá sobre comunicaciones pretéritas, cuyos contenidos —devenidos datos— se hallarán protegidos, en su caso, por los derechos a la intimidad y/o a la protección de datos y no, según dijimos, por el derecho al secreto de las comunicaciones.

Por su parte, el registro remoto (arts. 588 septies.a y ss. LECrim) está caracterizado por las notas de clandestinidad y dinamismo del examen de los contenidos alojados. A través de esta técnica se puede conocer no sólo el contenido del dispositivo en un momento determinado, sino también los

¹⁴¹ GONZÁLEZ NAVARRO, A., «Medios tecnológicos de investigación...», *op.cit.*, pág. 250; RODRÍGUEZ LAINZ, J.L., «Intervención judicial de comunicaciones...», *op.cit.*, pág. 4; y RICHARD GONZÁLEZ, M., *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*, La Ley, Madrid, 2017, pág. 207.

archivos que se vayan añadiendo o suprimiendo durante el tiempo de observación¹⁴².

Este carácter dinámico y subrepticio permite que, mediante esta técnica, sea posible interceptar las comunicaciones en tiempo real, poniéndose a disposición del agente que ejecute su práctica los contenidos comunicados y descifrados en el mismo momento y condiciones en que están siendo recibidos por el destinatario.

El recurso al registro remoto de dispositivos como técnica de intervención de comunicaciones ha sido la solución adoptada en algunos ordenamientos, como el alemán, para el acceso a comunicaciones cifradas.

No obstante, el legislador español no ha previsto diferencias entre la intervención de comunicación cifradas y no cifradas, ni regulado el registro remoto como una técnica de intervención de comunicaciones, sino en forma de diligencia de acceso a los contenidos almacenados en sistemas o dispositivos informáticos. Estas dos diligencias están sujetas, así, a un régimen jurídico diferenciado (arts. 588 ter y 588 septies LECrim), previéndose para una y otras diferentes presupuestos habilitantes y duración de la medida¹⁴³.

La utilización de la técnica del registro remoto para intervenir comunicaciones cifradas no parece encontrar problemas jurídicos insalvables.

¹⁴² Circular de la Fiscalía General del Estado, 2/2019, sobre interceptación de comunicaciones telefónicas y telemáticas, apdo. 4.1, págs. 52 y ss. La práctica de esta medida requiere el acceso al dispositivo mediante la introducción de un programa espía que permita a la autoridad encargada de su ejecución tomar el control del dispositivo objeto de examen. Normalmente este acceso se lleva a cabo aprovechando la conexión del dispositivo a una red pública o privada, valiéndose de canales abiertos de compartición de información —*bluetooth*, *NFC*, etc.— o mediante su incorporación oculta adjunta a una comunicación o archivo descargable; aunque, en ocasiones, será necesario manipular manualmente el dispositivo. El deber de colaboración, también previsto con ocasión de la regulación de esta diligencia (art. 588 septies.b LECrim), puede ser aquí útil para facilitar asistencia técnica sobre posibles vías de acceso al terminal o para solicitar al prestador que abra una vía de penetración al troyano (por ejemplo, disponiendo restricciones a la protección del antivirus). *Vid.* RODRÍGUEZ LAINZ, J.L., «Intervención judicial de comunicaciones...», *op.cit.*, pág. 2.

¹⁴³ VALVERDE MEGÍAS, R., «Intervención de comunicaciones telemáticas y registro remoto», *La interceptación de las comunicaciones telefónicas y telemáticas*, Jornadas de Formación del Centro de Estudios Jurídicos, 27 de abril de 2016, pág. 39.

El programa que debe instalarse en el dispositivo para que la autoridad encargada pueda examinarlo remotamente debe ser previamente configurado para el caso concreto y, por ello, es posible limitar su uso a la exclusiva captación de determinadas comunicaciones. De este modo, con independencia de la técnica utilizada, la intervención se circunscribe solamente a aquellos contenidos autorizados judicialmente y con las mismas garantías que en el caso de una interceptación de comunicaciones en curso¹⁴⁴.

En este supuesto, el régimen jurídico aplicable debe conectarse con el contenido de la medida y no con la técnica empleada. Así, la autorización dirigida solamente a la intervención de comunicaciones, aunque sea ejecutada mediante el registro remoto del dispositivo, deberá someterse al régimen previsto en los arts. 588 ter.a y siguientes de la Ley de Enjuiciamiento Criminal¹⁴⁵.

Podemos concluir, así, que existen diversas posibilidades de intervenir con éxito comunicaciones encriptadas sin necesidad de establecer una regulación general sobre las claves de cifrado.

No existe, sin embargo, una única solución, sino que la decisión de recurrir a una u otra de las técnicas aludidas —ataque de suplantación,

¹⁴⁴ «Que el programa del teléfono sea un troyano y el sistema de interceptación “exterior” sea un *sniffer* es irrelevante: lo importante es que en ambos casos el sistema utilizado ejecute satisfactoriamente y con garantías todo aquello —pero sólo aquello— para lo que ha sido autorizado judicialmente»; cfr. VALVERDE MEGÍAS, R., «Intervención de comunicaciones telemáticas y registro remoto», *op.cit.*, págs. 40-41. La regulación procesal penal alemana — art. 100.a) *Strafprozessordnung*— permite «intervenir y grabar contenidos y datos de la comunicación almacenados en el sistema informático del investigado, si los mismos también hubieran podido ser intervenidos y grabados de forma encriptada mientras estuviera pendiente el proceso de transmisión en la red pública de telecomunicaciones». *Vid.* GONZÁLEZ NAVARRO, A., «Medios tecnológicos de investigación...», *op.cit.*, págs. 263 y ss.

¹⁴⁵ En favor de este entendimiento se manifiesta la Circular de la Fiscalía General del Estado, 2/2019, sobre interceptación de comunicaciones telefónicas y telemáticas, apdo. 4.1, pág. 54. Asimismo, RODRÍGUEZ LAINZ, J.L., «Intervención judicial de comunicaciones...», *op.cit.*, pág. 11.

criptoanálisis o registro remoto— dependerá de la eficacia y proporcionalidad de su uso en el caso concreto.

Por su parte, el deber de colaboración de terceros técnicamente solventes se presenta como un recurso de carácter transversal a los problemas que surgen con ocasión de la necesidad de intervenir comunicaciones así protegidas.

La colaboración de los prestadores de servicios de telecomunicaciones puede resultar útil por sí misma, a través de la obligación de deshacer el cifrado por ellos implementado (art. 39 LGT). Pero también la prestación de asistencia de otros sujetos en tareas concretas necesarias para la ejecución de las diversas medidas: expedición de claves falsas que garanticen el éxito del ataque de suplantación, desarrollo de programas de criptoanálisis o apertura de *backdoors* en los dispositivos que posibiliten su registro¹⁴⁶.

¹⁴⁶ En jerga informática se denomina *backdoor* o puerta trasera la introducción de secuencias especiales en los códigos de programación como medios de obtener acceso a un programa o sistema evitando sus controles de seguridad. *Vid.* «puerta trasera» en *Diccionario Español de Ingeniería, sección Informática* (consulta online en: <http://diccionario.raing.es/es>).

CAPÍTULO CUARTO

SECRETO DE LAS COMUNICACIONES Y DATOS DE TRÁFICO

I. INTRODUCCIÓN

II. DATOS DE TRÁFICO: CONCEPTO Y REGULACIÓN

II.1. Datos de tráfico y datos *afines*

II.2. El uso de datos de tráfico en la investigación penal

A. La conservación generalizada de datos

B. La preservación de datos almacenados

C. La interceptación de datos en tiempo real

III. DATOS DE TRÁFICO Y DERECHOS FUNDAMENTALES AFECTADOS

III.1. Interceptación de datos de tráfico asociados a comunicaciones en curso

III.2. Acceso a datos de tráfico asociados a comunicaciones consumadas

A. Datos en poder del prestador del servicio

B. Datos en poder de los comunicantes

I. INTRODUCCIÓN

Toda comunicación genera un conjunto de datos precisos para su desarrollo.

Son datos *asociados* a toda comunicación que, aún *distintos y ajenos* al contenido, constituyen un nexo imprescindible con el proceso comunicacional. Entre ellos la identificación de emisor y destinatario —o *lugar* de entrega— y, en su función, la *ruta* —encaminamiento— que debe seguir para su adecuada transmisión.

Cuando nos ocupamos del ámbito objetivo del secreto en el art. 18.3 CE ya dejamos sentado el carácter formal del proceso y su proyección sobre la totalidad del proceso comunicativo: existencia de comunicación, contenido intelectual (mensaje) y datos externos asociados.

De hecho, habrá ocasiones en que estos últimos constituyan justamente el único contenido amparado por el secreto. En una comunicación infructuosa — *llamada perdida* en jerga de comunicación telefónica— no llegará a existir una transmisión de expresiones, pero sí el conjunto de datos reflejo del intento frustrado (número telefónico de origen y destino, hora de la llamada, encaminamiento, ...) cuyo secreto se hallará, según dejamos dicho, igualmente protegido.

El reconocimiento de esos datos como parte integrante del objeto del derecho al secreto de las comunicaciones se declaró en STC 114/1984, fruto de la integración, vía 10.2 CE, de la interpretación del TEDH en *Malone c. Reino Unido*.

El Tribunal de Estrasburgo enjuició la conformidad con el art. 8 CEDH del registro mediante contador (*metering* o *comptage*, en las versiones oficiales en inglés y francés), consistente en el «uso de un instrumento —un contador con reflejo

impreso— que registra los números marcados en un determinado aparato telefónico y la hora y duración de la llamada»¹.

No obstante, las actuales y mucho más amplias posibilidades técnicas de recopilación de datos confieren hoy a los prestadores del servicio de telecomunicaciones, el conocimiento de datos de valor y significado exorbitante respecto de los concretos procesos de comunicación. Ello requiere deslindar aquellas categorías de datos que forman parte del objeto del derecho de otras que, en su caso, encontrarán protección en otros derechos.

Una importancia mayor, y creciente, ha adquirido la determinación del ámbito temporal de la comunicación objeto del derecho. Nótese que la protección no puede alcanzar sino a la secuencia temporal asociada a la comunicación realizada. Ello obliga a una determinación rigurosa de los datos protegidos ex 18.3 CE ajustada al tiempo preciso en que la comunicación se desarrolla.

En la interpretación de estos dos elementos —delimitación objetiva y temporal del derecho al secreto de las comunicaciones— anidan las mayores discrepancias doctrinales y jurisprudenciales sobre el régimen jurídico de los datos de tráfico, agravadas por una deficiente y ajetreteada regulación normativa. Añádanse a ello los problemas derivados del acoplamiento de nuestro sistema iusfundamental a los pronunciamientos de tribunales supranacionales que manejan derechos cuyos objetos no se compadecen, en delimitación y alcance, con los de similar, pero no igual, naturaleza garantizados por nuestra Constitución.

¹ STEDH de 2 de agosto de 1984 (asunto *Malone c. Reino Unido*, § 56).

II. DATOS DE TRÁFICO: CONCEPTO Y REGULACIÓN

II.1. Datos de tráfico y datos *afines*

Cuando entablamos una comunicación electrónica se generan —de modo ajeno a las voluntades de emisor y receptor— una serie de datos que el propio artefacto precisa para posibilitar técnicamente la comunicación. Además, los proveedores de servicios de comunicaciones pueden tener acceso, por la propia naturaleza tecnológica del proceso y/o la relación contractual constituida, a otros datos no estrictamente vinculados ni asociados a procesos comunicativos concretos. Su variada gama requiere aclarar algunos conceptos.

Determinantes para el derecho fundamental objeto del presente trabajo son los datos de tráfico, esto es, aquellos «que se generan o tratan en el curso de una comunicación y que difieren del contenido material, entendiéndose por tal aquella información cuya transmisión voluntaria por el emisor al receptor motiva la comunicación»².

No obstante, existen datos cuya adscripción a esta categoría es dudosa y otros que, pese a su relación con los anteriores, deben quedar excluidos.

Así, en primer lugar, son «datos indubitadamente de tráfico» aquellos que tienen su origen en el proceso de comunicación y que no existirían si no se hubiera activado. Se hallan vinculados a la comunicación por una relación de dependencia funcional de naturaleza tecnológica. En esta categoría se incluyen los datos indicativos del origen de la comunicación (p.ej., número de teléfono del emisor), del destino de la comunicación, de la ruta seguida por la comunicación o encaminamiento, del momento y duración de la comunicación, del volumen de la información transmitida y del tipo de comunicación³.

Pese a que algunos autores parecen individualizar los datos de facturación, algún otro ha propuesto su exclusión como categoría autónoma por cuanto serían

² GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, pág. 62.

³ *Ibid.*, págs. 63 y ss.

solo una parte de los datos de tráfico que el operador utiliza para facturar los servicios prestados⁴.

En segundo lugar, serán «datos eventualmente de tráfico» aquellos que ocasionalmente pueden ser calificados, o no, como de tráfico: lo que sucede porque no siempre aparecen vinculados a procesos de comunicación. El mejor ejemplo es el de los datos de localización. Estos datos pueden ser de tráfico, cuando resultan precisos para realizar una comunicación, pero también pueden ser utilizados por los operadores para ubicar el dispositivo en el espacio radioeléctrico (datos de cobertura) o incluso cuando el contenido material en que la comunicación consiste es la localización misma (por ejemplo, cuando la enviamos vía *WhatsApp*)⁵.

Por último, quedan excluidos del concepto de datos de tráfico, los «datos de suscripción o de abonado», aquellos que el prestador del servicio de comunicación recaba del abonado al suscribir el contrato. No son datos de tráfico, pues son generados previamente a cualquier comunicación y no están ligados a la realización de una comunicación concreta. No obstante, alguno de estos datos —número de teléfono asignado al contratar el servicio— es también y simultáneamente dato de tráfico en el curso de una comunicación⁶.

⁴ Así, el art. 2 b) de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, define los datos de tráfico como «cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efecto de facturación de las mismas». En contra de la inclusión de estos últimos en la categoría de datos de tráfico, GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, pág. 63-75.

⁵ Los datos de localización son definidos en el art. 2.c) de la Directiva 2002/58/CE como «cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible al público». *Vid.* GONZÁLEZ LÓPEZ, J.J., «La retención de datos de tráfico de las comunicaciones en la Unión Europea: una aproximación crítica», *Diario La Ley*, 6456, 2006, pág. 2.

⁶ Cfr. GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, pág. 74 y FERNÁNDEZ RODRÍGUEZ, J.J., «Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente», *Revista Española de Derecho Constitucional*, 108, 2016, pág. 97. Esta distinción entre datos de tráfico (dependientes funcionalmente de una concreta comunicación) y datos de abonado (entre los que se encuentran los datos de identificación) se ha puesto de manifiesto por la jurisprudencia —por todas, STS, Sala de lo Penal, de 18 de marzo de 2010— y se encuentra hoy normativamente recogida (arts. 588 ter.j a 588 ter.m LECrim).

II.2. El uso de datos de tráfico en la investigación penal

El tráfico comunicativo genera, en la actual sociedad hiperconectada, un volumen de datos exorbitante y en igual medida pingüe, constituyendo una fuente de información muy valiosa; incluso para las autoridades encargadas de la investigación y persecución de delitos⁷.

Sin embargo, las posibilidades de recopilarlos están condicionadas por su volatilidad. Los Estados comenzaron muy pronto a buscar soluciones que permitiesen, además de su interceptación en tiempo real, la conservación de esos datos asociados de modo que permanecieran disponibles más allá del momento en que se generaran⁸.

Ha surgido así la conservación y preservación de datos como obligación de los operadores de comunicaciones. El diverso alcance con que se usan requiere ciertas apreciaciones.

A. La conservación generalizada de datos

La «conservación de datos» es la obligación generalizada de los operadores de almacenar determinadas categorías de datos vinculados a las comunicaciones que gestionan, con la finalidad de mantenerlos disponibles para su eventual utilización posterior. Se trata de una obligación *ope legis* que se limita a los datos tratados por los operadores que, de otro modo, serían eliminados o anonimizados una vez cumplida su función de intermediación de la comunicación o los usos propios de la relación contractual de la prestación del servicio (facturación, posibles reclamaciones, ...) ⁹.

⁷ Vid. MURRAY, D. y FUSSEY, P., «Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data», *Israel Law Review*, Vol. 52, 1, 2019, págs. 31–60.

⁸ RODRÍGUEZ LAINZ, J.L., «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», *Diario La Ley*, 6859 y 6860, 2008, pág. 1.

⁹ RODRÍGUEZ LAINZ, J.L., «La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones», *Diario La Ley*, 8901, 2017, pág. 2 y GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, págs. 387-388.

Este deber de conservación se encuentra regulado en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCD).

No obstante, y más allá de los problemas de rango puestos de manifiesto por la doctrina y la jurisprudencia¹⁰, la LCD se encuentra actualmente en una especie de limbo jurídico al haber sido anulada la normativa comunitaria que transponía.

La exigencia de conservación de los datos asociados a comunicaciones ha partido siempre de la iniciativa europea en forma de normas especiales de protección de datos, y como efecto o impacto de determinados actos terroristas especialmente cruentos¹¹.

Tras los atentados del 11 de septiembre se planteó desde la Unión Europea y otros Estados la necesidad de poner a disposición de las autoridades herramientas que permitieran investigar delitos cuya comisión requería el recurso a sistemas electrónicos de comunicación¹². Unos meses después se aprobará la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

¹⁰ Se ha considerado que, tratándose de una norma que establece limitaciones a derechos fundamentales —sea al derecho a la protección de datos, como defendemos, o al secreto de las comunicaciones—, debiera haberse aprobado con el rango de Ley Orgánica. *Vid.* GONZÁLEZ LÓPEZ, J.J., «Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones», *Revista General de Derecho Procesal*, 16, 2008, pág. 10 y ORTIZ PRADILLO, J.C., «Tecnología versus proporcionalidad en la investigación penal: la nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas», *La Ley Penal*, 75, 2010, pág. 5. También la jurisprudencia se ha pronunciado en ocasiones en estos términos: «[...] no deja de llamar la atención la clamorosa insuficiencia, desde el punto de vista de su jerarquía normativa, de una ley que, regulando aspectos intrínsecamente ligados al derecho al secreto de las comunicaciones, y a la protección de datos personales, no acata lo previsto en el art. 81.1 de la CE». Cfr. STS, Sala de lo Penal, de 20 de mayo de 2008 (FJ. 4.e).

¹¹ Llegándose a afirmar que «en cada momento se ha pretendido aprovechar la predisposición psicológica de la población a un aumento de las medidas de seguridad en detrimento de las garantías de libertad, para incorporar la conservación generalizada». GONZÁLEZ LÓPEZ, J.J., «La retención de datos de tráfico...», *op.cit.*, pág. 4.

¹² GUERRERO PICÓ, M.C., «Protección de datos personales e Internet: la conservación indiscriminada de los datos de tráfico», *Revista de la Facultad de Derecho de la Universidad de Granada*, 8, 2005, pág. 117.

Su art. 6.1 dispone, como regla general, la obligatoriedad de eliminar o hacer anónimos los datos tratados «cuando ya no sea necesario a los efectos de la transmisión de una comunicación», si bien permitiendo su tratamiento a efectos de facturación hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago (art. 6.2).

No obstante, el art. 15 permite excepcionar esa obligación de eliminar los datos cuando ello sea necesario, entre otras finalidades, para la prevención, investigación, descubrimiento y persecución de delitos. Y, para llevarlo a efecto, autoriza a los Estados a adoptar «medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado».

A partir de esta previsión, los Estados comienzan a aprobar normas dirigidas a imponer la conservación generalizada de datos. En el caso de España esta previsión se incorpora a nuestro ordenamiento mediante la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, tramitada simultáneamente a la citada Directiva y aprobada un día antes¹³.

El art. 12 imponía un deber de retención de los datos de conexión y tráfico por un período máximo de doce meses que no se llegó a aplicar, pues el desarrollo reglamentario previsto en su apartado 4 para determinar las categorías de datos a retener, plazos y condiciones nunca fue aprobado.

La comisión de nuevos actos terroristas reactivó el debate sobre la conservación de datos. Como reacción a los atentados del 11M, el Consejo Europeo emitió, el 25 de marzo de 2004, la *Declaración sobre la lucha contra el terrorismo* en la que afirma la necesidad de «darse prioridad a las propuestas relativas a la conservación de datos de tráfico de comunicaciones». Del mismo modo, la *Declaración del Consejo sobre la respuesta de la UE a los atentados de Londres*, de 13 de julio de 2005, acuerda dar «prioridad inmediata» a la aprobación de la normativa sobre «retención de datos de telecomunicaciones».

¹³ La introducción del «deber de retención» en la Ley se produce a partir de la Enmienda núm. 172 del Grupo Parlamentario Popular en el Senado, que se justifica precisamente en la próxima aprobación de la Directiva, «en la última fase de su tramitación, contando su contenido con el consenso del Consejo y el Parlamento Europeo». BOCG, Senado, núm. 66, de 6 de junio de 2002.

El resultado será la aprobación de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

Esta nueva norma cambia la perspectiva sobre la conservación de los datos de tráfico que deja de ser, como en su antecesora, una excepción, para convertirse en la regla general, lo que ha sido objeto de numerosas críticas¹⁴.

Así, impone a los Estados Miembros la obligación de conservar una serie de datos de tráfico de diversas categorías —enumerados en su art. 5— durante un período de tiempo no inferior a seis meses ni superior a dos años.

Esta Directiva se traspone por la citada Ley 25/2007, de 18 de octubre, de conservación de datos. Ley que sigue el criterio de la Directiva, estableciendo la obligatoriedad de conservar, durante un plazo de 12 meses (art. 5), determinados datos asociados a comunicaciones electrónicas con el objetivo de que estén disponibles para su cesión, mediante autorización judicial, a fin de la «detección, investigación y enjuiciamiento de delitos graves» (art. 1.1).

No obstante, el deber de conservación no se circunscribe exclusivamente a los datos de tráfico en el sentido definido *supra*, sino que también resulta de aplicación a los datos «de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado» (art. 1.2), quedando así sometidos todos ellos a un mismo régimen jurídico¹⁵.

Tras unos años de cierta estabilidad, aunque no carente de críticas, el sistema de conservación generalizada de datos asociados a las comunicaciones comenzó a tambalearse¹⁶. Así, el TJUE tuvo que enjuiciar la validez de la Directiva de 2006

¹⁴ Vid. VILASAU SOLANA, M., «La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad», *IDP. Revista de Internet, Derecho y Política*, 3, 2006, págs. 1-15 y RODOTÁ, S., «La conservación de los datos de tráfico en las comunicaciones electrónicas», *IDP. Revista de Internet, Derecho y Política*, 3, 2006, págs. 53-60.

¹⁵ RODRÍGUEZ LAINZ, J.L., «El principio de proporcionalidad...», *op.cit.*, págs. 6-7.

¹⁶ Vid. POLLICINO, O., «La tutela de la *privacy* digital: el diálogo entre el Tribunal de Justicia de la Unión Europea y las jurisdicciones nacionales», *Revista de Estudios Políticos*, 173, 2016, págs. 195-244.

desde la perspectiva de los derechos a la vida privada y a la protección de datos reconocidos en la CDFUE como respuesta a las cuestiones prejudiciales acumuladas en los asuntos C-293/12 y C-594/12.

El resultado fue la STJUE, Gran Sala, de 8 de abril de 2014, en el asunto conocido como *Digital Rights Ireland*, en la que el tribunal declaró la invalidez de la citada Directiva por no respetar el principio de proporcionalidad, al imponer el deber de conservación «de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin [establecer] ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves» (§57).

Pese a que la Ley de Conservación de Datos española reconocía en su Preámbulo que su objetivo principal era la transposición de la Directiva anulada, una parte de la doctrina, avalada posteriormente por la jurisprudencia, consideró que tal anulación no se extendía automáticamente a nuestra norma interna.

En primer lugar, porque entre Directiva y norma de transposición no existe una relación de validez y, una vez aprobada la norma interna, esta adquiere vigencia de acuerdo al sistema de fuentes interno. Pero, además, porque, pese a la declaración de invalidez de la Directiva 2006/24/CE, el art. 15 de la Directiva 2002/58/CE permaneció en vigor, permitiendo a los Estados, como dijimos, adoptar medidas legislativas de conservación de datos. Ello, en principio, constituía un asidero jurídico válido para la Ley 25/2007¹⁷.

¹⁷ RODRÍGUEZ LAINZ, J.L., «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones», *Diario La Ley*, 8308, 2014, págs. 3-5. Del mismo modo, el Tribunal Supremo no dudó en considerar que la declaración de invalidez de la Directiva 2006/24/CE no afectaba a la vigencia de la ley española de conservación de datos, por cuanto que los reproches que el TJUE realiza sobre aquella no era aplicables a la norma interna. Así, en las SSTS, Sala de lo penal, de 7 de julio de 2015, y de 23 de noviembre de 2015, dirá: «La STJUE Gran Sala de 8 de abril de 2014 la desautorizó [a la Directiva de 2006] porque: a) no establecía límites temporales; b) ni concretaba el concepto delito grave; c) inconcreción regulación autoridades con facultades; d) laxitud plazos; y e) medidas sobre aseguramiento integridad y confidencialidad. [...]. La doctrina ha estimado que en España, por el contrario, una adecuada interpretación de la Ley 25/2007 superaba esas objeciones. Ni puede considerarse que la transposición está subordinada como reglamento a la ley. Esa interpretación, tal como ha venido siendo impuesta por una restrictiva jurisprudencia de este Tribunal Supremo aleja la citada ley y la práctica de los Tribunales de los reproches del Tribunal de Justicia Europeo» (FJ.1.3 y FJ. 7, respectivamente). Sobre la incidencia que la STJUE ha tenido en otros Estados Miembros, vid. VAINIO, N. y MIETTINEN, S., «Telecommunications data retention after *Digital Rights Ireland*:

No obstante, las dificultades de este *statu quo* no tardaron en manifestarse. En abril de 2015, un Tribunal sueco elevó al TJUE una cuestión prejudicial para que valorase si la legislación sueca sobre conservación de datos era conforme al art. 15 de la Directiva de 2002 a la luz de los derechos fundamentales de la CDFUE.

La normativa sueca disponía, de forma similar a la Directiva de 2006 y a la Ley española, el deber de conservar indiscriminadamente todos los datos relativos a comunicaciones electrónicas por un periodo de 6 meses.

La respuesta a esta cuestión prejudicial, acumulada a otra elevada por Reino Unido sobre el acceso a los datos conservados, se contiene en la STJUE, Gran Sala, de 21 de diciembre de 2016 (asunto *Tele2 Sverige AB*)¹⁸.

El Tribunal considera que una norma que imponga un deber de conservación generalizado —como el de la ley sueca y, por tanto, como el de la española— convierte en regla lo que la Directiva 2002/58 permite con carácter excepcional (§89 y 104). Además, al no superar el test de proporcionalidad, no puede considerarse justificada en una sociedad democrática, como exige su artículo 15.1 (§107). Por ello, para el tribunal:

«[...] el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los

legislative and judicial reactions in the Member States», *International Journal of Law and Information Technology*, 23, 2015, págs. 290-309.

¹⁸ La conflictividad en esta materia no termina con la STJUE en el asunto *Tele2*. Con fecha de 15 de enero de 2020 se publicaron las Conclusiones del Abogado General Campos Sánchez-Bordona a los asuntos C-623/17, C-511/18 y C-512/18, y C-520/18. En todos ellos se plantean cuestiones prejudiciales sobre la conformidad con el derecho de la Unión de normativas nacionales —de Reino Unido, Francia y Bélgica, respectivamente— que prevén la conservación generalizada de datos de tráfico para la lucha contra amenazas graves a la seguridad nacional, especialmente por el riesgo terrorista. El Abogado General considera aplicable la jurisprudencia del TJUE en los asuntos *Digital Rights Ireland* y *Tele2* y, por tanto, contrarias a la Directiva las normas nacionales que permiten conservar, general e indiferenciadamente, todos los datos asociados a todas las comunicaciones de todos los usuarios, animando a los Estados a hallar fórmulas que permitan una *conservación selectiva de datos* respetuosa con los derechos fundamentales. Por su parte, las Conclusiones del Abogado General Giovanni Pitruzzella en el asunto C-746/18, presentadas en fecha 21 de enero de 2020, abordan, para el caso de Estonia, la relación de proporcionalidad entre la gravedad del delito investigado y las categorías de datos y el periodo a los que se accede para su incorporación al proceso penal —como ya hiciera el TJUE en su Sentencia de 2 de octubre de 2018—, así como la calificación de la posición del Ministerio Fiscal en el proceso como «autoridad independiente».

datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica» (§112).

Los efectos de esta sentencia en la Ley de Conservación de Datos española han sido puestos de manifiesto por la doctrina, señalando que, si bien se mantiene formalmente vigente, debe considerarse contraria al derecho de la Unión Europea en el sentido manifestado por el TJUE y, en consecuencia, materialmente inaplicable tal y como determina el art. 4 bis.1 LOPJ¹⁹.

No obstante, el Tribunal Supremo ha tratado de salvar la validez de esta norma con base en una interpretación que no resulta, a nuestro juicio, satisfactoria. Por un lado, la STS, Sala de lo Penal, de 18 de abril de 2017, pese a haber sido dictada con posterioridad a la STJUE en el asunto *Tele2*, ni siquiera la menciona. Por otro, la STS, Sala de lo Penal, de 1 de junio de 2017, considera, en sintonía con sus precedentes de 7 de julio y de 23 de noviembre de 2015, que las deficiencias puestas de manifiesto por el TJUE en la normativa sueca se salvan en nuestro ordenamiento por la exigencia de autorización judicial para la cesión de tales datos:

«[...] las exigencias señaladas por el TJUE en nuestra normativa interna, tanto la protección del derecho a la intimidad como el principio de proporcionalidad, están sujetas a la autorización de una autoridad independiente de la administrativa cual es la judicial, y se contraen a la investigación y enjuiciamiento de delitos graves contemplados en el Código Penal y en las leyes penales especiales, de forma que en cada caso será el Juez de Instrucción correspondiente el que decida la cesión de los datos de tráfico en las comunicaciones electrónicas, lo que desde luego implica que la decisión debe ser ajustada al principio de proporcionalidad establecido expresamente en nuestra ley procesal (artículo 588 bis a).5 LECrim)» (FJ. 2.5).

¹⁹ «Los Jueces y Tribunales aplicarán el Derecho de la Unión Europea de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea». Sobre esta cuestión, *vid.* COLOMER HERNÁNDEZ, I., «Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016», RUDA GONZÁLEZ, A. y JEREZ DELGADO, C. (Dir.), *Estudios sobre Jurisprudencia Europea. Materiales del I y II Encuentro anual del Centro español del European Law Institute*, Sepin, Madrid, 2018, págs. 767-781; RODRÍGUEZ LAINZ, J.L., «La definitiva defenestración...», *op.cit.*, págs. 1-24 y BALLESTEROS MOFFA, L.A., «La difícil situación de la Ley 25/2007 de conservación y cesión de datos de tráfico y localización en las comunicaciones electrónicas: la “tala” de su base comunitaria y los desfavorables vientos desde sus homólogos europeas», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 44, 2017, págs. 1-26.

Sin embargo, las SSTJUE en *Digital Rights Ireland* y en *Tele2* declaran la invalidez de la Directiva y de otras normativas nacionales por la desproporcionalidad en la norma interna sobre la conservación incondicionada de los datos independientemente del modo de aplicación. Consideramos por ello que la posición de nuestro Tribunal Supremo dirigida a salvar la validez de ley española con base en las garantías previstas para la cesión de esos datos a las autoridades no resulta convincente.²⁰.

En la actualidad se encuentra en fase de elaboración el Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se derogará, de aprobarse, la Directiva 2002/58/CE.

La propuesta mantiene el criterio de la Directiva de 2002. Esto es, impone como norma general la supresión o anonimización de datos cuando ya no sean necesarios para transmitir una comunicación (art. 7.2), permitiendo su conservación hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse su pago con arreglo a la legislación nacional (art. 7.3). Respecto a su conservación más allá de este plazo, el art. 11 permite a los Estados miembros desarrollar medidas de conservación específicas, pero con la advertencia explícita de que «sean conformes al Derecho de la Unión, habida cuenta de la jurisprudencia del Tribunal de Justicia sobre la interpretación de la Directiva sobre privacidad y comunicaciones electrónicas y de la Carta de los Derechos Fundamentales» (apdo. 1.3 de la Exposición de Motivos).

Por su parte, el acceso a los datos conservados para su incorporación al proceso penal se encuentra regulado en los arts. 588 ter.j y siguientes de la Ley de Enjuiciamiento Criminal. Una regulación que reclama dos observaciones.

²⁰ Sobre la posición del Tribunal Supremo respecto de la aplicabilidad de la LCD puede verse: RODRÍGUEZ LAINZ, J.L., «La jurisprudencia del tribunal de Luxemburgo sobre regímenes de conservación preventiva de datos en la Doctrina del Tribunal Supremo», *Diario La Ley*, 9087, 2017, págs. 1-9.

Por un lado, pese a que, como dijimos, la LCD prevé un mismo régimen jurídico para la conservación de datos de tráfico y de abonado, la LECrim diferencia las modalidades de acceso a unos u otros.

Así, mientras que el art. 588 ter.j exige autorización judicial para la cesión de datos conservados que «se encuentren vinculados a procesos de comunicación» —datos de tráfico en sentido estricto—, el art. 588 ter.m permite al Ministerio Fiscal o la Policía Judicial recabar directamente de los prestadores datos de identificación²¹.

Por otro lado, el art. 588 ter.j permite la cesión de datos de tráfico que hayan sido conservados por una doble vía: datos conservados en cumplimiento de un deber legalmente impuesto —LCD— o datos conservados «por propia iniciativa, por motivos comerciales o de otra índole», posibilidad de conservación permitida por el art. 6.2 de la Directiva 2002/58/CE, si bien solamente durante el plazo de impugnación de la factura o de exigencia del pago.

No obstante, si el deber de conservación previsto en la LCD no puede ser aplicado al ser contrario al Derecho de la Unión, esta medida debe circunscribirse únicamente a aquellos conservados por iniciativa de los prestadores de servicios, lo que limita temporalmente la posibilidad de acceder a datos de tráfico en el proceso penal²².

A estos efectos, por tanto, puede resultar de gran utilidad la medida de preservación de datos.

B. La preservación de datos almacenados

La «preservación de datos de tráfico» es la medida de aseguramiento dirigida a perpetuar el almacenamiento de determinados datos correspondientes a

²¹ Algunos autores han considerado que el acceso a datos de identificación sin necesidad de autorización judicial resulta contrario al Derecho de la Unión Europea. Cfr. PERALTA GUTIÉRREZ, A. y AGUIRRE ALLENDE, P., «El TJUE y el acceso a los datos de abonado en el seno de la instrucción penal», *Diario La Ley*, 9420, 2019, págs. 1-11.

²² COLOMER HERNÁNDEZ, I., «Uso y cesión de datos...», *op.cit.*, pág. 779 y RODRÍGUEZ LAINZ, J.L., «La definitiva defenestración...», *op.cit.*, pág. 17.

personas singularizadas y comunicaciones concretas, y cuya obligatoriedad viene impuesta por la autoridad habilitada legalmente para ello en el contexto de una investigación delictiva en marcha. Al igual que la conservación, opera también sobre datos ya almacenados y pretende su depósito más allá de los plazos habituales, evitando así que se pierdan y asegurando su disponibilidad cuando el acceso a los mismos sea autorizado. Pero, a diferencia de aquella, la preservación tiene como objeto datos individualizados y puede imponerse, no solo a los prestadores de servicios de comunicaciones, sino también a otros sujetos poseedores de los datos sobre los que se dirige²³.

Esta medida, también denominada *quick freeze* y defendida por algunos autores por ser menos invasiva que la conservación generalizada²⁴, se contempla en el art. 588 *octies* LECrim, bajo la rúbrica de *orden de conservación de datos*:

«El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes».

C. La interceptación de datos en tiempo real

Además de la conservación y preservación de datos de comunicaciones finalizadas, los órganos de persecución penal pueden tomar conocimiento de los datos de tráfico mediante la interceptación de comunicaciones en curso.

Debe entenderse por «interceptación de datos» la aprehensión, en tiempo real y con alcance individualizado, de datos correspondientes a comunicaciones en tránsito. La interceptación se produce previa incoación de un proceso penal concreto y tras la autorización de la toma de conocimiento de dichos datos en

²³ GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, págs. 451-453.

²⁴ VILASAU SOLANA, M., «La Directiva 2006/24/CE sobre conservación de datos...», *op.cit.*, pág. 6.

tiempo real, ya sean éstos el único objeto de interceptación o junto al contenido de la comunicación²⁵.

Esta posibilidad de acopio dinámico de datos de tráfico forma parte, por tanto, de la regulación de la medida de interceptación de comunicaciones telefónicas y telemáticas, prevista en los arts. 588 *ter* a y siguientes LECrim.

En este sentido, el art. 588 *ter* b.2 LECrim, al delimitar el ámbito de la diligencia, dispone:

«La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario».

La forma de practicar la interceptación de los datos asociados por parte de los operadores se regula en el art. 39 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. A estos efectos, los apartados 5 a 7 contienen un listado de datos a interceptar, si bien el apartado 8 dispone, de conformidad con el principio de necesidad que debe presidir cualquier medida que afecte a derechos fundamentales, que solo serán interceptados «aquéllos que estén incluidos en la orden de interceptación legal»²⁶.

La *conservación y preservación* de datos son acciones que se llevan a cabo por los prestadores de servicios de comunicaciones, postergándose su toma de conocimiento por otros sujetos, en caso de que se produzca, a un momento posterior. Por ello, desde el punto de vista de los órganos encargados de la

²⁵ RODRÍGUEZ RUBIO, C., «La injerencia en el derecho al secreto de las comunicaciones a través de la regulación de las medidas de investigación tecnológica», *Revista Europea de Derechos Fundamentales*, 28, 2016, pág. 276. Asimismo, GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, pág. 388.

²⁶ Las condiciones y el procedimiento técnico de interceptación se regulan en los arts. 83 y siguientes del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

persecución penal, hablaremos de *acceso* a datos de tráfico, cuando se trate de recabar datos relativos a comunicaciones ya consumadas.

La *interceptación*, por su parte, si bien puede ser realizada —y generalmente lo será— por el prestador del servicio, su participación es instrumental respecto de los agentes facultados, a quienes se les facilitarán los datos interceptados en tiempo real²⁷.

En ambos casos nos hallamos ante datos que pueden aportar mucha información sobre los hábitos de vida y las relaciones sociales de las personas, lo que exige, para su mejor garantía, la precisa delimitación de los derechos fundamentales afectados en cada caso²⁸.

²⁷ El art. 94 del Real Decreto 424/2005 dispone: «La interceptación se realizará en tiempo real, sin más retardo que el mínimo imprescindible para realizar el encaminamiento y transmisión, e ininterrumpidamente durante el plazo establecido en la orden de interceptación legal. Si no se pudiera facilitar la información relativa a la interceptación a la que se refiere el artículo 88 en tiempo real por causa de fuerza mayor, se efectuará al finalizar la conexión y, en todo caso, lo antes posible».

²⁸ FERNÁNDEZ RODRÍGUEZ, J.J., «Los datos de tráfico de comunicaciones...», *op.cit.*, pág. 99. Como gráficamente ejemplifica RODOTÁ, «[i]ncluso sólo la conservación de las direcciones del remitente y del destinatario permite reconstruir la trama de las relaciones personales y sociales (¿cuántas veces he llamado a una determinada persona?), políticas y sindicales (¿con qué organizaciones estoy en contacto?), económicas (¿cuáles son las empresas, los agentes de bolsa con los que mantengo relaciones?), concernientes a la fe religiosa (¿mi interlocutor es la parroquia, la sinagoga, la mezquita?)»; cfr. RODOTÁ, S., «La conservación de los datos de tráfico...», *op.cit.*, págs. 57-58.

III. DATOS DE TRÁFICO Y DERECHOS FUNDAMENTALES AFECTADOS

Los datos externos de comunicaciones integran el ámbito objetivo del secreto protegido por el artículo 18.3 CE, en la medida en que éste se proyecta sobre el proceso de comunicación y posee carácter formal.

Esta consideración, aceptada desde la doctrina *Malone* del TEDH y acogida en nuestro ordenamiento por la STC 114/1984, suscita algunas observaciones.

En primer lugar, no es trasladable sin más a las posibilidades técnicas de las actuales comunicaciones electrónicas, pues hoy es posible recabar muchos más datos que los descritos en las resoluciones aludidas²⁹.

Por ello, su aplicación debe venir hoy exclusivamente referida a los datos de tráfico en sentido estricto, es decir, aquellos vinculados a un concreto proceso comunicativo. No forman parte del objeto del 18.3 CE, sin embargo, los datos de suscripción que, en su caso, y en cuanto que tratados por los operadores y almacenados en ficheros automatizados, quedarán al amparo del derecho fundamental a la protección de datos.

Desde el punto de vista del objeto del derecho, por tanto, no cabría duda de que cualquier descubrimiento no consentido de los datos de tráfico constituiría una injerencia en el derecho fundamental al secreto de las comunicaciones.

No obstante, para deslindar los derechos fundamentales afectados por inmisiones en los datos de tráfico, resulta de gran importancia la delimitación del derecho al secreto de las comunicaciones desde el punto de vista de su eficacia temporal. Criterio que exigirá dejar fuera del objeto de este derecho los actos que operen sobre estos datos en momentos distintos a la secuencia temporal en que la comunicación se produce.

Como venimos manteniendo a lo largo del presente trabajo, la protección del 18.3 CE se proyecta sobre el proceso comunicativo, pero, una vez recibida la comunicación, su resultado —que deja de ser comunicación en sentido dinámico

²⁹ MARCHENA GÓMEZ, M., «La vulneración de derechos fundamentales por ministerio de la Ley (a propósito del art. 33 de la Ley General de Telecomunicaciones)», *Diario La Ley*, 7572, 2011, págs. 1-2.

para convertirse en archivo o dato estático— pasa a incluirse en objeto, en su caso, de otros derechos.

Por tanto, serán la pertenencia funcional a una concreta comunicación (ámbito objetivo) y la inmisión durante el tránsito comunicativo (ámbito temporal) los elementos que determinen que un dato vinculado a las comunicaciones se incluye en el objeto del derecho protegido por el art. 18.3 CE³⁰.

No obstante, parte de la doctrina y algunas resoluciones jurisprudenciales han considerado oportuno extender el ámbito temporal del objeto del derecho al secreto de las comunicaciones a momentos posteriores a su finalización. Ello habilitaría la protección de este derecho, no solo frente a la interceptación de datos de comunicaciones en curso, sino también frente al acceso a datos de tráfico de comunicaciones finalizadas.

En este sentido, es necesario destacar la importancia que han tenido ciertas resoluciones jurisprudenciales del TEDH, que han considerado vulnerado el art. 8 del Convenio por el acceso a datos en su dimensión estática.

Ahora bien, el amplio objeto del artículo 8 CEDH está dotado de una mayor elasticidad que los diversos derechos autónomos recogidos en el art. 18 CE en los que, cada uno separadamente, poseen objetos con contornos estrictamente delimitados. Precisamente por ello el tribunal de Estrasburgo resuelve con arreglo a unos criterios más flexibles que aquellos en los que se desempeña el Tribunal Constitucional español. Pese a ello, los pronunciamientos de la Corte europea parecen haber propiciado algunas imprecisiones al interpretar nuestra corte nacional, *vía* 10.2, los derechos fundamentales internos.

³⁰ En similar sentido, GONZÁLEZ LÓPEZ, J.J., «Consideraciones acerca de las dificultades conceptual e iusfundamental planteadas por los datos de las comunicaciones electrónicas en la investigación penal», CABEZUDO RODRÍGUEZ, N. (Coord.), *Inclusión digital: perspectivas y experiencias*, Universidad de Zaragoza, Zaragoza, 2011, págs. 163-164. Este doble parámetro de la protección dispensada por el art. 18.3 CE se resume con total claridad en el Fundamento Jurídico 4 de la STC 241/2012, de 17 de diciembre, cuando afirma: «[...] el concepto de secreto de la comunicación, cuando opera, cubre no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores [...]. A lo que debe añadirse que la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan otros derechos».

III.1. Interceptación de datos de tráfico asociados a comunicaciones en curso

La interceptación de datos de tráfico asociados a procesos comunicativos en curso constituye injerencia en el derecho fundamental al secreto de las comunicaciones. Tal y como resulta de la proyección sobre determinados datos asociados a las comunicaciones de los ámbitos objetivo, subjetivo y temporal del derecho garantizado en el art. 18.3 CE³¹.

Desde el punto de vista de su delimitación objetiva, el secreto posee carácter formal e impregna el proceso de comunicación en su totalidad. Por ello, cualquier inmisión en el proceso comunicativo constituirá ruptura del secreto, se pretenda con ello desvelar el contenido transmitido o conocer otras características de la comunicación.

En atención a ello, los datos cuyo secreto garantiza el derecho fundamental serán solamente los vinculados al proceso concreto (datos de tráfico *stricto sensu*) y que se refieran a comunicaciones protegidas por el 18.3; a saber, transmisión técnicamente mediada a través de canal cerrado de expresiones de sentido entre personas determinadas.

Respecto a la delimitación subjetiva del derecho garantizado en el art. 18.3 CE, el concepto de secreto se compromete cuando las inmisiones en su objeto pretenden obtener un conocimiento que se mantiene oculto.

Por ello, el secreto sobre los datos de tráfico no rige para los comunicantes. Tampoco es oponible a los prestadores del servicio de comunicación, puesto que su conocimiento de los datos de tráfico es técnicamente imprescindible para que el proceso comunicativo sea posible. El tratamiento por los operadores de datos de tráfico de comunicaciones en curso, en el modo de condición inherente para el ejercicio del derecho, no constituirá injerencia alguna en el art. 18.3 CE³².

Otra cosa cabe decir para el caso en que la interceptación se ejecute materialmente por los prestadores de servicio, pero actuando instrumentalmente para desvelar los datos de tráfico en provecho de terceros ajenos, como serían los

³¹ GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, pág. 136.

³² *Ibid.*, págs. 151-154.

órganos encargados de la persecución penal. En este caso resultará afectado el derecho fundamental al secreto de las comunicaciones, en la medida en que la actuación del prestador del servicio excede del tratamiento necesario para llevar a cabo la comunicación, única causa habilitante para adquirir conocimiento de tales datos. Su actuación instrumental respecto de terceros supone levantar el secreto y permitirles acceder a un conocimiento que hasta el momento permanecía oculto y, por ello, incide en el objeto del 18.3 CE³³.

Por último, en atención a la delimitación temporal del derecho considerado, no cabe duda de que la interceptación de datos de tráfico en tiempo real está frontalmente impedida por el 18.3 CE. Si la garantía de secreto «alcanza al proceso de comunicación mismo» —STC 70/2002, de 3 de abril (FJ. 9)— su protección se dirige precisamente a evitar las inmisiones producidas durante el intervalo delimitado por su inicio y conclusión.

Lo determinante es la interceptación de los datos de tráfico durante la comunicación en curso por un sujeto no habilitado, lo que sucederá tanto si los datos se aprehenden por terceros ajenos al proceso como si se ejecuta por los prestadores del servicio actuando por orden de terceros; con independencia de que la toma de conocimiento por éstos se produzca posteriormente³⁴.

Por ello, la sujeción a las garantías del 18.3 CE —en especial, la necesidad de autorización judicial— se referirá a datos de tráfico de comunicaciones futuras, y ello tanto si el conocimiento de tales datos por los órganos encargados de la persecución penal se produce en tiempo real como si se ponen a su disposición una vez consumadas³⁵.

³³ GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, pág. 148.

³⁴ Así, respecto al acceso al listado de llamadas se ha dicho que «[...] lo relevante consiste en examinar si la pretensión se refiere a las comunicaciones futuras o a las llamadas ya realizadas. Sólo en el primer caso quedará afectado el art. 18.3 CE, ya que los listados telefónicos incorporan datos para cuyo conocimiento y registro resultaría necesario acceder de forma directa al proceso de comunicación mientras éste está teniendo lugar»; LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, *op.cit.*, págs. 64-65.

³⁵ En similar sentido, MARCHENA GÓMEZ afirma que «[...] se trata de datos electrónicos contemplados desde una perspectiva dinámica, o lo que es lo mismo, datos que afloran y se registran como consecuencia de una comunicación bidireccional que está siendo objeto de interferencia, en virtud de una decisión judicial adoptada en el marco de un proceso penal», cfr. MARCHENA GÓMEZ,

Este es el sentido de la STC 123/2002, de 20 de mayo (FJ. 6), cuando afirma que «los listados telefónicos incorporan datos [...] para cuyo conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación mientras está teniendo lugar, con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso»³⁶.

La solicitud de interceptación de datos de tráfico de comunicaciones futuras es, además, el hecho que se somete a la conformidad con el art. 8 CEDH en *Malone*³⁷.

Esta situación es distinta a la que se produce cuando la solicitud se dirige al conocimiento de datos de tráfico relativos a comunicaciones pretéritas, que fueron legítimamente recopilados y que se encuentran registrados en determinados soportes. A ello dedicamos el siguiente apartado.

III.2. Acceso a datos de tráfico asociados a comunicaciones consumadas

A diferencia de la captación de datos de tráfico de comunicaciones activas, el acceso a datos de tráfico almacenados en un soporte físico, una vez finalizado el proceso comunicativo, no forma parte del objeto del derecho fundamental.

Una vez que la comunicación ha sido desactivada o el mensaje, en el caso de las comunicaciones alternativas, recibido por su destinatario los datos de tráfico

M., «La vulneración de derechos fundamentales...», *op.cit.*, págs. 11-12. Vid. también GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, pág. 157.

³⁶ No podemos, por ello, estar de acuerdo con algún autor que ha afirmado que esta sentencia «supone una marcha atrás en el planteamiento que se había llevado a cabo en la STC nº 70/2002», cfr. FRÍGOLS BRINES, E., «La protección constitucional de los datos de las comunicaciones...», *op.cit.*, pág. 75. Ambas sentencias (70 y 123/2002) son complementarias: la protección dispensada por el derecho fundamental al secreto de las comunicaciones solo alcanza a las intervenciones mientras la comunicación está en tránsito, pero, mientras que el tratamiento de los datos que realizan los operadores no constituye, en la medida en que es técnicamente necesario, una injerencia en el derecho, sí tiene tal consideración recabar esos mismos datos por mandato de la policía.

³⁷ «[...] su línea fue conectada, a petición de la Policía, a un aparato contador que registraba automáticamente todos los números marcados en el disco», STEDH de 2 de agosto de 1984 (asunto *Malone c. Reino Unido*; §17).

asociados se escinden del proceso comunicativo dinámico finalizado para quedar registrados como datos estáticos³⁸.

Por ello, si bien conservan una conexión de sentido con la concreta comunicación que los originó —y a la que identifican—, las acciones que frente a su resultado se produzcan no son subsumibles en el objeto del 18.3 CE y, por tanto, la tutela de los datos de tráfico almacenados en el modo que fuere se inscribe en el ámbito objetivo, en su caso, de otros derechos.

En la medida en que el fundamento constitucional del derecho reside, según dijimos, en la especial vulnerabilidad de las comunicaciones que requieren para su transmisión la intermediación de un tercero ajeno a los interlocutores —SSTC 123/2002, de 20 de mayo (FJ. 5), y 281/2006, de 9 de octubre (FJ. 3)—, y que el bien jurídico que el secreto tutela es la libertad de las comunicaciones, su vulneración «requiere la interferencia directa en el proceso de comunicación [...] mediante el empleo de cualquier artificio técnico de captación, sintonización o desvío y recepción de la señal telefónica como forma de acceso a los datos confidenciales de la comunicación, es decir, a su existencia, contenido y a las circunstancias externas del proceso de comunicación»³⁹.

No obstante, y pese a la condición dinámica que, según la jurisprudencia aludida, caracteriza al secreto, determinadas resoluciones jurisprudenciales han optado por extender la protección formal del 18.3 CE a datos de tráfico en sentido estático, recopilados con la comunicación concluida mediante el registro de dispositivos o archivos.

³⁸ «Las comunicaciones pretéritas almacenadas en el dominio virtual (ya datos), no son proceso comunicacional en el sentido del art. 18.3 CE, como tampoco lo son los datos personales, imágenes e informaciones que circulan por la red o se acumulan en el disco duro del dispositivo técnico». ZOCO ZABALA, C., «Secreto de las comunicaciones en la frontera...», *op.cit.*, págs. 323-324.

³⁹ STC 56/2003, de 24 de marzo (FJ. 3). En este sentido, LÓPEZ-BARAJAS PEREA señala: «Dado que el art. 18.3 CE lo que tutela es la libertad de las comunicaciones, no resulta justificado extender su ámbito cuando el secreto de la transmisión de la información en que la comunicación consiste ya ha sido salvaguardado», cfr. LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, *op.cit.*, pág. 66. También la normativa europea tiene en cuenta esta distinción. Así, la Directiva 2014/41/UE, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal deja fuera de la regulación específica de la intervención de telecomunicaciones (arts. 30 y 31) el acceso a «datos históricos de tráfico», que remite al régimen general (*vid.* Considerando núm. 30). También RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, pág. 35.

Consideramos, sin embargo, que esta dilatación de la eficacia temporal del derecho al secreto de las comunicaciones no se adecúa a su fundamento constitucional ni al bien jurídico que tutela. Puede además resultar, según veremos, problemática por la inexcusable exigencia de resolución judicial para su limitación, siendo superflua para asegurar un nivel óptimo de protección de los datos de tráfico archivados⁴⁰.

En suma, consumada la comunicación, tal y como reconoce el propio Tribunal Constitucional, «la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos» —STC 70/2002, de 3 de abril (FJ. 9)—.

Es más, el acceso a datos almacenados se caracteriza por la diversidad de agentes en cuya posesión pueden hallarse los datos, por lo que su régimen jurídico de acceso será también diverso⁴¹. Los datos de tráfico pueden así estar soportados en los archivos registrados por los proveedores de servicios de telecomunicaciones o en bases de datos privadas de los propios comunicantes (memoria de un teléfono móvil o de un ordenador).

A. Datos en poder del prestador del servicio

Los prestadores de servicios de telecomunicaciones pueden estar en posesión de datos de tráfico, relativos a las comunicaciones que gestionan, bien como cumplimiento de un deber legal de conservación —regulado en la LCD, con las salvaguardas referidas—, bien como consecuencia del propio tratamiento realizado para la intermediación técnica de la comunicación y su posterior archivo por motivos comerciales (facturación, reclamación, oferta de servicios, etc.).

En ambos casos, en cuanto su acceso se produce con la comunicación ya consumada, están tutelados por el derecho fundamental a la protección de datos y no por el secreto de las comunicaciones. Así ha sido puesto de manifiesto por la

⁴⁰ GONZÁLEZ LÓPEZ, J.J., «Consideraciones acerca de las dificultades conceptual e iusfundamental...», *op.cit.*, págs. 162-163.

⁴¹ GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico...*, *op.cit.*, pág. 293.

doctrina al considerar que «el tratamiento de los datos vinculados a las comunicaciones electrónicas que efectúan los operadores conlleva necesariamente la organización o estructura de los datos recabados» y, por tanto, «las operaciones de obtención de tales datos con fines de investigación penal se enmarcarán en el ámbito de cobertura del derecho a la protección de los datos de carácter personal»⁴².

También el Tribunal Supremo ha situado la remisión de datos de tráfico por los operadores en el seno del derecho a la protección de datos, advirtiendo que la correcta interpretación de la doctrina *Malone* exige diferenciar «cuándo unos datos personales pueden afectar al secreto a las comunicaciones y cuándo conservados y tratados por las operadoras, no se están refiriendo a comunicación alguna, es decir, datos estáticamente almacenados, conservados y tratados por operadores que se hallan obligados a la reserva frente a terceros»⁴³.

No cabe pues el recurso al derecho fundamental al secreto de las comunicaciones cuando se trata de recabar datos pertenecientes a comunicaciones finalizadas. Como dijimos, la vulneración de este derecho requiere la interferencia directa en el proceso de comunicación (STC 56/2003, de 24 de

⁴² GONZÁLEZ LÓPEZ, J.J., «Consideraciones acerca de las dificultades conceptual e iusfundamental...», *op.cit.*, pág. 175. Del mismo modo, se ha señalado que «[...] la entrega por la operadora del listado de las llamadas ya ejecutadas con anterioridad desde un determinado número de teléfono no afecta al contenido propio del derecho al secreto de las comunicaciones, toda vez que se trata, en definitiva, de datos de carácter personal, custodiados en ficheros automatizados»; *vid.* LÓPEZ-BARAJAS PEREA, I., «El deber de conservación de datos en la Unión Europea y sus límites», *Revista de Derecho de la Unión Europea*, 16, 2009, pág. 210. En el mismo sentido, cfr. RODRÍGUEZ LAINZ, J.L., «El principio de proporcionalidad...», *op.cit.*, pág. 24; MARCHENA GÓMEZ, M., «La vulneración de derechos fundamentales...», *op.cit.*, págs. 11-12; ORTIZ PRADILLO, J.C., «Tecnología versus proporcionalidad en la investigación penal...», *op.cit.*, págs. 5-6; y ANCOS FRANCO, H., «El tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones. Comentario a la Consulta 1/1999 de la Fiscalía General del Estado», *Diario La Ley*, 4812, 1999, pág. 9.

⁴³ STS, Sala de lo Penal, de 18 de marzo de 2010 (FJ. 3). «El registro de las llamadas efectuadas desde un determinado número de teléfono forma parte del conjunto de datos que las correspondientes compañías telefónicas obtienen y conservan para poder determinar el precio que periódicamente debe abonarles el titular de aquél [...]; en forma semejante a como hacen las entidades bancarias con los titulares de las cuentas corrientes [...]. Se trata, en definitiva, de datos de carácter personal, custodiados en ficheros automatizados»; STS, Sala de lo Penal, de 22 de marzo de 1999 (FJ. 2). También consideran afectado en este caso el derecho fundamental a la protección de datos, entre otras, las SSTS, Sala de lo Penal de 7 de diciembre de 2001 (FJ. 2); 6 de marzo de 2006 (FJ. 2); 3 de octubre de 2007 (FJ. 3); 14 de abril de 2015 (FJ. 5); 7 de julio de 2015 (FJ. 1.3) y 23 de noviembre de 2015 (FJ. 7).

marzo [FJ. 3]), siendo así reconocido también por aquellas resoluciones que han considerado afectado el art. 18.3 CE cuando la obtención de los datos se produce con la comunicación consumada⁴⁴.

La inclusión en el objeto del derecho al secreto de las comunicaciones de los datos de tráfico conservados exigiría, por tanto, entender como «interferencia directa en el proceso de comunicación» el tratamiento efectuado por los operadores sobre ellos y su posterior conservación, actuaciones ambas que debieran precisar, en consecuencia, autorización judicial como requisito indispensable establecido en el art. 18.3 para legitimar tales interferencias.

Sin embargo, la legislación —de rango ordinario— permite el tratamiento de esos datos e impone su conservación sin necesidad de que dichas actividades estén judicialmente autorizadas. Ello es así, precisamente, porque la actuación de los prestadores de servicio no puede tener consideración de interferencia en el proceso comunicativo sino que, muy al contrario y según advertimos, es condición inherente de su efectividad. Del mismo modo, el TEDH ha reconocido que estos datos pueden ser obtenidos legítimamente por la operadora «para asegurar la exactitud de los cargos que se exigen al abonado, examinar sus reclamaciones o descubrir posibles abusos»⁴⁵.

Por ello, la adquisición y conservación de datos de tráfico se sitúa más allá del derecho del 18.3. De ahí que la legislación que permite su tratamiento, conservación

⁴⁴ «[L]os listados telefónicos incorporan datos [...] para cuyo conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación mientras está teniendo lugar»; STC 123/2002, de 20 de mayo (FJ. 6).

⁴⁵ STEDH de 2 de agosto de 1984 (asunto *Malone c. Reino Unido*; § 84). El TEDH distingue en esta sentencia el recabo de esos datos por parte de las operadoras *motu proprio* y la posterior entrega a las autoridades, de su intervención como consecuencia del mandato de la autoridad: «El Estado no exige que el *Post Office* establezca registros de esta clase, pero, si existen, puede obligarle a facilitar los datos como medios de prueba en los procesos civiles o penales en la forma acostumbrada, a saber, por la vía de *subpoena*. A este respecto, la situación del *Post Office* es la misma de cualquier poseedor de anotaciones de interés para el caso, como, por ejemplo, un Banco. La Policía y el Estado sólo pueden ordenar la aportación de los datos registrados por el *Post Office* por los medios normales. Sucede, sin embargo, que el *Post Office*, en algunas ocasiones, registra y comunica lo registrado, a petición de la policía, si las informaciones son indispensables para investigaciones de delitos graves y no pueden conseguirse de ninguna otra fuente» (§56). La conservación se limita, además, a «a aquellas categorías de datos que ya han sido tratadas o generadas, no imponiendo la obtención (el archivo) de datos que no son tratados por los operadores»; cfr. GONZÁLEZ LÓPEZ, J.J., «Comentarios a la Ley 25/2007...», *op.cit.*, pág. 6. En similar sentido, VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, pág. 1625.

y posterior cesión a los órganos encargados de la persecución penal deba considerarse como desarrollo del artículo 18.4 CE⁴⁶.

Las Directivas que sucesivamente se han ocupado de regular los datos de tráfico —Directivas 97/66/CE, 2002/58/CE y 2006/24/CE— se reconocen a sí mismas como *lex specialis* de la normativa de protección de datos en el sector de las comunicaciones electrónicas⁴⁷. En el mismo sentido se manifestó el Consejo de Estado en su Dictamen 32/2007, de 22 de febrero de 2007, sobre el Anteproyecto de la Ley de Conservación de datos, al afirmar que a la vista de la separación del ámbito de protección constitucional del derecho al secreto de las comunicaciones (que alcanza al proceso de comunicación mismo), en relación con los ámbitos de protección de otros derechos, «la cuestión merece ser examinada desde la perspectiva del derecho a la protección de datos que [...] puede considerarse como el más directamente amenazado por las medidas previstas en el Anteproyecto». Por lo demás, la LCD se estructura como una norma de protección de datos, regulando en su Capítulo II los deberes de los sujetos obligados de conservación, cesión, protección y seguridad de los datos y estableciendo excepciones a los derechos generalmente reconocidos en la normativa de protección de datos de acceso y cancelación⁴⁸.

Las opiniones favorables a extender la garantía formal del secreto de las comunicaciones al acceso a datos pertenecientes a comunicaciones consumadas parecen entender que, en otro caso, los datos de tráfico se hallarían desprovistos de protección⁴⁹.

⁴⁶ ORTIZ PRADILLO, J.C., «Tecnología versus proporcionalidad en la investigación penal...», *op.cit.*, pág. 16.

⁴⁷ Del mismo modo, el Reglamento 2016/679 de 27 de abril de 2016 (Reglamento general de protección de datos) establece en su Considerando 173 que «debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento» y, en conexión con ello, la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE, dispone en su Considerando 5: «Las disposiciones del presente Reglamento precisan y complementan las normas generales sobre la protección de datos personales establecidas en el Reglamento (UE) 2016/679 en lo que respecta a los datos de comunicaciones electrónicas que pueden considerarse datos personales».

⁴⁸ RODRÍGUEZ LAINZ, J.L., «El principio de proporcionalidad...», *op.cit.*, pág. 15.

⁴⁹ Así, la Consulta 1/1999, de 22 de enero, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones. Algún autor ha defendido que la conservación también afecta

Sin embargo, su exclusión del objeto del derecho del 18.3 CE no cuestiona que los datos de tráfico constituyan un bien jurídico digno de protección, sino que una delimitación iusfundamental constitucionalmente conforme determina su inclusión en el objeto del 18.4 CE, al tratarse de datos registrados en un soporte físico que son susceptibles de tratamiento y que, más allá de su origen en concretos procesos comunicativos, poseen una entidad y valor informativo propios⁵⁰.

Por último, la regulación de las posibilidades de acceso a datos de tráfico conservados se encuentra en el art. 588 ter j LECrim, en una sección diferenciada de la interceptación de datos de tráfico en tiempo real (que se regula junto a la intervención de las comunicaciones), en lógica coherencia con el hecho de hallarnos ante medidas limitativas de derechos fundamentales distintos.

Solo se permite su incorporación al proceso como fuente de prueba mediante autorización judicial y se restringe, en principio, a los delitos que permiten la intervención de las comunicaciones. No obstante, estas garantías no pueden derivarse, por lo hasta ahora dicho, del art. 18.3 CE, sino que vienen determinadas, como reconoce el propio preámbulo de la ley que las introdujo, por un lado, por la exigencia de autorización judicial prevista ya en la LCD para la cesión de datos de tráfico a los agentes facultados (arts. 1.1 y 6) y, por otro, en atención al principio de proporcionalidad que exige las máximas cautelas debido a la ingente cantidad de datos de tráfico que se generan diariamente y la sensibilidad de la información que los mismos pueden revelar, lo que justifica un régimen reforzado y singular respecto al régimen jurídico general de protección de datos⁵¹.

al secreto de las comunicaciones, pero solo respecto de los datos de identificación de los comunicantes (en puridad, de los terminales de los interlocutores) y no de otros datos de tráfico, como la duración o la localización de la comunicación, que afectarían, en su opinión, al derecho a la intimidad. Cfr. FERNÁNDEZ RODRÍGUEZ, J.J., «Los datos de tráfico de comunicaciones...», *op.cit.*, págs. 100 y ss.

⁵⁰ ANCOS FRANCO, H., «El tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones...», *op.cit.*, págs. 5-6.

⁵¹ «La reforma acoge el criterio fijado por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, e impone la exigencia de autorización judicial para su cesión a los agentes facultados, siempre que se trate de datos vinculados a procesos de comunicación. Su incorporación al proceso solo se autoriza cuando se trate de la investigación de un delito que, por razones vinculadas al principio de proporcionalidad, sea de los que justifican el sacrificio de la inviolabilidad de las comunicaciones», Apartado IV del Preámbulo de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley

B. Datos en poder de los comunicantes

El acceso a datos de tráfico asociados a comunicaciones consumadas a través del registro de dispositivos en poder de los comunicantes no compromete el derecho fundamental al secreto de las comunicaciones. Constituye una injerencia en el derecho fundamental a la intimidad del art. 18.1 CE en la medida en que el examen de los contenidos que dichos dispositivos albergan permite generar «una definición del perfil vital íntimo del usuario»⁵².

En este sentido, el Tribunal Constitucional ha afirmado, en Sentencia 173/2011, de 7 de noviembre (FJ. 2), lo siguiente:

«Si no hay duda de que los datos personales relativos a una persona individualmente considerados [...] están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal [...] no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano»⁵³.

No obstante, debido a la diversidad de contenidos que pueden alojarse en este tipo de dispositivos, determinadas voces doctrinales y jurisprudenciales han sugerido la conveniencia de ofrecer un tratamiento unitario afirmando la existencia de un «derecho al propio entorno virtual» que integraría los objetos de los distintos derechos declarados en el art. 18 CE⁵⁴.

de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. *Vid.*, sobre la necesidad de autorización judicial para la cesión de datos de tráfico, GONZÁLEZ LÓPEZ, J.J., «Comentarios a la Ley 25/2007...», *op.cit.*, pág. 8; y MARCHENA GÓMEZ, M., «La vulneración de derechos fundamentales...», *op.cit.*, pág. 8.

⁵² ZOCO ZABALA, C., «Secreto de las comunicaciones en la frontera...», *op.cit.*, pág. 332. La exclusión de injerencia en el 18.3 CE en estos casos es defendida también en VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», *op.cit.*, pág. 1620.

⁵³ También el TEDH ha considerado el acceso a dispositivos informáticos como una injerencia en la vida privada del art. 8 CEDH: «[...] el acceso a los archivos del ordenador personal del demandante y la condena resultante constituyen una “injerencia de las Autoridades públicas” en el derecho a la vida privada del interesado», STEDH de 30 de mayo de 2017 (asunto *Trabajo Rueda c. España*). Un comentario a esta sentencia puede encontrarse en: OCÓN GARCÍA, J., «Derecho a la intimidad y registro de dispositivos informáticos: a propósito del asunto *Trabajo Rueda c. España*», *Revista Española de Derecho Constitucional*, 113, 2018, págs. 327-343.

⁵⁴ «[L]a ponderación judicial de las razones que justifican [...] el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo y [...] su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores

En todo caso, y como venimos manteniendo, los datos archivados en los terminales no están protegidos por el art. 18.3 CE, pues, tratándose de comunicaciones finalizadas, su pretendida tutela a través del secreto de las comunicaciones desbordaría su objeto *vía* eficacia temporal.

En estos términos se había venido pronunciando el Tribunal Supremo, que, con base en la doctrina constitucional que circunscribe el secreto de las comunicaciones al proceso de la comunicación, distingue las injerencias producidas sobre comunicaciones activas, objeto del 18.3 CE, de las llevadas a cabo sobre comunicaciones concluidas y, por tanto, susceptibles de vulnerar el 18.⁵⁵

Igualmente, la STC 70/2002, de 3 de abril (FJ. 9) considera que la intervención por la Guardia Civil de una carta ya leída que estaba en posesión de su destinatario «no interfiere un proceso de comunicación, sino que el citado proceso ya se ha consumado, lo que justifica el tratamiento del documento como tal (como efectos del delincuente que se examinan y se ponen a disposición judicial) y no en el marco del secreto de las comunicaciones». En este caso la aprehensión recae sobre el contenido comunicado por lo que, con más razón, debería ser proyectable sobre los datos de tráfico.

A mayor abundamiento, el Tribunal Constitucional ha mantenido desde las SSTC 123/2002, de 20 de mayo (FJ. 5), y 281/2006, de 9 de octubre (FJ. 3), que la específica protección constitucional «reside en la especial vulnerabilidad de la

del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria»; cfr. STS, Sala de lo Penal, de 17 de abril de 2013 (FJ. 8). También en esta línea, SSTS, Sala de lo Penal, de 18 de julio de 2014, 24 de febrero de 2015, 4 de diciembre de 2015 y 10 de marzo de 2016. Sobre el origen, reconocimiento y alcance de este derecho, *vid.* ORTIZ PRADILLO, J.C., «Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos», BAUZÁ REILLY, M. y BUENO DE MATA, F. (Coords.), *El derecho en la sociedad telemática. Estudios en homenaje al profesor Valentín Carrascosa López*, Andavira, Santiago de Compostela, 2012, págs. 57-86; LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», DÍAZ MARTÍNEZ, M. y LÓPEZ-BARAJAS PEREA, I. (Coords.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant Lo Blanch, Valencia, 2018, págs. 135-167; y ZOCO ZABALA, C., «Secreto de las comunicaciones en la frontera...», *op.cit.*, págs. 321 y ss.

⁵⁵ Así, la STS, Sala de lo Penal, de 25 de noviembre de 2008 (FJ. 3), afirma: «La Audiencia distinguió con acierto entre "comunicación *ex novo*" y "comunicación concluida", al recoger la doctrina consolidada del Tribunal Constitucional, lo que supondría un distinto régimen jurídico. [...]. En nuestro caso se trataba de unas comunicaciones por Internet, ya celebradas y concluidas, de tal suerte que sólo constituía material de archivo". En el mismo sentido, SSTS, Sala de lo Penal de 27 de junio de 2002 (FJ. 3) y 30 de noviembre de 2005 (FJ. 1).

confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación». Finalizada la comunicación los datos de tráfico se hallan en poder de los comunicantes y, por tanto, desaparecida la vulnerabilidad que origina su protección, estos pueden decidir conservar o borrar dichos registros, sustrayéndolos así de eventuales inmisiones ajenas⁵⁶.

No obstante, la STC 230/2007, de 5 de noviembre, rompe la línea doctrinal mantenida hasta el momento al residenciar en el art. 18.3 el acceso de la Guardia Civil al registro de llamadas memorizado en un terminal, por cuanto «dicho acceso no resulta conforme a la doctrina constitucional reiteradamente expuesta sobre que la identificación de los intervinientes en la comunicación queda cubierta por el secreto de las comunicaciones»⁵⁷.

En este pronunciamiento el Tribunal toma en consideración únicamente el ámbito objetivo del secreto que, como hemos venido diciendo, se proyecta también sobre los datos de tráfico. Sin embargo, no repara, erróneamente según creemos, en su ámbito temporal, lo que hubiese determinado la exclusión del acceso enjuiciado de la protección dispensada por el 18.3 CE por tratarse de datos de comunicaciones consumadas⁵⁸.

⁵⁶ Esta recuperación del *dominus* por parte de los comunicantes sobre la comunicación finalizada se tiene en cuenta por la STS, Sala de lo Penal, de 30 de noviembre de 2005 (FJ. 1), que, enjuiciando el acceso desde de un terminal telefónico a la lista de llamadas entrantes y salientes, afirma que «[s]e trata de una comprobación de una agenda que contiene datos almacenados y que pudieron ser borrados por el titular o, incluso, bloqueados por el titular».

⁵⁷ Esta doctrina ha tenido, inevitablemente, repercusión en la jurisprudencia del Tribunal Supremo. Así, por ejemplo, la STS, Sala de lo Penal, de 11 de marzo de 2010 (FJ. 3), con base en la nueva línea interpretativa del Tribunal Constitucional, afirma que «[...] la Guardia Civil examinó el listado de llamadas que aparecía en el teléfono móvil, sin consentimiento del titular y sin autorización judicial, por lo que se produjo una vulneración del derecho del titular de la línea al secreto de sus comunicaciones telefónicas, en cuanto que, sin autorización judicial, se accedió a datos obtenidos durante el proceso de comunicación relativos a la identidad de los comunicantes y al momento y duración temporal de la llamada». También en este sentido, aunque con redacción algo confusa, STS, Sala de lo Penal, de 3 de marzo de 2020 (FJ. 2).

⁵⁸ LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas, op.cit.*, pág. 66. En una sentencia anterior, la 56/2003, de 24 de marzo (FJ. 3), el Tribunal Constitucional ya había confrontado con el art. 18.3 el acceso por parte de la Guardia Civil a datos de comunicaciones consumadas alojados en el dispositivo telefónico de uno de los comunicantes, si bien salvando la legitimidad de la inmisión en el consentimiento de su titular.

Es muy posible, y así ha sido puesto de manifiesto por algunos autores, que este cambio doctrinal tenga como origen una mejorable interpretación de la STEDH de 3 de abril de 2007 (asunto *Copland c. Reino Unido*), dictada solo unos meses antes y a la que la propia sentencia del Tribunal Constitucional hace expresa referencia (FJ. 3)⁵⁹.

En la citada sentencia, el TEDH confronta el art. 8 CEDH con el acceso por el empleador a los dispositivos informáticos de su propiedad utilizados por una empleada. Pero, sin embargo, el escrutinio se produce, de entre los objetos del amplio art. 8 CEDH, desde el parámetro general de la vida privada y no estrictamente desde el derecho al secreto de la correspondencia. Conclusión fácilmente alcanzable si atendemos al hecho de que el tribunal arranca su argumentación delimitando el alcance de la vida privada (*Scope of private life*, §41) y, sobre todo, valora conjuntamente datos de comunicaciones mantenidas en canal cerrado (correos electrónicos y llamadas telefónicas) con datos de navegación a través de internet, no amparables por el art. 18.3 CE⁶⁰.

Por lo tanto, hubiese sido igualmente respetuoso con el art. 10.2, y más preciso en cuanto a la delimitación de los derechos fundamentales internos afectados, valorar el registro efectuado por la Guardia Civil en la STC 230/2007 desde el punto de vista del derecho a la intimidad, como proponía la resolución recurrida y como el mismo Tribunal Constitucional había entendido en ocasiones anteriores.

Por su parte, el acceso a contenidos alojados en dispositivos informáticos se encuentra en la actualidad reglamentado, tras la reforma operada por la Ley Orgánica 13/2015, en la Ley de Enjuiciamiento Criminal, bajo la rúbrica *Registro de*

⁵⁹ Cfr. RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones...*, *op.cit.*, pág. 32 y RIVERO SÁNCHEZ-COVISA, F.J., *Revisión del concepto constitucional...*, *op.cit.*, pág. 26.

⁶⁰ «[E]l Tribunal considera que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la demandante, sin su conocimiento, constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia, en el sentido del artículo 8 del Convenio», STEDH de 3 de abril de 2007 (asunto *Copland c. Reino Unido*), § 44.

dispositivos de almacenamiento masivo de información (arts. 588 sexies a y siguientes)⁶¹.

La regulación de esta medida avala en cierto modo la interpretación realizada hasta el momento sobre el acceso a datos de tráfico soportados en terminales informáticos pues, si bien permite acceder al contenido de ordenadores y a «instrumentos de comunicación telefónica o telemática», resulta patente que no está desarrollando una diligencia que incida en el derecho fundamental al secreto de las comunicaciones.

En primer lugar, porque no somete tal medida a una lista cerrada de delitos, como lo hace al regular la intervención de comunicaciones. Pero, sobre todo, porque permite, para casos de urgencia, el acceso directo a los datos del dispositivo por parte de la Policía Judicial o del Ministerio Fiscal (art. 588 sexies c.4). La práctica directa y ulterior convalidación judicial de la intervención no es posible —fuera de los casos de suspensión individual prevista en el 55.2 CE— para la limitación del derecho fundamental al secreto de las comunicaciones, en el que la necesidad de autorización judicial previa no admite excepciones, pero lo cierto es que ha sido avalada por la jurisprudencia reiteradamente en supuestos de injerencias leves en el objeto del derecho a la intimidad⁶².

Cabe concluir, por tanto, que los datos de tráfico, entendiendo por tales aquellos que se hallan vinculados a una concreta comunicación por una relación de dependencia funcional, están protegidos por el derecho fundamental al secreto de las comunicaciones en tanto su acopio se produzca sobre procesos comunicativos en curso. Sin embargo, el acceso a datos de tráfico relativos a comunicaciones consumadas en poder de prestadores de servicios de telecomunicaciones o

⁶¹ «[E]n rigor, las normas habilitantes para aquellos casos en los que el proceso comunicativo ha concluido —o aún no ha empezado— no serán las contenidas en los artículos 588 ter LECrim, en la medida en que, como se ha dicho, no existe proceso comunicativo, sino las previstas en los artículos 588 sexies LECrim, relativos al registro de dispositivos de almacenamiento masivo de información»; cfr. GONZÁLEZ NAVARRO, A., «Medios tecnológicos de investigación...», *op.cit.*, pág. 270. Sobre la regulación y derechos fundamentales afectados por esta medida, *vid.* LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual...», *op.cit.*, págs. 135-167; y OCÓN GARCÍA, J., «Derecho a la intimidad y registro de dispositivos informáticos...», *op.cit.*, págs. 327-343.

⁶² Por todas, SSTC 207/1996, de 16 de diciembre (FJ. 4), 70/2002, de 3 de abril (FJ. 10), 173/2011, de 7 de noviembre (FJ. 7), y 115/2013, de 9 de mayo (FJ. 6).

archivados en dispositivos en posesión de los comunicantes desbordan el objeto del 18.3 CE y su tutela corresponde a otros derechos (protección de datos e intimidad).

CAPÍTULO QUINTO

EL CONTENIDO DEL DERECHO FUNDAMENTAL AL SECRETO DE LAS COMUNICACIONES

I. LA DOBLE DIMENSIÓN DEL DERECHO FUNDAMENTAL

II. CONTENIDO SUBJETIVO DEL DERECHO

II.1. La intervención constitucional de las comunicaciones ¿límite o delimitación?

II.2. El legislador del artículo 18.3 CE: la previsión del límite

A. La necesidad de *interpositio legislatoris*

B. La «calidad» de la norma limitadora

C. Fundamentos de la limitación

D. Los límites a la actividad limitadora del legislador

D.1. El contenido esencial como límite de los límites

D.2. La proporcionalidad del límite como parámetro de constitucionalidad de la ley

II.3. El juez del artículo 18.3 CE: la aplicación del límite

A. El juicio sobre la decisión de intervención

A.1. Presupuestos para la aplicación del límite

A.2. El test de proporcionalidad

B. La resolución judicial

C. Práctica de la intervención y control judicial

III. CONTENIDO OBJETIVO. EL SECRETO DE LAS COMUNICACIONES EN LAS RELACIONES ENTRE PARTICULARES

III.1. Fundamentos constitucionales de la dimensión objetiva de los derechos fundamentales

III.2. Dimensión objetiva del derecho fundamental al secreto de las comunicaciones

A. El efecto irradiante de los derechos fundamentales

B. El deber de protección de los derechos fundamentales

III.3. El derecho fundamental al secreto de las comunicaciones en las relaciones entre particulares

I. LA DOBLE DIMENSIÓN DEL DERECHO FUNDAMENTAL

El origen de la categoría que hoy denominamos *derecho fundamental* se encuentra en las declaraciones de derechos de finales del XVIII; y nacen, como es sabido, como derechos del ciudadano frente al poder público.

Sirviéndose de la preexistente categoría de derecho subjetivo, los derechos fundamentales se configuran, en primer término, como derechos de defensa del ciudadano frente a la actividad del Estado¹. Son, por ello, derechos públicos subjetivos.

La relación poder público – derecho fundamental es en principio, por tanto, de carácter negativo. El Estado está obligado a no lesionar la esfera individual protegida por los derechos fundamentales, a abstenerse de cualquier injerencia en ella. Se encuentra así, en primer lugar, vinculado negativamente a los derechos fundamentales. Esta prohibición de inmisión del poder público en el ámbito vedado por el derecho fundamental garantiza al ciudadano un ámbito de libertad y, al tiempo, le confiere una acción para reaccionar jurídicamente contra su incumplimiento.

Mediante el secreto de las comunicaciones se prohíben injerencias ilegítimas y, a su través, se garantiza la libertad para llevar aquéllas a cabo. Pero tal prohibición no es, en el art. 18.3 CE, de carácter absoluto, sino que

¹ «[L]os derechos fundamentales son, ante todo, derechos frente al Estado (STC 5/1981, FJ. 9) o frente al poder (STC 197/1988, FJ. 4), afirmación cuyo fundamento no está, o no está sólo, en la historia, sino, en lo que aquí más importa, en el sentido mismo de lo que es, y para lo que sirve, una Constitución». JIMÉNEZ CAMPO, J., *Derechos fundamentales. Concepto y garantías*, Trotta, Madrid, 1999, pág. 35.

la norma iusfundamental prevé al mismo tiempo, con las garantías que analizaremos, un espacio de injerencia constitucionalmente conforme.

En tal sentido, el contenido jurídico-subjetivo del derecho fundamental al secreto de las comunicaciones consistirá en la potestad de su titular para reaccionar frente al incumplimiento de dicha prohibición, en la medida en que no se hubieran observado las salvaguardas constitucionales exigidas para excepcionarla.

No obstante, junto a esta primigenia dimensión subjetiva, se ha señalado doctrinal y jurisprudencialmente la existencia de una dimensión objetiva de los derechos fundamentales².

La categoría de derecho subjetivo incorpora, cuando actúa como bastidor del derecho fundamental, una carga ideológica, un contenido valorativo que le acompaña jurídicamente³. El reconocimiento de ese contenido en el seno de las normas iusfundamentales, al tiempo que refuerzan su validez —«son fundamento del orden político», art. 10.1 CE—, les dota de una dimensión objetiva que ilumina todos los sectores del ordenamiento,

² Una visión histórica de esta doble dimensión y su incidencia en diversos ordenamientos puede hallarse en DI MARTINO, A., «La doppia dimensione dei diritti fondamentali», *Rivista del Gruppo di Pisa*, 2, 2016, págs. 1-63. Entre nosotros, *vid.*, entre otros, SALVADOR MARTÍNEZ, M., «Sobre el contenido objetivo de los derechos fundamentales», APARICIO PÉREZ, M.A. (Coord.), *Derechos Constitucionales y Formas Políticas. Actas del Congreso sobre derechos Constitucionales y Estado autonómico*, Cedecs, Barcelona, 2001, págs. 199-218; SALVADOR MARTÍNEZ, M., «El doble contenido de los derechos fundamentales en la doctrina alemana», *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, 7, 1997-1998, págs. 115-142; GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva...*, *op.cit.*; FERNÁNDEZ SEGADO, F., «La teoría jurídica de los derechos fundamentales en la doctrina constitucional», *Revista Española de Derecho Constitucional*, 39, 1993, págs. 195-250; y BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, págs. 50 y ss. Sobre la múltiple dimensión de los derechos fundamentales en nuestro sistema constitucional puede verse CRUZ VILLALÓN, P. y PARDO FALCÓN, J., «Los derechos fundamentales en la Constitución Española de 1978», *Boletín Mexicano de Derecho Comparado*, 97, 2000, págs. 65-154.

³ CHUECA RODRÍGUEZ, R., «Debilidades estructurales del derecho fundamental», *op.cit.*, pág. 44.

actuando como criterios ordenadores en forma de «impulsos orientados» de la actuación de los poderes constituidos⁴.

La construcción dogmática inicial de la doble dimensión —subjetiva y objetiva— de los derechos fundamentales corresponde al Tribunal Constitucional Federal alemán, quien, en el conocido asunto *Lüth* —*BVerfGE* 7, 198, de 15 de enero de 1958— considera que:

«[...] los derechos fundamentales se encuentran destinados a asegurar en primer lugar la esfera de libertad de los individuos frente a las intervenciones de los poderes públicos; son derechos de defensa de los ciudadanos en contra del Estado. [...]. Por otro lado, también es cierto que la Ley Fundamental no pretende ser un ordenamiento de valores neutral (*BVerfGE* 2, 1 [12]; 5, 85 [134 y ss., 197 y ss.]; 6, 32 [40 ss.]), sino que ha establecido —en su capítulo sobre derechos fundamentales— un orden de valores objetivo, a través del cual se pone de manifiesto la decisión fundamental de fortalecer el ámbito de aplicación de los derechos fundamentales (*Klein / v. Mangoldt, Das Bonner Grundgesetz*, t. III, 4, notas al Art. 1, p. 93). La dignidad del ser humano y el libre desarrollo de la personalidad (la cual se desenvuelve en el interior de una comunidad social) forman el núcleo de este sistema de valores, el cual constituye, a su vez, una decisión jurídico-constitucional fundamental, válida para todas las esferas del derecho; así, este sistema de valores aporta directivas e impulsos al Poder Legislativo, a la Administración y a la Judicatura».

Por su parte, nuestro Tribunal Constitucional consideró tempranamente que este doble carácter también se deriva del sistema iusfundamental de la Constitución de 1978. En una de sus primeras sentencias —*STC* 25/1981, de 14 de julio (FJ. 5)— afirma:

⁴ En este sentido, *vid.* CHUECA RODRÍGUEZ, R., «Debilidades estructurales del derecho fundamental», *op.cit.*, pág. 46; JIMÉNEZ CAMPO, J., *Derechos fundamentales...*, *op.cit.*, pág. 30; y SALVADOR MARTÍNEZ, M., «Sobre el contenido objetivo...», *op.cit.*, pág. 201. También nuestro Tribunal Constitucional —*STC* 53/1985, de 11 de abril (FJ. 4)—: «los derechos fundamentales [...] son la expresión jurídica de un sistema de valores que, por decisión del constituyente, ha de informar el conjunto de la organización jurídica y política».

«En primer lugar, los derechos fundamentales son derechos subjetivos, derechos de los individuos no sólo en cuanto derechos de los ciudadanos en sentido estricto, sino en cuanto garantizan un *status* jurídico o la libertad en un ámbito de la existencia. Pero al propio tiempo, son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado social de Derecho o el Estado social y democrático de Derecho, según la fórmula de nuestra Constitución (art. 1.1)»⁵.

Así pues, más allá de la obligación del Estado de sujeción a la indemnidad de los derechos fundamentales, los poderes públicos están vinculados positivamente y forzados por tanto al logro de su efectividad⁶.

Por otro lado, y pese a que los derechos fundamentales nacen y mueren, en términos estrictos, en relación al Estado⁷, el contenido ideológico que incorporan no posee una naturaleza estatal, sino que proyecta una aspiración universal al alinearse con un sistema de valores compartido entre las democracias avanzadas y reconocerse en instrumentos internacionales de protección de derechos⁸.

⁵ La doble dimensión de los derechos fundamentales «se infiere de un texto constitucional que, tras proclamar el Estado social y democrático de Derecho (art. 1.1 CE), y, por ende, comprometer a los poderes públicos en la promoción de la libertad y la igualdad el individuo (art. 9.2 CE), eleva el libre desarrollo de la personalidad y el respeto a los derechos de los demás a la condición de fundamento del orden político y de la paz social (art. 10.1 C.E.)»; ATC 382/1996, de 18 de diciembre (FJ. 3).

⁶ STC 53/1985, de 11 de abril (FJ. 4). Obligación positiva que afecta con especial intensidad al legislador, pero que extiende a toda la actividad estatal: «a la conformación material de prescripciones de Derecho por parte del legislador o normador [...]; a la actuación del ejecutivo en el ámbito de sus funciones y a la interpretación y aplicación de prescripciones por parte del juez». Cfr. BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 50.

⁷ «Los derechos fundamentales acaban con las Constituciones. Ello es tanto como afirmar que acaban, hoy por hoy, con los Estados, dentro de los Estados, en el interior del ordenamiento estatal»; CRUZ VILLALÓN, P., «Formación y evolución...», *op.cit.*, pág. 42.

⁸ «[...] los derechos fundamentales responden a un sistema de valores y principios de alcance universal que subyacen a la Declaración Universal y a los diversos convenios internacionales sobre Derechos Humanos, ratificados por España, y que, asumidos como decisión constitucional básica, han de informar todo nuestro ordenamiento jurídico», *vid.* STC 21/1981, de 15 de junio (FJ. 10).

Esta doctrina de la doble dimensión ha terminado por asumirse en el ámbito del Convenio Europeo de Derechos Humanos. Si bien el enfoque original del Convenio trasluce una dimensión defensiva e individual de los derechos, el Tribunal de Estrasburgo fue apreciando la existencia en su articulado de un orden objetivo de valores, del que dimanaban obligaciones objetivamente exigibles a los Estados firmantes⁹.

Estas obligaciones, aunque de alcance variable para los diversos derechos del Convenio, han sido puestas de manifiesto, en lo que aquí interesa, en el caso del art. 8 CEDH. El TEDH ha declarado así que «aunque el artículo 8 tiene esencialmente como objeto la protección del individuo contra las injerencias arbitrarias de los poderes públicos, no se limita a obligar al Estado a abstenerse de tales injerencias. A esta obligación negativa pueden añadirse obligaciones positivas inherentes a un respeto efectivo de la vida privada o familiar»¹⁰.

La importancia de la doble dimensión de los derechos fundamentales ha terminado por causar una suerte de novación del concepto inicial de derecho fundamental, al incorporar un potencial irradiante sobre el ordenamiento jurídico como totalidad: un mandato de optimización impuesto a los poderes públicos y, mediatamente, una eventual eficacia en las relaciones entre particulares¹¹.

⁹ DI MARTINO, A., «La doppia dimensione...», *op.cit.*, págs. 48 y ss.

¹⁰ STEDH de 26 de marzo de 1985 (asunto *X e Y c. Países Bajos*, §23). Más recientemente, en similar sentido: SSTEDH de 7 de febrero de 2012 (asunto *Von Hannover c. Alemania*, §98); 16 de julio de 2014 (asunto *Hämäläinen c. Finlandia*, §62); y 5 de septiembre de 2017 (asunto *Barbulescu c. Rumania*, §107).

¹¹ CHUECA RODRÍGUEZ, R., «Debilidades estructurales del derecho fundamental», *op.cit.*, pág. 46

A ello prestaremos atención en el presente capítulo. Reparando, en primer término, en el contenido subjetivo del derecho al secreto de las comunicaciones y las posibles restricciones a su ejercicio para, en un segundo apartado, analizar las consecuencias derivadas del reconocimiento de la dimensión objetiva del derecho que estudiamos.

II. CONTENIDO SUBJETIVO DEL DERECHO

«Se garantiza el secreto de las comunicaciones [...], salvo resolución judicial». El 18.3 CE explicita de esta forma la máxima tantas veces repetida según la cual no existen derechos fundamentales absolutos¹².

No obstante, el precepto constitucional no precisa las condiciones y circunstancias en que el derecho activa la excepción, sino tan solo el órgano encargado de llevarla a cabo.

El objeto del derecho —el secreto de las comunicaciones, en los términos ya definidos— no se garantiza por la norma iusfundamental disponiendo una incondicional prohibición de ruptura, sino previendo las condiciones de su levantamiento legítimo: expresamente, por resolución judicial. La facultad de reaccionar frente a la inobservancia de tales condiciones integra, como dijimos, el contenido subjetivo del derecho¹³.

Dedicamos las páginas que siguen al análisis de las circunstancias que permiten levantar, según constitución, en el caso concreto, el secreto de las comunicaciones. Y por tanto, los supuestos en que, de producirse contravención, apodera al titular del derecho a accionar jurídicamente para obtener la declaración judicial de ilicitud.

II.1. La intervención constitucional de las comunicaciones ¿límite o delimitación?

La Constitución habilita en determinadas ocasiones al poder público para restringir de algún modo los derechos fundamentales que, *prima facie*, declara; ya sea mediante la mera interpretación de las normas

¹² Por todas, STC 11/1981, de 8 de abril (FJ. 7): «ningún derecho, ni aún los de naturaleza o carácter constitucional, pueden considerarse como ilimitados».

¹³ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 56.

constitucionales, ya exigiendo una actividad —normativa o judicial— para determinar tal restricción.

El ordenamiento acoge previsiones constitucionales que permiten excluir, o excluyen directamente, la protección dispensada a conductas que, en principio, podrían estar incluidas en el objeto del derecho fundamental¹⁴.

Sin embargo, esas restricciones no comparten en todos los casos las mismas características y esa diversidad condiciona el modo en que operan los poderes constituidos habilitados para tal fin.

Por ello, doctrinalmente se han elaborado diferentes clasificaciones acerca de las restricciones, o límites en sentido amplio, que pueden incidir sobre los derechos fundamentales y su configuración constitucional.

En este sentido, JIMÉNEZ CAMPO distingue entre limitación y delimitación de los derechos fundamentales. Mientras que el concepto *delimitación* incluiría «todas las acciones públicas que contribuyen a definir los contornos generales y objetivos de un derecho fundamental», los límites serían solamente aquellas habilitaciones constitucionales que permiten al poder público constreñir, excepcionar o privar de un derecho ya definido¹⁵.

De esta manera, mediante la delimitación se definen los contornos del derecho fundamental, se establece qué acciones caen dentro de su objeto y cuáles, sin embargo, quedan fuera. Esta definición puede venir dada por los propios términos en que se expresa la norma constitucional (lo que el autor denomina *delimitación directa*) o por la mera convivencia del derecho con otros derechos y bienes constitucionalmente reconocidos (*delimitación indirecta*)¹⁶. A su vez, la delimitación directa puede venir expresada bien en

¹⁴ BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, Dykinson, Madrid, 2004, pág. 78. En el mismo sentido, BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 120.

¹⁵ JIMÉNEZ CAMPO, J., *Derechos fundamentales...*, *op.cit.*, pág. 38.

¹⁶ No obstante, como el propio autor señala, los términos en que en ocasiones se expresa la Constitución difieren de la distinción propuesta. Así, por ejemplo, el art. 20.4 CE señala que «[e]stas libertades tienen su *límite* en el respeto a los derechos reconocidos en este Título...», cuando, en la propuesta de JIMÉNEZ CAMPO, estaríamos ante un caso de delimitación. Esta

términos positivos (mediante la definición de la conducta garantizada —en los capítulos precedentes hemos «delimitado» los conceptos de *comunicación* y *secreto* en el art. 18.3 CE—), o bien en términos negativos, excluyendo de la garantía iusfundamental ciertas conductas¹⁷.

Por otro lado, nos hallaríamos ante *límites*, estrictamente considerados, en aquellos casos en que la Constitución permite al legislador restringir o privar de la titularidad o del ejercicio de un derecho fundamental, una vez delimitado, a un sujeto o a un colectivo —como sucede para el caso de la libertad sindical en el art. 28.1—; y también cuando la propia norma que declara el derecho posibilita su privación singular. A este segundo grupo pertenecen, entre otros, el secuestro judicial de publicaciones (art. 20.5), la posibilidad de prohibir reuniones en lugares de tránsito público (21.2) y también, para el derecho objeto del presente trabajo, la posibilidad de intervención judicial de comunicaciones¹⁸.

Por su parte, VILLAVERDE MENÉNDEZ diferencia entre límites internos y límites externos —o límites en sentido propio—. Los primeros vendrían a

terminología es también frecuente en la jurisprudencia del Tribunal Constitucional: «Todo derecho tiene sus *límites* que, como señalaba este Tribunal en Sentencia de 8 de abril de 1981 en relación a los derechos fundamentales, establece la Constitución por sí misma en algunas ocasiones, mientras en otras el *límite* deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos»; cfr. STC 2/1982, de 29 de enero (FJ. 5). En otras ocasiones, no obstante, ha utilizado los términos en el sentido propuesto: «El derecho a la propia imagen, como cualquier otro derecho, no es un derecho absoluto, y por ello su contenido se encuentra *delimitado* por el de otros derechos y bienes constitucionales»; STC 14/2003, de 28 de enero (FJ. 5). *Vid.*, en el mismo sentido, la nota siguiente. *Cursiva añadida*.

¹⁷ Así sucede, por ejemplo, cuando el art. 22.5 CE excluye las asociaciones paramilitares del objeto del derecho fundamental de asociación: este tipo de asociaciones no ven «limitado» su derecho fundamental a asociarse libremente, sino que las asociaciones de tal carácter no se encuentran protegidas, desde el principio, por el derecho fundamental. JIMÉNEZ CAMPO, J., *Derechos fundamentales...*, *op.cit.*, págs. 39 y ss. Para el caso del derecho de reunión, esta distinción entre limitación y delimitación ha sido expresamente afirmada por el Tribunal Constitucional: «Las reuniones no pacíficas [...] ya resultan excluidas del derecho de reunión por el primer párrafo de este precepto. El párrafo segundo del art. 21 CE no *delimita* el contenido del derecho de reunión, sino que establece un *límite* a su ejercicio y otorga a los poderes públicos una facultad que, como veremos, estos deben ejercer proporcionadamente...»; cfr. STC 66/1995, de 8 de mayo (FJ. 3). *Cursiva añadida*.

¹⁸ JIMÉNEZ CAMPO, J., *Derechos fundamentales...*, *op.cit.*, pág. 38.

configurar el ámbito protegido por el derecho excluyendo determinadas conductas que, por ello, no pertenecen a las amparadas en abstracto por el derecho fundamental. Los límites externos, sin embargo, excluyen de la garantía iusfundamental una de las conductas que son objeto de protección por el derecho fundamental¹⁹.

Dentro de los límites internos —que son en rigor «criterios de delimitación del objeto del derecho fundamental en cuestión»— se encuentran aquellos que vienen dispuestos explícitamente por la Constitución (que denomina «límites positivos» y entre los que señala el caso del art. 20.5 CE), así como los derivados de la coexistencia de los derechos fundamentales con otras normas constitucionales («límites lógicos»)²⁰.

En todo caso, estos límites internos, en la medida en que definen el derecho fundamental, pueden ser *concretados* por los poderes públicos a través de la interpretación directa de las normas constitucionales. Los límites externos, sin embargo, habilitan a un poder público para que, potestativamente, restrinja alguna de las conductas protegidas por el derecho fundamental. Son, por tanto, contingentes y, por ello, requieren ser *creados* por el órgano habilitado. En caso contrario, e incluso si el límite dispuesto normativamente no es aplicado efectivamente en el caso concreto, la conducta constitucionalmente limitable seguirá gozando de protección²¹.

Así pues, la posibilidad de levantar el secreto de las comunicaciones constituye, siguiendo las clasificaciones propuestas, un límite —externo— al derecho fundamental previsto en el 18.3 CE, pues supone la negación a una persona concreta (y sobre unas concretas comunicaciones durante un tiempo

¹⁹ VILLAVERDE MENÉNDEZ, I., «Concepto, contenido...», *op.cit.*, pág. 344 y BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, págs. 120 y ss.

²⁰ BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, págs. 120-121. Los *límites internos positivos* —que también denomina *límites explícitos* en VILLAVERDE MENÉNDEZ, I., «Concepto, contenido...», *op.cit.*, pág. 344— se identifican, así, con lo que JIMÉNEZ CAMPO denomina *delimitación directa*, de igual forma que los *límites internos lógicos* se corresponden con lo que éste califica como *delimitación indirecta*.

²¹ VILLAVERDE MENÉNDEZ, I., «Concepto, contenido...», *op.cit.*, pág. 345.

concreto) de una conducta que inicialmente está protegida por el derecho: la garantía de secreto, la prohibición de su ruptura²².

Contrariamente, ZOCO ZABALA ha entendido que se trata de «un “límite interno” de la definición constitucional del contenido de este derecho fundamental», pues su previsión excluye desde un principio determinadas expectativas de la garantía constitucional «sin necesidad de que un poder público habilitado cree una norma para realizar esa exclusión (que es la función de los límites externos)»²³.

No podemos compartir esta postura. La intervención de las comunicaciones judicialmente acordada supone una exención temporal a la prohibición de ruptura de secreto que dispone la norma iusfundamental, pero tal prohibición, sólo temporalmente eximida, forma parte del objeto del derecho²⁴.

La facultad de intervenir judicialmente las comunicaciones no *delimita* el derecho fundamental, no define su objeto protegido; sino que la decisión de levantar el secreto en el caso concreto supone, en puridad, una limitación. Antes y después de la autorización de intervención su titular se beneficia de la entera protección del derecho fundamental, en los términos en que hubiere sido delimitado, pero tal protección resulta completamente excluida para las comunicaciones objeto de intervención durante su vigencia²⁵.

Tampoco podemos estar de acuerdo con esta autora cuando afirma que «las consecuencias prácticas que se derivan de una u otra concepción no

²² «La intervención judicial de las comunicaciones integra una limitación del derecho al secreto de las mismas prevista en el propio texto constitucional (art. 18.3 CE)»; STC 146/2006, de 8 de mayo (FJ. 2b).

²³ ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 63.

²⁴ De esta manera, la aplicación del límite así previsto «consiste, justamente, en hacer de lo que inicialmente era un uso ilícito del poder público, un uso lícito del mismo»; cfr. VILLAVARDE MENÉNDEZ, I., «Concepto, contenido...», *op.cit.*, pág. 335.

²⁵ Resulta gráfica la STC 85/1994, de 14 de marzo (FJ.3), cuando afirma: «Se omite en ella toda referencia a la carencia de motivación de la providencia que otorgó *la autorización limitativa o excluyente, diríamos mejor, del derecho fundamental consagrado en el art. 18.3 CE*». *Cursiva añadida.*

difieren en gran medida, pues la intervención judicial, se defina como límite en sentido propio, o como criterio delimitador del contenido del derecho (como límite interno del contenido del derecho fundamental) tiene que ser motivada de modo suficiente»²⁶.

Consideramos, por el contrario, que el hecho de calificar como delimitación o como limitación la posibilidad de intervenir las comunicaciones posee implicaciones de calado. La delimitación, en tanto que actividad de interpretación del derecho fundamental para definir sus fronteras, no siempre requiere —aunque tampoco impide— la intervención del legislador²⁷. El juez puede *ex constitutione* interpretar de qué modo los criterios de delimitación expresamente previstos (la flagrancia del delito para el caso de la inviolabilidad del domicilio o el carácter paramilitar de las asociaciones) o los demás derechos o bienes constitucionales (la protección de la infancia en el caso de las libertades informativas, por ejemplo) demarcan las fronteras de un concreto derecho fundamental. Sin embargo, los límites externos requieren, como veremos en los subsiguientes epígrafes de este trabajo, de un acto de creación normativa para establecer las condiciones en que el órgano judicial puede, efectivamente y en el caso concreto, aplicar tal limitación, es decir, privar a un sujeto concreto del derecho fundamental primariamente definido²⁸.

²⁶ ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 63.

²⁷ En este sentido, JIMÉNEZ CAMPO señala que la delimitación constitucional reclama en ocasiones del legislador la precisión de determinados conceptos (lo que califica como «delimitación constitucional mediata»). Esto sucede, por ejemplo, cuando el 16.1 CE dispone que «el orden público protegido por la ley» *delimita* las libertades ideológicas, religiosa y de culto. La ley que defina dichos conceptos estará culminando lo que el autor denomina como «delimitación legislativa derivada del derecho fundamental». *Vid.* JIMÉNEZ CAMPO, J., *Derechos fundamentales...*, *op.cit.*, págs. 40-41.

²⁸ Claro que el juez deberá en ambos casos expresar las razones de la concreta virtualidad de un derecho fundamental, pero con diferente alcance. Al delimitar un derecho fundamental su motivación responderá por qué una determinada conducta no forma parte del objeto del derecho, y tales razones podrán tener como único basamento lo dispuesto en la Constitución. Por el contrario, la posibilidad de limitar un derecho fundamental requiere indefectiblemente que estén legalmente previstos los presupuestos y condiciones en que tal límite puede ser aplicado, y el objeto de la motivación será la expresión de la existencia y observancia de dichos presupuestos y condiciones. Contrariamente a lo que aquí defendemos, RODRÍGUEZ RUÍZ considera que en nuestro sistema iusfundamental solo son posibles los denominados por la doctrina alemana como «límites inmanentes», aquellos que se hallan implícitos en el

II.2. El legislador del artículo 18.3 CE: la previsión del límite

A. La necesidad de *interpositio legislatoris*

El artículo 18.3 CE prevé en su inciso final la posibilidad de que el poder público acceda al reducto secreto que garantiza en su primera proposición. No obstante, la literalidad del precepto identifica explícitamente sólo el órgano encargado de autorizar tal posibilidad: el juez.

Aunque algo hemos avanzado ya, se trata ahora de determinar con mayor profundidad si esta previsión limitativa es premisa suficiente para que el órgano judicial habilitado constitucionalmente pueda alzar el secreto o si, por el contrario, requiere de la previa actividad del legislador para precisar, no sólo el órgano judicial competente y el procedimiento oportuno, sino también los presupuestos y condiciones en que el juez, *ex lege* por tanto, puede autorizar su práctica.

Doctrina y jurisprudencia son unánimes al considerar la previa intervención legislativa como el escenario más conveniente en términos de precisión y homogeneidad del límite. Pero no se trata ahora de valorar la actividad del legislador desde un juicio de oportunidad o conveniencia, sino de necesidad.

Resulta en este sentido ineludible realizar una advertencia previa. El ordenamiento infraconstitucional español nunca ha estado —desde la entrada en vigor de la Constitución y, por tanto, desde el reconocimiento del derecho fundamental que venimos considerando— carente de norma que permitiese al juez, en la fase instructora del proceso penal, alzar el secreto de determinadas comunicaciones. La Ley de Enjuiciamiento Criminal preveía ya desde 1882 la posible intervención de la correspondencia postal y telegráfica

texto constitucional. De tal manera que tales límites serían concretables por cualquier operador jurídico, sirviendo la Constitución como norma jurídica directamente aplicable para la restricción de los derechos fundamentales en casos concretos. *Vid.* RODRÍGUEZ RUIZ, B., «El coste de los derechos fundamentales. Un comentario de la STC 49/1999, de 5 de abril», *Teoría y Realidad Constitucional*, 3, 1999, págs. 320-321.

del procesado «si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa».

El problema, al tiempo de aprobarse la Constitución, no residía, por tanto, en la carencia de regulación legal del límite constitucionalmente admitido, sino en su insuficiencia. Y ello tanto por la falta de previsión expresa de la posibilidad de intervenir ciertas comunicaciones —hasta 1988 no se regula, pese a su práctica frecuente, la intervención de comunicaciones telefónicas en la LECrim— como, colmado lo anterior, por la escasa precisión de los presupuestos y condiciones fijados en la norma para llevarla a cabo.

En este escenario, el Tribunal Constitucional pareció admitir en un primer momento, si bien *obiter dicta*, la posibilidad de limitar judicialmente el derecho al secreto de las comunicaciones sin recurso al legislador. La normatividad de la Constitución y la eficacia directa de sus derechos fundamentales bastarían para que el juez pueda levantar el secreto con base en la nuda previsión constitucional.

Así, la STC 22/1984, de 17 de febrero (FJ. 3), en un recurso de amparo por pretendida vulneración del 18.2, al no estar la autorización judicial de entrada y registro normativamente prevista para el caso *a quo*, afirma:

«[El Ministerio Fiscal] entiende que fuera de los casos del art. 546 de la LECr y de aquellos otros en que tal medida se encuentre expresamente establecida por una Ley, como es el caso del art. 130 de la Ley Tributaria para que el recaudador pueda entrar en el domicilio del contribuyente moroso, el Juez no puede expedir un mandamiento de entrada y registro. Esta tesis no puede ser compartida. De conformidad con una larga y ya tradicional doctrina de este Tribunal, la Constitución no es sólo la norma que fundamenta la organización política de la comunidad y el ordenamiento jurídico entero, sino que es también una norma de ejecución y efectos inmediatos. Ello es, además indiscutible respecto de los preceptos contenidos en los arts. 14 y 30, por ser objeto del proceso de amparo. Por consiguiente, la autoridad judicial está investida de la suficiente potestad para otorgar las autorizaciones de entrada y registro, de la

misma manera que ocurre en el apartado 3 del art. 18, donde se inviste a los Jueces de potestad para permitir el levantamiento parcial del secreto de las comunicaciones»²⁹.

Consideramos que la postura mantenida en este caso por el Tribunal Constitucional no es atendible. Si bien nadie duda hoy de la eficacia directa que tienen, al menos respecto de los poderes públicos, los derechos fundamentales, tal conclusión no puede extenderse sin más, como parece hacer la resolución citada, a todas las normas contenidas en los artículos 14 a 30 de la Constitución.

La aplicabilidad inmediata de las normas iusfundamentales puede predicarse de algunas, como, para el caso, las que crean derechos de libertad, una vez delimitadas según dijimos, pero no posee igual eficacia en el caso de los límites a ellas previstos que, en tanto excepciones a la norma general, deben ser restrictivamente interpretados³⁰.

En el caso del derecho fundamental al secreto de las comunicaciones, el artículo 18.3 CE sólo prevé respecto a su posible limitación una norma competencial: identifica el órgano encargado de restringir el derecho, pero no

²⁹ Cursiva añadida.

³⁰ «[...] la fuerza expansiva de todo derecho fundamental restringe, por su parte, el alcance de las normas limitadoras que actúan sobre el mismo; de ahí la exigencia de que los límites de los derechos fundamentales hayan de ser interpretados con criterios restrictivos y en el sentido más favorable a la eficacia y a la esencia de tales derechos»; *vid.* STC 159/1986, de 16 de diciembre (FJ. 6) y, en igual sentido, STC 254/1988, de 21 de diciembre (FJ. 3). En la doctrina científica cfr., entre otros, BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, *op.cit.*, págs. 312-313 y MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 101. En el mismo sentido, sostiene con acierto JIMÉNEZ CAMPO que «[s]i así no fuera, me parece claro que se relativizarían todas las garantías servidas, en nuestro Estado de Derecho, por la mediación de la ley, comenzando por la exigencia de seguridad jurídica, con la consecuencia inaceptable de que la proclamación del principio de constitucionalidad vendría a entrañar la práctica abolición del principio de legalidad». Cfr. JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 59, nota 24. Existen, no obstante, opiniones doctrinales que defienden la directa aplicabilidad del art. 18.3 CE, «y ello no sólo en lo que concierne a la tutela del derecho que en él se reconoce, sino también a la posibilidad, prevista expresamente en su formulación, de que su ejercicio sea limitado en supuestos concretos por decisión judicial»; RODRÍGUEZ RUIZ, B., «El caso *Valenzuela Contreras* y nuestro sistema de derechos fundamentales», *Revista Española de Derecho Constitucional*, 56, 1999, pág. 229. También en RODRÍGUEZ RUIZ, B., «El coste de los derechos fundamentales...», *op.cit.*, pág. 321.

los supuestos y condiciones en que tal restricción puede ser aplicada. La explícita previsión de la necesidad de resolución judicial en el 18.3 CE debe, por tanto, ser vista como una garantía de segundo grado: en los supuestos en que el legislador posibilite alzar el secreto será el juez quien autorice, pero en estricta sujeción a la norma legal dictada³¹.

El juez, sometido únicamente al imperio de la ley (117.1 CE), no puede crear límites a los derechos fundamentales, sino solo aplicar los previstos por el legislador. Por tanto, la habilitación al juez del 18.3 CE no puede entenderse como un apoderamiento para levantar el secreto incondicionadamente, sino como una habilitación, implícita si se quiere, al legislador para que regule el procedimiento y presupuestos de la limitación. Sólo pues a la ley corresponde el desarrollo y regulación del ejercicio de los derechos fundamentales (arts. 81.1 y 53.1 CE)³².

³¹ JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 58 y BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 126.

³² La exigencia de *interpositio legislatoris* en el caso del 18.3 CE es prácticamente unánime en la doctrina. En este sentido se manifiestan JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, págs. 5 y ss. —también en JIMÉNEZ CAMPO, J., *Derechos fundamentales...*, *op.cit.*, pág. 47—; MARTÍN MORALES, R., *El régimen constitucional...*, *op.cit.*, pág. 101; NOYA FERREIRO, L., «Presupuestos constitucionales de las medidas de intervención de las comunicaciones I», *Dereito. Revista xurídica da Universidade de Santiago de Compostela*, 2, 1999, pág. 166; BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 184; BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, *op.cit.*, *passim*; ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, *op.cit.*, pág. 23; FERNÁNDEZ RODRÍGUEZ, J.J., *Secreto e intervención de las comunicaciones...*, *op.cit.*, pág. 114 y ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 62. También jurisprudencialmente se ha asumido esta posición. Así, la STC 49/1999, de 5 de abril (FJ. 3) dirá: «La literalidad de dicho precepto [18.3 CE] puede inducir a pensar que la única garantía que establece inmediatamente la Constitución, en materia de intervenciones telefónicas, es la exigencia de autorización judicial. Sin embargo, un análisis más detenido de la cuestión pondrá de manifiesto que eso no es así». En el mismo sentido se ha manifestado el Tribunal Supremo: «[...] sólo el Juez, pero no a su libre albedrío, sino siempre de acuerdo con la Ley y conforme a sus principios, es el único que puede acordar una intervención telefónica», ATS, Sala de lo Penal, de 18 de junio de 1992 (FJ. 2). Por su parte, RODRÍGUEZ RUIZ, si bien considera conveniente el establecimiento por ley de los criterios de restricción, no entiende la *interpositio legislatoris* como requisito necesario para la aplicabilidad del límite al secreto de las comunicaciones. Llega a esta conclusión tras considerar que la reserva de ley del art. 53.1 CE y la resolución judicial del 18.3 son «requisitos alternativos y de aplicación independiente». La reserva de ley operaría, según la autora, en supuestos en que la restricción del derecho se lleva a cabo en términos generales; la resolución judicial del 18.3, susceptible a su entender

Por otra parte, la previsión legal del límite es también exigida en el ámbito del Convenio de Roma por el art. 8.2 que, tras declarar el derecho al respeto de la correspondencia en su primer apartado, señala que «[n]o podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley...»³³.

En suma, el inciso final del art. 18.3 debe ser leído en términos similares a los previstos en el segundo apartado del art. 15 de la Constitución italiana: «La limitación [*del secreto de las comunicaciones*] sólo podrá producirse por auto motivado de la autoridad judicial *con las garantías establecidas por la ley*»³⁴.

Más allá de la resolución antes citada, el Tribunal Constitucional ha venido afirmando, con carácter general, la necesaria observancia del principio de legalidad respecto de las medidas limitativas de los derechos fundamentales en general y también, lógicamente, en cuanto a la prevista para el secreto de las comunicaciones³⁵.

de aplicación directa, para la restricción individual del ejercicio del derecho en instancias concretas. Cfr. RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones...*, *op.cit.*, págs. 102 y ss. y RODRÍGUEZ RUIZ, B., «El caso *Valenzuela Contreras...*», *op.cit.*, págs. 231-232.

³³ No obstante, por un lado, el TEDH ha entendido el término ley en su acepción material y no formal, incluyendo, por tanto, la jurisprudencia. Por todas, STEDH de 26 de abril de 1979 (asunto *Sunday Times c. Reino Unido*, §47): «The Court observes that the word “law” in the expression “prescribed by law” covers not only statute but also unwritten law». Por otro lado, para el ordenamiento español anterior a la previsión legal de interceptación de comunicaciones telefónicas (anterior a 1988), consideró que el art. 18.3 CE constituía, a efectos formales, base legal suficiente, pero no —como se dirá— en cuanto a su previsibilidad y calidad. *Vid.* STEDH de 30 de julio de 1998 (asunto *Valenzuela Contreras c. España*, §49).

³⁴ «In base all'art. 15 della Costituzione, lo stesso diritto è inviolabile nel senso che il suo contenuto di valore non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia che la disciplina prevista risponda ai requisiti propri della riserva assoluta di legge e la misura limitativa sia disposta con atto motivato dell'autorità giudiziaria»; Corte Constitucional italiana, Sentenza n. 366 del 1991.

³⁵ Así, se ha afirmado, por ejemplo, que «cualquier restricción en el ejercicio de un derecho fundamental necesita encontrar una causa específica prevista por la ley» (STC 177/1998, de 14 de septiembre; FJ. 3), que «la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental» (STC 292/2000, de 30 de noviembre; FJ. 11), o que «la ausencia de previsión legal de una medida limitativa de un derecho fundamental constituye

En el ámbito específico del derecho que nos ocupa, la importante STC 49/1999, de 5 de abril, afirma:

«[...] por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal. Esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, desempeña una doble función, a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos "únicamente al imperio de la Ley" y no existe, en puridad, la vinculación al precedente (SSTC 8/1981, 34/1995, 47/1995 y 96/1996) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas»³⁶.

Respecto a la primera función señalada, se pretendió ver en el art. 18.3 CE esa necesaria autorización de los representantes para interferir en los derechos fundamentales, si bien en unos términos que consideramos demuestran la nula virtualidad de tal afirmación. Así, se dice que «desde la exigencia de que una norma legal habilite la injerencia, parece difícil negar que la propia Constitución contiene tal habilitación: desde esta perspectiva, *los Jueces y Tribunales pueden, pues, acordarla, cuando concurran los presupuestos materiales pertinentes*»³⁷, a lo que podría añadirse que, no

una lesión autónoma del derecho sustantivo afectado [...] y es condición previa imprescindible de la legitimidad constitucional de las injerencias del poder público en los derechos fundamentales» (STC 169/2001, de 16 de julio; FJ. 3).

³⁶ STC 49/1999, de 5 de abril (FJ. 4). En igual sentido, SSTC 169/2001 de 16 de julio (FJ. 6), y 70/2002, de 3 de abril (FJ. 10).

³⁷ STC 49/1999, de 5 de abril (FJ. 4). *Cursiva añadida.*

precisando la norma esos «presupuestos materiales», no podrán acordarla en ningún caso. Habilitación, si se quiere, pero no bastante.

Con todo, respecto de la exigencia de *interpositio legislatoris* que venimos considerando para la limitación del 18.3, el Tribunal ha diferenciado entre aquellos supuestos en que la ausencia de ley es absoluta y aquellos otros en que, como dijimos, el problema pivota sobre la insuficiencia de la previsión legislativa³⁸.

En esta segunda situación se encontraba el juez instructor en el proceso penal que, si bien disponía de expresa habilitación para la intervención de la correspondencia, no hallaba norma procesal alguna —al menos hasta 1988— sobre la intervención de comunicaciones telefónicas. En atención a la importancia y cantidad de diligencias de este tipo realizadas en ausencia de norma específica, el Tribunal consideró salvada su constitucionalidad integrando la insuficiente habilitación constitucional —aun cuando expresamente mencione las comunicaciones telefónicas— con la necesaria observancia de la aplicación analógica de los requisitos legislativamente previstos para «la detención y apertura de la correspondencia postal y telegráfica»³⁹.

³⁸ Para los registros judiciales de dispositivos de almacenamiento masivo de información llevados a cabo antes de la reforma de la LECrim de 2015, en tanto que limitación de los derechos a la intimidad y/o a la protección de datos personales, el Tribunal Supremo ha considerado que no podía entenderse como una situación de «ausencia absoluta de previsión legal», sino que la ocupación y conservación judicial de los vestigios y pruebas del delito prevista en el art. 326 LECrim, aunque insuficiente, operaba como base legal que, con la observancia de los criterios jurisprudencialmente dispuestos, permitía su aplicación. *Vid.* STS, Sala de lo Penal, de 14 de octubre de 2019 (FJ. 1.3). Sobre la interpretación analógica o extensiva de habilitaciones legales para la práctica de intervenciones corporales, puede verse VIDAL FUEYO, M.C., «Juez y pasividad del legislador. Las intervenciones corporales», *Revista Española de Derecho Constitucional*, 74, 2005, págs. 361-394.

³⁹ «Es cierto que la observación de las telecomunicaciones supone una grave injerencia en la esfera de la intimidad personal (*sic*), constitucionalmente reconocida, y como tal injerencia *ha de estar sometida al principio de legalidad* (STC 150/89, f.j.5), y, en especial, al de proporcionalidad (STC 37/89, ff.jj. 7 y 8), el cual se refiere no solo a la relativa gravedad de la infracción punible para justificar la naturaleza de la medida (SSTEDH, de 6 de septiembre de 1978 y de 2 de agosto de 1984), sino también a las garantías exigibles de autorización judicial específica y razonada y de *respeto en su realización de requisitos similares a los existentes*

La integración analógica o extensiva realizada viene a confirmar la necesaria exigencia de previsión legislativa de los límites para que su posible aplicación por el juez se considere constitucionalmente legítima. Exigencia que se ha visto recientemente ratificada por el Tribunal Constitucional a través de la anulación de una diligencia acordada judicialmente para un supuesto carente de habilitación legislativa⁴⁰.

Por tanto, el juez sólo podrá autorizar la intervención de las comunicaciones en aquellos procesos que el legislador haya previsto, lo que sucede para el caso de nuestro ordenamiento jurídico actualmente vigente en la investigación penal (arts. 579 y ss. y 588 ter.a y ss. LECrim), en la investigación penal militar (arts. 187 y 188 Ley Orgánica 2/1989, de 13 de abril, Procesal Militar) y en el procedimiento concursal (art. 1 Ley Orgánica 8/2003, de 9 de julio, para la Reforma Concursal, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial)⁴¹.

en otro tipo de control de comunicaciones»; cfr. ATC 344/1990, de 1 de octubre. Cursiva añadida.

⁴⁰ Pese a que no compartimos, por las razones señaladas *supra* (Capítulo II, apdo. I.3.A), que la diligencia —grabación de conversaciones directas— incida sobre el derecho fundamental al secreto de las comunicaciones, esta es la *ratio decidendi* en la STC 145/2014, de 22 de septiembre (FJ. 7), donde se afirma lo siguiente: «En el supuesto actual no nos enfrentamos [...] con la posibilidad de suplir sus déficits en los términos descritos, con ocasión del examen de una intervención telefónica judicialmente acordada [...], sino que analizamos una intervención de las comunicaciones absolutamente extraña al ámbito de imputación de dicha regulación. En efecto, no es que la norma no resulte singularmente precisa al fin acordado (calidad de la ley); la objeción reside, antes que en ello, en que abierta e inequívocamente la norma invocada no regula una intervención secreta de las comunicaciones directas en dependencias policiales entre detenidos. Disposición jurídica que es imprescindible, pues sólo con su fundamento puede existir imposición judicial de la medida en el caso concreto [...]. [...] la doctrina elaborada por el Tribunal Constitucional y por la Sala Segunda del Tribunal Supremo sobre la insuficiencia de la regulación legal (en materia de comunicaciones telefónicas) y la posibilidad de suplir los defectos de la ley, no puede ser trasladada a un escenario de injerencia en el secreto de las comunicaciones en el que no exista previsión legal alguna».

⁴¹ Aunque no se desarrolla, en rigor, en el seno de un proceso, también la garantía de resolución judicial se ha acordado para autorizar la intervención de comunicaciones por parte del Centro Nacional de Inteligencia (Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia).

Consideramos así que la aplicación directa y exclusiva de la previsión constitucional, defendida por un sector de la doctrina, no se soporta en nuestro ordenamiento constitucional y, por tanto, debe rechazarse.

B. La «calidad» de la norma limitadora

La reserva de ley no se colma con la mera existencia de la medida limitativa del derecho fundamental, sino que, en atención a los principios de seguridad jurídica e igualdad en la aplicación de las normas, debe satisfacer criterios de previsibilidad y precisión⁴².

Las exigencias de *calidad* de la ley habilitante de la intervención han venido principalmente impulsadas por diversas resoluciones del Tribunal Europeo de Derechos Humanos sobre la intervención de comunicaciones telefónicas en el proceso penal⁴³.

Como dijimos, pese a que a la entrada en vigor de la Constitución la ley procesal penal regulaba solamente la intervención de correspondencia y telegrafía, el Tribunal Constitucional español consideró que no eran contrarias a la Constitución las autorizaciones de intervención de comunicaciones

⁴² Como recuerda la STC 76/2019, de 22 de mayo (FJ. 8), «[s]egún reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas —unas veces— de predeterminación normativa y —otras— de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales». *Vid.* también LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la medida», *Revista de Derecho Político*, 98, 2017, págs. 91-119.

⁴³ Sobre esta cuestión, puede verse CATALÁ I BAS, A., «La problemática adecuación de la legislación española sobre escuchas telefónicas a las exigencias del Convenio Europeo de Derechos Humanos y sus consecuencias», *Revista del Poder Judicial*, 66, 2002, págs. 13-71; MARTÍN-RETORTILLO BAQUER, L., «La calidad de la ley según la jurisprudencia del Tribunal Europeo de Derechos Humanos (Especial referencia a los casos “Valenzuela Contreras” y “Prado Bugallo”, ambos contra España)», *Derecho Privado y Constitución*, 17, 2003, págs. 377-406. CATALÁ I BAS, A., «Escuchas telefónicas: un encuentro con el Tribunal Constitucional y un desencuentro con el legislador español», *Revista Europea de Derechos Fundamentales*, 15, 2010, págs. 279-294 y OCÓN GARCÍA, J., «La incidencia de las resoluciones del TEDH...», *op.cit.*, págs. 259-272.

telefónicas que, atendidas las garantías previstas para la correspondencia, acogieran una rigurosa motivación del juicio de oportunidad y la proporcionalidad de la intervención⁴⁴.

Por su parte, el TEDH había venido declarando, respecto de otros ordenamientos estatales, que la necesaria previsión legislativa de injerencia (art. 8.2 CEDH) debía incluir determinados requisitos de accesibilidad y precisión:

«Se requiere, primero, que la ley sea asequible; el ciudadano debe poder disponer de suficiente información, según las circunstancias, sobre las normas jurídicas aplicables a determinado caso. En segundo lugar, sólo se puede considerar como ley la norma que se expresa con la suficiente precisión para permitir al ciudadano que ajuste su conducta, y que pueda, en su caso con los adecuados asesoramientos, prever razonablemente, según sean las circunstancias, las consecuencias que pueda ocasionar una acción determinada [...]. [...] la ley debe emplear términos lo suficientemente claros para que puedan conocer todos en qué circunstancias y mediante qué requisitos permite el Poder público hacer uso de esta medida secreta y posiblemente peligrosa, que afecta al derecho al respeto a la vida privada y a la correspondencia»⁴⁵.

Esta declaración general fue precisada por el TEDH en los asuntos *Huvig y Kruslin*, donde, al enjuiciar la necesaria previsibilidad de las escuchas telefónicas en el proceso penal francés, señala los siguientes requisitos a

⁴⁴ Así se consideró, para intervenciones telefónicas practicadas antes de 1988, entre otras resoluciones, en el ATC 344/1990, de 1 de octubre y en las SSTC 85/1994, de 14 de marzo (FJ. 3) y 181/1995, de 11 de diciembre (FJ. 5). Esta integración analógica ha sido rechazada, consideramos que acertadamente, por la doctrina, considerando necesaria la aprobación de una regulación íntegra de los supuestos y procedimientos para alzar el secreto de una comunicación telefónica. Cfr. JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, págs. 63-64. También en favor de un riguroso desarrollo de las condiciones de intervención: ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 130.

⁴⁵ STEDH de 2 de agosto de 1984 (asunto *Malone c. Reino Unido*, §§ 67-68). No obstante, y pese a que las resoluciones del Tribunal Constitucional mencionadas en la cita anterior hacen expresa referencia a esta sentencia del Tribunal de Estrasburgo, no se valora en ellas la situación del ordenamiento español a la luz de las exigencias de calidad de la ley.

cumplir por la norma que las permita: determinación de las personas que puedan ser sometidas a esta medida, naturaleza de los delitos sobre cuya investigación pueda recaer, límites de su duración, condiciones para levantar las actas que recojan las conversaciones, precauciones para remitir los registros intactos para su examen por el juez y la defensa y, en fin, circunstancias de borrado y destrucción de las grabaciones⁴⁶.

Estos requisitos podían servir como parámetros de valoración de la regulación nacional sobre intervención de la correspondencia. Los arts. 579 y ss. LECrim sólo exigían indicios de obtener a su través el descubrimiento o comprobación de algún hecho o circunstancia importante de la causa (art. 579 LECrim), la determinación de la correspondencia objeto de intervención en el auto (art. 583), la apertura judicial de la correspondencia (art. 586) y la constancia de lo acaecido durante su práctica (art. 588).

De tal manera que, al enjuiciar la constitucionalidad de una autorización de intervención telefónica fundada en tan exigua base legal, la STC 46/1996, de 26 de marzo (FJ. 5) declara, *obiter dicta*, que, si el TEDH había señalado en los asuntos mencionados que el ordenamiento francés no establecía con suficiente claridad el alcance y los procedimientos para practicar tal intervención, lo mismo podía decirse para el caso de la regulación existente en el proceso penal español⁴⁷.

La confrontación directa de las exigencias del TEDH con la situación del Derecho nacional español sobre intervención de comunicaciones telefónicas

⁴⁶ SSTEDH de 24 de abril de 1990 (asuntos *Huvig y Kruslin c. Francia*, §§ 34 y 35 respectivamente). Se ha criticado que, al establecer con tal grado de precisión las garantías a cumplir por la norma interna para satisfacer el art. 8.2 CEDH, el Tribunal de Estrasburgo viene a sustituir al legislador nacional. Cfr. CATALÁ I BAS, A., «Diálogo entre tribunales y creación de un sistema europeo de derechos humanos abierto en red», *Revista Europea de Derechos Fundamentales*, 28, 2016, pág. 18.

⁴⁷ No obstante, la insuficiencia legal no constituye la *ratio decidendi* de la sentencia para anular el material probatorio obtenido a través de las escuchas, sino que su inconstitucionalidad se sustenta en la divergencia entre la autorización concedida y la intervención practicada —se intervienen las comunicaciones de A aprovechando la prórroga de la autorización de intervención sobre B— y la ausencia de control por parte del Juez en la ejecución de la medida.

anterior a 1988 se plasmó en el conocido asunto *Valenzuela Contreras*. Con el resultado esperado: el TEDH declara que «el Derecho español, escrito y no escrito, no indicaba con suficiente claridad el alcance y las modalidades del ejercicio de las facultades discrecionales de las autoridades en el ámbito considerado»⁴⁸.

Pese a todo, el Tribunal Constitucional español se va a resistir a considerar contraria al 18.3 CE la autorización judicial de intervención de comunicaciones, sobre la base de una regulación declarada manifiestamente deficiente en las exigencias de previsibilidad por la Corte europea.

La STC 49/1999, de 5 de abril, constituye el *leading case* en esta materia. El Tribunal Constitucional confirmará, según dijimos, la necesidad de intervención del legislador en la previsión del límite asumiendo, al tiempo, la jurisprudencia de Estrasburgo en el sentido de considerar la reserva de ley no sólo desde un punto de vista formal, sino también como garantía material que, en atención al principio de seguridad jurídica, implica exigencias respecto al contenido de la ley⁴⁹.

En este sentido, asevera que, «desde las exigencias de certeza que han de presidir cualquier injerencia en un derecho fundamental, es también patente que el art. 18.3 CE, al no hacer referencia alguna a los presupuestos y condiciones de la intervención telefónica, resulta insuficiente para determinar

⁴⁸ STEDH de 30 de julio de 1998 (asunto *Valenzuela Contreras c. España*, §61). En particular, señala que no están previstas ni en el art. 18.3 CE ni en las disposiciones vigentes de la LECrim «la definición de las categorías de personas cuyas líneas telefónicas pueden ser intervenidas por orden judicial; la naturaleza de los delitos que pueden dar lugar a dicha orden judicial; la duración máxima de la ejecución de la medida; el procedimiento de transcripción resumida de las conversaciones interceptadas, así como el uso y la destrucción de las grabaciones realizadas» (§59). Sobre esta sentencia, puede verse RODRÍGUEZ RUIZ, B., «El caso *Valenzuela Contreras...*», *op.cit.*, págs. 223-250 y SÁNCHEZ YLLERA, I., «*Valenzuela Contreras c. España* (STEDH de 30 de julio de 1998): La deficiente calidad de las normas que habilitan la intervención de las comunicaciones telefónicas», ALCÁCER GUIRAO, R., BELADIEZ ROJO, M. y SÁNCHEZ TOMÁS, J.M., *Conflicto y diálogo con Europa. Las condenas a España del Tribunal Europeo de Derechos Humanos*, Madrid, Civitas, 2013, págs. 443-470.

⁴⁹ «[E]s necesaria la intervención de la ley y la norma legal de que se trate ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica» (FJ. 5).

si la decisión judicial es o no el fruto previsible de la razonable aplicación de lo decidido por el legislador» (FJ. 4) y que, por tanto, «la situación del Ordenamiento jurídico español [anterior a 1988] ha de estimarse contraria a lo dispuesto en el art. 18.3 CE» (FJ. 5).

Sin embargo, al ponderar las consecuencias de tal afirmación, el Tribunal diferencia entre el *peligro* del actuar arbitrario que la ausencia de precisión legislativa puede conllevar y el hecho de que el juez, efectivamente, haya actuado arbitrariamente.

Así, pese a afirmar que «estamos en presencia de una vulneración del art. 18.3 CE, autónoma e independiente de cualquier otra: la insuficiencia de la ley, que sólo el legislador puede remediar y que constituye, por sí sola, una vulneración del derecho fundamental», permite salvar la legitimidad constitucional de la autorización de intervención si el juez hubiera actuado *como si* existiera una ley que precisara los supuestos y condiciones de intervención:

«En efecto: si, pese a la inexistencia de una ley que satisficiera las genéricas exigencias constitucionales de seguridad jurídica, los órganos judiciales, a los que el art. 18.3 de la Constitución se remite, hubieran actuado en el marco de la investigación de una infracción grave, para la que de modo patente hubiera sido necesaria, adecuada y proporcionada la intervención telefónica y la hubiesen acordado respecto de personas presuntamente implicadas en el mismo, respetando, además, las exigencias constitucionales dimanantes del principio de proporcionalidad, no cabría entender que el Juez hubiese vulnerado, por la sola ausencia de dicha ley, el derecho al secreto de las comunicaciones telefónicas».

Nos hallamos ante una forma de razonamiento ciertamente llamativo que sólo se explica, según creemos, en la necesidad de asumir la jurisprudencia del TEDH y, a su vez, en la intención de salvaguardar una diligencia ampliamente utilizada en la investigación de delitos que, de otro modo, hubiera

dado pie a multitud de procedimientos dirigidos a la anulación de procesos penales⁵⁰.

Pues si, como la propia sentencia afirma, la previsibilidad legal de la medida es exigencia del principio de seguridad jurídica e implica que el ciudadano conozca «cuál ha de ser la actuación del poder en aplicación del Derecho» (FJ. 4), mal puede compadecer esa expectativa razonable del ciudadano con un razonamiento judicial solo conocido una vez el secreto ha sido ya excepcionado⁵¹.

Hasta ahora hemos analizado los pronunciamientos jurisprudenciales relativos a la situación del ordenamiento jurídico español anterior a 1988, carente por tanto de regulación específica de las condiciones de intervención de comunicaciones telefónicas en el proceso penal.

Sin embargo, la actividad legislativa que vino a colmar el vacío no mejoró en gran medida la regulación existente desde el punto de vista de las exigencias de calidad de la ley indicadas por el Tribunal de Estrasburgo.

La Ley Orgánica 4/1988, de 25 de mayo, introdujo la diligencia de intervención de comunicaciones telefónicas en los apartados 2 y 3 del art. 579 LECrim:

«2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

⁵⁰ *Vid. infra*, nota 57.

⁵¹ En similar sentido se expresa el Voto Particular que el magistrado Cruz Villalón emite a la sentencia que venimos considerando: «no comparto la idea de una especie de vulneración calificada de "autónoma e independiente de cualquier otra" del derecho fundamental determinada por las carencias en la calidad de la ley que, sin embargo, pueden ser, por así decir, posteriormente "neutralizadas" por medio de una actuación judicial particularmente respetuosa del derecho fundamental en cuestión (fundamento jurídico 5º). [...] no creo que podamos decir que se ha vulnerado el derecho fundamental por la deficiencia de la ley y, sin embargo, afirmar que la lesión puede ser contrarrestada por el juez, pues las carencias de previsibilidad no son susceptibles de una subsanación *ex post facto*».

3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos».

Pero pese al avance que la reforma supuso respecto de la anterior situación, los pronunciamientos del TEDH en los asuntos *Huvig y Kruslin*, dictados solo dos años después de su entrada en vigor, pusieron en evidencia sus carencias: no establecía los delitos para cuya investigación podía activarse esta diligencia, ni su duración máxima, ni las condiciones de utilización, conservación y destrucción de las grabaciones⁵².

Conocedor de tal situación, el Tribunal Supremo trató de integrar jurisprudencialmente los requisitos exigidos por el TEDH. Puesta de manifiesto la imperfección de la reforma por la Sentencia de la Sala de lo Penal de 21 de febrero de 1991 (FJ. 4), será el Auto, de la misma Sala, de 18 de junio de 1992 (en el conocido como asunto *Naseiro*) el que señale que «dada la citada y grave insuficiencia de la regulación actualmente vigente, es obligado llevar a cabo una especie de construcción por vía jurisprudencial de la forma correcta de realización de tal medida [...]», procediendo a establecer, con apoyo en la doctrina del TEDH, las garantías que debían presidir las intervenciones telefónicas —*v.gr.* establecerla solo en caso de delitos graves, control judicial periódico de la medida, entrega de fuentes originales, modo de aplicación de la medida, límites, etc. (FJ. 11)—⁵³.

⁵² Puede hallarse un buen acopio de opiniones doctrinales poniendo de manifiesto las carencias de la nueva norma respecto de las exigencias del TEDH en CATALÁ I BAS, A., «La problemática adecuación...», *op.cit.*, págs. 62 y ss.

⁵³ En similar sentido, la STS, Sala de lo Penal, de 7 de noviembre de 1997 (FJ. 3), dirá sobre la reforma de la LECrim: «Destaca la escasez normativa, tan puesta de manifiesto por autores y jurisprudencia, tanto más lamentable cuanto nos hallamos ante la limitación de un derecho fundamental y ante una fuente de medios probatorios tan presente y operativa en la ordinaria investigación desarrollada en medios judiciales y policiales. Ante una regulación tachada de incompleta, asistemática e insuficiente, puede decirse que ha sido la jurisprudencia la que ha ido creando en torno a ella todo un cuerpo doctrinal del mejor cuño, contando en base a ello con un régimen jurídico parangonable a ordenamientos europeos caracterizados por velar,

La nueva situación fue objeto de examen del TEDH en Sentencia de 18 de febrero de 2003 (asunto *Prado Bugallo c. España*). Y, pese a considerar que la reforma suponía un «progreso innegable», las modificaciones introducidas seguían siendo insuficientes para responder a las garantías exigidas⁵⁴.

En la decena de resoluciones que siguen a la STC 49/1999, aun cuando todas enjuician intervenciones telefónicas dictadas al amparo del reformado 579 LECrim, el Tribunal Constitucional ni siquiera entra a valorar la nueva redacción, y ello pese a que su insuficiencia había venido siendo reseñada por la jurisprudencia ordinaria desde su entrada en vigor⁵⁵. Aplicará sin solución de continuidad su doctrina en los términos allí establecidos: las insuficiencias legislativas pueden ser salvadas en atención al buen hacer judicial, y ello pese a reiterar constantemente en su jurisprudencia posterior que «la intervención de las comunicaciones telefónicas sólo puede entenderse

con la mayor sensibilidad y estilo democrático, por el respeto y sobrevivencia de los derechos fundamentales».

⁵⁴ El TEDH admite (§§ 31 y 32) que las deficiencias de la norma habían sido ya paliadas en parte por la jurisprudencia española, pero con posterioridad a la fecha de los hechos enjuiciados (la intervención se había producido entre septiembre de 1990 y enero de 1991), por lo que dichas resoluciones no podían ser tenidas en cuenta en el caso *a quo*. Puede encontrarse un comentario a esta resolución en CATALÁ I BAS, A., «Sentencia del Tribunal Europeo de Derechos Humanos Prado Bugallo c. España de 18 de febrero de 2003», *Revista Europea de Derechos Fundamentales*, 1, 2003, págs. 127-135.

⁵⁵ Solo la STC 166/1999, de 27 de septiembre (FJ. 3) parece asemejar tímidamente la nueva regulación a las exigencias del Tribunal europeo cuando señala que «[e]stos presupuestos, fijados en el art. 597.2 y 3 LECrim y coincidentes con la jurisprudencia del TEDH (reiterada en el caso Valenzuela contra España, Sentencia del TEDH de 30 de julio de 1998, §46 y ss.), residen en la existencia de una investigación en curso por un hecho constitutivo de infracción punible grave, en atención al bien jurídico protegido y a la relevancia social del mismo, y en la existencia de indicios sobre el hecho constitutivo de delito y sobre la conexión con el mismo de las personas investigadas». En todo caso, si bien todas las garantías de la nueva ley estaban presentes en la jurisprudencia del TEDH, no todas las requeridas por éste se habían visto colmadas con ocasión de la reforma. Por otro lado, los recurrentes del procedimiento de amparo que dio lugar a la STC 33/2003, de 13 de febrero, imputan a la nueva regulación diversas deficiencias, pero declarado vulnerado el derecho de defensa por defectos en el principio acusatorio, el Tribunal Constitucional considera innecesario analizar el resto de las vulneraciones alegadas y no entra, por tanto, a valorar el nuevo escenario legislativo.

constitucionalmente legítima si está legalmente prevista con suficiente precisión»⁵⁶.

La respuesta sólo llegará, al igual que entonces, frente a la interpelación directa del TEDH. Unos meses después de la Sentencia *Prado Bugallo*, y quince años después de la reforma de la LECrim, la STC 184/2003, de 23 de octubre, afrontará por primera vez de forma explícita el examen de las exigencias de calidad de la nueva regulación.

El Tribunal Constitucional confirma lo que ya había sido puesto de manifiesto por el Tribunal Supremo y el TEDH: «el art. 579 LECrim no es por sí mismo norma de cobertura adecuada, atendiendo a las garantías de certeza y seguridad jurídica, para la restricción del derecho fundamental al secreto de las comunicaciones telefónicas (art. 18.3 CE)» (FJ. 5). Sin embargo, no ve obstáculos para mantener su doctrina sobre la sanación judicial de los defectos legislativos.

Siendo unánimes las opiniones en la doctrina científica y jurisprudencial respecto de la insuficiencia de la ley, los recurrentes solicitan al Tribunal el planteamiento de la cuestión interna de inconstitucionalidad sobre el art. 579 LECrim, petición que es rechazada en los siguientes términos:

«[...] la existencia de una situación que no se ajusta a las exigencias de previsibilidad y certeza en el ámbito del derecho fundamental al secreto de las comunicaciones que reconoce el art. 18.3 CE, que, sin embargo, no se resolvería adecuadamente a través del planteamiento de la cuestión de inconstitucionalidad sobre el art. 579 LECrim. [*Pues dicho mecanismo*] está previsto para actuar sobre disposiciones legales que en su contenido contradicen la Constitución, pero no respecto de las que se avienen con aquélla y cuya inconstitucionalidad deriva no de su enunciado, sino de lo que en éste se silencia, deficiencias que pueden predicarse del art. 579 LECrim sin otro precepto que lo complementa, que no existe en nuestro ordenamiento jurídico.

⁵⁶ SSTC 171/1999, de 27 de septiembre (FJ. 5); 126/2000, de 16 de mayo (FJ. 2); 14/2001, de 29 de enero (FJ. 2); 138/2001, de 18 de junio (FJ. 3); 202/2001, de 15 de octubre (FJ. 2); y 82/2002, de 22 de abril (FJ. 3).

En estos casos, [...] el planteamiento de la cuestión de inconstitucionalidad resulta inútil, en la medida en que la reparación de la eventual inconstitucionalidad solo podría alcanzarse supliendo las insuficiencias de las que trae causa y no mediante la declaración de inconstitucionalidad y, en su caso, nulidad de un precepto que no es contrario a la Constitución por lo que dice, sino por lo que deja de decir».

Además, el Tribunal hace explícito en esta sentencia lo que hasta el momento eran meras conjeturas: su doctrina de integrar jurisprudencialmente las insuficiencias de la ley —y el rechazo ahora del planteamiento de la cuestión de inconstitucionalidad— tiene como objetivo seguir disponiendo de esta diligencia como herramienta ciertamente eficaz para la investigación penal⁵⁷.

Descartada la vulneración por mera deficiencia de la ley, la jurisprudencia del Tribunal Constitucional sobre las vulneraciones del art. 18.3 CE alegadas en amparo se centra, a partir de este momento, en analizar la existencia del supuesto habilitante de la intervención, la observancia del principio de proporcionalidad en la decisión de autorizarla, la existencia de motivación suficiente y el correcto control de la práctica de la medida⁵⁸.

Sólo la STC 26/2006, de 30 de enero, volverá, en respuesta a la impugnación realizada por los recurrentes, sobre la deficiente calidad de la norma habilitante. En este caso, producida la intervención de las

⁵⁷ «El ejercicio por este Tribunal de su tarea depuradora de normas contrarias a la Constitución culminaría, en su caso, con una declaración de inconstitucionalidad por defecto de la disposición legal —art. 579 LECrim— que agravaría el defecto mismo —la falta de certeza y seguridad jurídicas— al producir un vacío mayor. *Los intereses constitucionalmente relevantes que con el art. 579.3 LECrim se tutelan se verían absolutamente desprotegidos por cuanto aquella declaración podría comportar, cuando menos, la obligación de los poderes públicos de inaplicar la norma viciada de inconstitucionalidad*»; STC 184/2003, de 23 de octubre (FJ. 7).

⁵⁸ SSTC 165/2005, de 20 de junio; 205/2005, de 18 de julio; 259 y 261/2005, de 24 de octubre; 26/2006, de 30 de enero; 104/2006, de 3 de abril; 136 y 146/2006, de 8 de mayo; 150/2006, de 22 de mayo; 219 y 220/2006, de 3 de julio; 239/2006, de 17 de julio; 253/2006, de 11 de septiembre; 148/2009, de 15 de junio; 197/2009, de 28 de septiembre; 219 y 220/2009, de 21 de diciembre; 5/2010, de 7 de abril; 26/2010, de 27 de abril; 68 y 72/2010, de 18 de octubre; 87/2010, de 3 de noviembre; 9/2011, de 28 de febrero; y 25/2011, de 14 de marzo.

comunicaciones en el año 2000, el Tribunal considera que la tacha de vaguedad e indeterminación de la regulación debía ser matizada puesto que, al ser la limitación posterior a la jurisprudencia del Tribunal Supremo en el asunto *Naseiro* y a la STC 49/1999, «[n]o puede afirmarse, en el momento actual, que el Derecho interno no respete las exigencias derivadas del art. 8 CEDH»⁵⁹.

Ahora bien, conviene subrayar que, aun cuando esta solución pudiera ser válida en el ámbito del CEDH —donde la previsión legal requerida es considerada en su acepción material⁶⁰—, no puede serlo internamente, ya que el problema de la insuficiencia de la ley, formalmente exigida (art. 53.1 CE), debía ser necesariamente resuelto por el legislador⁶¹.

No obstante, superado el riesgo de exposición a nuevas condenas por parte del TEDH, tardará todavía mucho tiempo en afrontar la solución⁶², a pesar de que el desarrollo de nuevas formas de comunicación y, sobre todo, la generalización de su uso —con la consecuente necesidad del recurso a su

⁵⁹ STC 26/2006, de 30 de enero (FJ. 5).

⁶⁰ En la Decisión de 26 de septiembre de 2006 (asunto *Abdulkadir Coban c. España*) el TEDH inadmite la demanda precisamente por entender que la insuficiencia normativa motivo de anteriores condenas había sido paliada mediante la incorporación, vía doctrina jurisprudencial, de las condiciones exigidas para que la «ley» fuere lo suficientemente clara y precisa. Solución nuevamente confirmada por la Decisión de inadmisión de 7 de septiembre de 2010 (asunto *Fernández Saavedra c. España*).

⁶¹ Así, el Tribunal Constitucional en Sentencia 184/2003, de 23 de octubre (FJ. 7), recuerda que «[e]s al legislador a quien corresponde, en uso de su libertad de configuración normativa propia de su potestad legislativa, remediar la situación completando el precepto legal. [...] siendo función de la tarea legislativa de las Cortes ponerle término en el plazo más breve posible». Incluso el TEDH en *Abdulkadir Coban* considera que «es deseable una modificación legislativa incorporando a la Ley los principios que se desprenden de la jurisprudencia del Tribunal».

⁶² Como acertadamente afirma CATALÁ I BAS, «producido el diálogo judicial en cuestión sin la posterior modificación legislativa, el TEDH considera zanjado el problema, aunque se haya cerrado en falso a nivel interno, pues la carencia o insuficiencia de la norma sigue existiendo, con lo cual la sentencia del TEDH provoca el efecto pernicioso de paralizar o ralentizar reformas internas que mejorarían la calidad de la norma estatal», cfr. CATALÁ I BAS, A., «Diálogo entre tribunales...», *op.cit.*, pág. 29. También se ha señalado que la jurisprudencia del TEDH puede servir para espolear a los legisladores nacionales en MARTÍN-RETORTILLO BAQUER, L., «La calidad de la ley...», *op.cit.*, *passim*.

intervención para la investigación penal— continuó creciendo exponencialmente.

La posibilidad de intervenir comunicaciones telemáticas se encontraba, así, en la misma situación en que hasta 1988 habían estado las telefónicas. E igual fue también la solución, consistente en la integración analógica de los requisitos previstos para otros tipos de comunicaciones:

«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 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»⁶³.

Una solución llegó finalmente con la aprobación —diecisiete años después de la primera condena del TEDH a España— de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

La reforma incorpora al articulado de la LECrim, como expresamente reconoce su Preámbulo, los criterios que jurisprudencialmente habían sido señalados como de necesaria observancia y, efectivamente, resultan

⁶³ STS, Sala de lo Penal, de 26 de noviembre de 2014 (FJ. 8). Sobre la asimilación de la práctica de intervención de correos electrónicos respecto a las comunicaciones telefónicas, *vid.* SSTS, Sala de lo Penal, de 14 de noviembre de 2013 (FJ. 4), y 22 de diciembre de 2014 (FJ. 2). Por su parte, el Tribunal Constitucional no ha tenido ocasión de pronunciarse sobre la insuficiente cobertura de la ley procesal para el caso de la intervención de comunicaciones telemáticas, ya que en los asuntos en que la injerencia se había producido sobre este tipo de comunicaciones (SSTC 241/2012, de 17 de diciembre —intercambio de mensajería instantánea a través de *chat*—; 170/2013, de 7 de octubre, y 26/2018, de 5 de marzo—correo electrónico—), la misma había sido ocasionada por la intervención de un particular.

perfectamente reconocibles todas y cada una de las garantías que el TEDH había considerado que debían estar presentes en la ley para entenderla conforme al Convenio en términos de previsibilidad y precisión⁶⁴.

Finalmente, cabe decir que los defectos de rigor en la ordenación de la intervención de comunicaciones no son patrimonio exclusivo de la ley procesal penal.

El escaso desarrollo de los presupuestos y condiciones en que puede ser judicialmente alzado el secreto es también predicable de la regulación contenida en la Ley Orgánica 2/1989, de 13 de abril, Procesal Militar (arts. 187 y 188) y en la Ley Orgánica 8/2003, de 9 de julio, para la Reforma Concursal (art. 1).

Con todo, la incidencia de la insuficiencia legislativa es en estos casos menor, pues se ha visto en cierto modo corregida con la reforma de la LECrim a que ambas se remiten: *in totum* en el caso de la primera (Disposición Adicional Primera de la Ley Procesal Militar) y específicamente para la intervención de las comunicaciones telefónicas en el proceso concursal (art. 1.4 de la Ley de Reforma Concursal)⁶⁵.

No obstante, si bien la reforma de la LECrim en 2015 pone fin a los problemas en el momento actual, no puede ser en ningún caso considerada como una solución definitiva de futuro.

Las exigencias de calidad de la ley en el ámbito que venimos considerando van a exigir la constante evaluación y actualización de la norma. El desarrollo de los sistemas de comunicación continuará avanzando —lo

⁶⁴ Así, entre otras cuestiones, regula las personas susceptibles de ser sometidas a la medida (588 ter.b y c); los delitos para cuya investigación se puede acordar (588 ter.a); la duración (588 bis.e y 588 ter.g); el control judicial de la medida (588 ter.f); el acceso de las partes a las grabaciones (588 ter.i) o la destrucción de los registros (588 bis.k).

⁶⁵ Sobre la previsión legislativa de la intervención de comunicaciones por parte del CNI, *vid.* SÁNCHEZ BARRILAO, J.F., «Servicios de inteligencia, secreto y garantía judicial de los derechos», *Teoría y Realidad Constitucional*, 44, 2019, págs. 309-339.

sigue haciendo— y requerirá adaptar la normativa a fin de habilitar una intervención legítima y previsible por parte de los poderes públicos.

Por ello, frente a lo que pudiera parecer, no hemos atendido en este epígrafe a un problema pasado con el único objetivo de realizar un acta de daños meramente testimonial, sino para destacar los errores a evitar y deducir las soluciones a las que pudiera tener que recurrirse en el futuro.

A estos efectos, la estricta previsión legal de los límites es exigencia de seguridad jurídica y garantía de los derechos fundamentales del procesado. Pero, al mismo tiempo, la posibilidad de intervenir comunicaciones es, cada vez más, una herramienta a menudo indispensable para el efectivo desarrollo de la investigación penal, bien constitucionalmente protegido de gran relevancia.

El necesario equilibrio que debe encontrarse entre estos bienes jurídicos se ve determinado por los diferentes ritmos seguidos por el desarrollo tecnológico y el normativo. Pero la habitual dilación del legislador no puede inclinar la balanza en perjuicio de las garantías. El caso analizado sirve de ejemplo de lo que no debería repetirse: 25 años median entre los primeros reproches en pronunciamientos del TEDH estableciendo los criterios legislativos de calidad de la norma habilitante y la efectiva intervención del legislador español despejándolos.

El derecho comparado puede ofrecernos algunas soluciones. Tal vez sería útil el recurso a la conocida como doctrina del periodo transitorio utilizada por el Tribunal Constitucional alemán. Ante situaciones de insuficiencias o deficientes regulaciones de medidas restrictivas de derechos fundamentales que, sin embargo, son esenciales para el desempeño de las tareas encomendadas al Estado —como esta de la intervención de las comunicaciones en la investigación penal—, el TCF ha optado por instar al legislador a reparar dicha situación, estableciendo en ocasiones un plazo

determinado⁶⁶. Durante ese periodo transitorio se permite recurrir excepcionalmente a la medida, siempre que, en atención a las circunstancias del caso concreto, «resulte indispensable para el mantenimiento de la actividad con capacidad funcional»⁶⁷.

La implantación de este mecanismo en nuestro sistema de control de constitucionalidad requeriría de la actuación del legislador orgánico, pues la actual redacción del art. 39 LOTC conecta indefectiblemente declaración de inconstitucionalidad y nulidad de los preceptos de tal modo calificados.

Sin embargo, el mecanismo no es completamente desconocido, ni para el prelegislador español ni para el Tribunal Constitucional.

Así, por un lado, el proyecto legislativo que culminaría con la reforma de la Ley del Tribunal en el año 2007 incluía determinadas previsiones en este sentido.

El artículo 39 del Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional, preveía la posibilidad de, declarada la inconstitucionalidad de un precepto, diferir los efectos de su nulidad hasta un plazo máximo de tres años cuando, según rezaba la Exposición de Motivos, «expresamente se justifique la concurrencia

⁶⁶ Así, por ejemplo, respecto de diligencia de colocación de micrófonos para la captación de conversaciones orales, la *BVerfGE* 109, 279, de 3 de marzo de 2004, dispone: «En la medida en que las disposiciones impugnadas del Código de Procedimiento Penal son incompatibles con la Ley Fundamental, el legislador está obligado a establecer un estatus legal constitucional a más tardar el 30 de junio de 2005. Hasta esta fecha, las normas impugnadas pueden seguir aplicándose, teniendo en cuenta la protección de la dignidad humana y el principio de proporcionalidad».

⁶⁷ «Tal defecto generalmente tiene la consecuencia de que la medida impugnada debe ser anulada como inconstitucional. Por el contrario, es más consistente la opinión del Tribunal Administrativo Superior y el Tribunal Administrativo Federal de aceptar la escapatoria por un período de transición para dar al legislador la oportunidad de establecer la regulación legal [...]. El reconocimiento básico de esta necesidad no significa, sin embargo, que dentro del período de transición la regulación anterior seguiría siendo aplicable como si fuera constitucionalmente inobjetable. Hasta que el legislador establezca el estado constitucional, los poderes de las autoridades y los tribunales para intervenir en ámbitos protegidos por el derecho constitucional se reducen a lo que es esencial en el caso específico». *BVerfGE* 41, 251, de 27 de enero de 1976. *Vid.* ETXEBERRÍA GURIDI, J.F., «La previsión legal y las diligencias de investigación restrictivas de derechos fundamentales (A propósito de la STC 49/1999 de 5 de abril)», *Diario La Ley*, 4215, 1999, págs. 16 y ss.

de algún interés constitucional que resulte protegido por la adopción de este efecto extraordinario». Y se señalaba como causa explícita para ese modo de proceder la necesaria actuación del legislador cuando la inconstitucionalidad hubiere estado motivada por la insuficiencia de la ley:

«3. Cuando la sentencia declare la inconstitucionalidad por insuficiencia normativa podrá conceder un plazo al legislador para que actúe en consecuencia. Si este incumpliera dicho mandato, el Tribunal Constitucional resolverá lo que proceda para subsanar la insuficiencia»⁶⁸.

En cualquier caso, esta propuesta de reforma decayó ya en el Informe de la Ponencia.

Por otro lado, y pese al tenor literal del art. 39.1 LOTC⁶⁹, el Tribunal Constitucional ha atemperado en diversos pronunciamientos la inescindible vinculación que la ley realiza entre inconstitucionalidad y nulidad⁷⁰.

La mera declaración de inconstitucionalidad ha sido utilizada en aquellos casos en que los efectos de la nulidad son técnicamente inadecuados o ineficaces: casos de carencias en la regulación o, más en general, cuando los efectos de la nulidad empeoren la situación tachada de inconstitucional⁷¹.

⁶⁸ Art. 39.3 del Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional (BOCG, Congreso de los Diputados, núm. 60-1, de 25 de noviembre de 2005).

⁶⁹ «Cuando la sentencia declare la inconstitucionalidad, declarará igualmente la nulidad de los preceptos impugnados, así como, en su caso, la de aquellos otros de la misma Ley, disposición o acto con fuerza de Ley a los que deba extenderse por conexión o consecuencia»

⁷⁰ Vid. PUNSET BLANCO, R., «Las sentencias declaratorias de la inconstitucionalidad de las leyes: consideraciones sobre la posible reforma de los artículos 39.1 y 40.1 de la LOTC», *Anuario de Derecho Constitucional y Parlamentario*, 7, 1995, págs. 33-48; GÓMEZ MONTORO, Á.J., «Artículo 39», REQUEJO PAGÉS, J.L. (Coord.), *Comentarios a la Ley Orgánica del Tribunal Constitucional*, Tribunal Constitucional – Boletín Oficial del Estado, Madrid, 2001, págs. 578-608; y MAS BADÍA, M.D., «El alcance temporal de la declaración de inconstitucionalidad de las leyes civiles. Especial referencia a las valencianas», *Derecho Privado y Constitución*, 31, 2017, págs. 317-386.

⁷¹ JIMÉNEZ CAMPO, J., «Qué hacer con la ley inconstitucional», AA.VV., *La sentencia sobre la constitucionalidad de la Ley. Actas de las II Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Tribunal Constitucional – Centro de Estudios Constitucionales, Madrid, 1997, pág. 53. Vid., entre otras, SSTC 45/1989, de 20 de febrero (FJ. 11), 222/1992, de 11 de diciembre (FJ. 7), 96/1996, de 30 de mayo (FJ. 23), 235/1999, de 20 de diciembre (FJ. 13), 138/2005, de 26 de mayo (FJ. 6), y 273/2005, de 27 de octubre (FJ. 9). En algunos

C. Fundamentos de la limitación

Hemos visto que la posibilidad constitucionalmente admisible de limitar por resolución judicial el ejercicio del derecho fundamental al secreto de las comunicaciones debe encontrar previsión específica en una habilitación legal, cierta y precisa.

Queda, sin embargo, por determinar si el legislador opera con total libertad para prever la intervención de las comunicaciones o si, por el contrario, tal previsión debe necesariamente encontrar fundamento en lo dispuesto por la Constitución.

El Tribunal Constitucional se ha pronunciado expresamente en favor de los escenarios que hemos denominado de delimitación indirecta, esto es, en los casos en que la Constitución no establece explícitamente ninguna contención al objeto o contenido del derecho fundamental declarado. En estos supuestos, según dijimos, los demás derechos fundamentales y bienes constitucionalmente protegidos operan como criterios de delimitación del derecho y, por tanto, en caso de que tal delimitación se lleve a cabo por el legislador, su actividad deberá orientarse necesariamente a su protección⁷².

Respecto del fundamento a que debe atender la previsión legal de los límites en sentido estricto encontramos opiniones diversas en la doctrina.

casos el Tribunal Constitucional ha diferido los efectos de la nulidad hasta el momento en que se llevase a cabo la actuación legislativa necesaria —SSTC 195/1998, de 1 de octubre (FJ. 5), 208/1999, de 11 de noviembre (FJ. 8), y 151/2017, de 21 de diciembre (FJ. 8)— e incluso estableciendo un plazo concreto para subsanar los defectos que motivaron la declaración de nulidad — SSTC 164/2013, de 26 de septiembre (FJ. 7); 164/2014, de 7 de octubre (FJ. 3); y 13/2015, de 5 de febrero (FJ. 5)—. En este sentido, *vid.* PONS PORTELLA, M., «La nulidad diferida de las leyes en caso de omisión de informes autonómicos preceptivos», *Anales de la Facultad de Derecho*, 35, 2018, págs. 29-45.

⁷² En estos términos se expresa la STC 292/2000. Tras recordar que la Constitución no impone límites expresos al derecho fundamental a la protección de datos y que, por tanto, solo en su coexistencia con otros derechos y bienes jurídicos de rango constitucional pueden hallarse criterios para su delimitación, dispone que el apoderamiento legal para llevar a cabo dicha tarea «sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos». STC 292/2000, de 30 de noviembre (FJ. 11).

Por un lado, algunos autores consideran que, cuando la Constitución simplemente habilita al poder legislativo para restringir un derecho —ya sea directamente, ya de modo implícito mediante la habilitación al juez, como ocurre en el caso del 18.3—, su tarea debe ajustarse a la protección proporcionada de otros concretos bienes o valores constitucionales⁷³.

Por otro lado, para VILLAVERDE MENÉNDEZ debe reconocérsele al legislador en el caso de los límites externos un margen de maniobra mayor que cuando se ocupa simplemente de delimitar, pues la propia Constitución ha querido, mediante la expresa habilitación al poder público, que sea éste quien decida «qué bienes o intereses jurídicos se erigirán en restricción de un derecho fundamental»⁷⁴.

No obstante, la libertad de configuración que pudiera tener el legislador se ha visto, para el caso de los límites a los derechos fundamentales, mediatizada por la influencia del CEDH. Pues, al recoger la posibilidad expresa de introducir restricciones a alguno de los derechos que declara (arts. 8 a 11), hace explícitas también las finalidades u objetivos a que tal restricción debe necesariamente orientarse.

Para el caso que aquí nos interesa, el art. 8.2 CEDH dispone que los límites que pudieran preverse legalmente deben ser necesarios para la consecución de alguno de los siguientes objetivos: «la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, la protección de los derechos y las libertades de los demás».

⁷³ BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, *op.cit.*, págs. 303-304 y RODRÍGUEZ RUIZ, B., «El coste de los derechos fundamentales...», *op.cit.*, págs. 320-321. No obstante, el primero matiza su afirmación al añadir que «la previsión constitucional de la necesaria intervención judicial para la actualización de esos límites en el caso concreto constituye en sí misma una garantía, que puede hacer lícitos límites que de otro modo no lo serían». Por lo demás esta es la solución prevista expresamente en la Constitución portuguesa, cuyo art. 18.2 limita las restricciones a los derechos fundamentales a «las necesarias para salvaguardar otros derechos e intereses protegidos por la Constitución».

⁷⁴ BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, págs. 130-132.

Una lista ciertamente extensa que, tanto por el número de finalidades a las que permite orientar la legislación como por la amplitud de los términos en que se expresan, permite hallar justificación para un variadísimo elenco de restricciones.

Con todo, en las previsiones legislativas establecidas hasta el momento en nuestro ordenamiento para la intervención de las comunicaciones, es posible identificar nítidamente un fundamento tanto en derechos, bienes y valores constitucionalmente protegidos, como en alguno de los objetivos previstos en el CEDH.

La posibilidad de intervenir comunicaciones en el proceso penal se orienta a la persecución y castigo del delito, finalidad expresamente prevista en el CEDH (seguridad pública) y sobre la que el Tribunal Constitución ha dicho que constituye «un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana»⁷⁵.

Lo mismo puede decirse, para el ámbito de su propia jurisdicción, de la previsión de intervención de comunicaciones en el proceso penal militar.

Tampoco plantea mayores problemas la identificación de un fundamento respetuoso con el Convenio en el resto de los casos: la posibilidad de levantar el secreto por los servicios de inteligencia responde a la seguridad nacional y a la prevención de la comisión de delitos. Por su parte, intervenir las comunicaciones del concursado tiene como finalidad, según expresamente dispone la norma en su Exposición de Motivos, asegurar la normal tramitación del procedimiento. En tanto que su objeto es satisfacer las deudas de los acreedores, al tiempo que tratar de garantizar la subsistencia de la empresa, el fundamento de la previsión legal del límite debe identificarse con la protección de los derechos de los demás y con el bienestar económico del país.

⁷⁵ STC 292/2000, de 30 de noviembre (FJ. 9). En el mismo sentido, SSTC 49/1999, de 5 de abril (FJ. 8), y STC 198/2003, de 10 de noviembre (FJ. 7).

D. Los límites a la actividad limitadora del legislador

D.1. El contenido esencial como límite de los límites

Más allá del objetivo al que se dirija la previsión legislativa del límite, el legislador en esta tarea está condicionado por otros enunciados constitucionales. Este es el caso del artículo 53.1 CE, que exige del legislador de los derechos fundamentales el respeto a su «contenido esencial»⁷⁶.

En nuestro caso el contenido esencial del derecho fundamental al secreto de las comunicaciones se identifica con la garantía judicial prevista constitucionalmente. El legislador no podrá en ningún caso prescindir, en la normación del límite, de la fiscalización judicial del alzamiento del secreto.

Pero, además, consideramos que integra también el contenido esencial del art. 18.3 CE que su posible limitación se prevea solamente para aquellos casos en que tal medida pueda servir razonablemente a la consecución de un fin legítimo y en que su aplicación se produzca en términos restrictivos.

Esto es, si el derecho consiste en la prohibición de levantar el secreto de las comunicaciones salvo en casos excepcionales y con las debidas garantías, se tornará irreconocible si se permite aplicar la excepción en atención a fines infundados o supuestos inadecuados de modo patente.

En primer lugar, no se trata solamente de que la norma no permita implementar tal medida para fines distintos a los que puedan identificarse constitucionalmente, sino tampoco cuando sea claramente inoportuna.

En segundo lugar, también dañará su contenido esencial toda previsión legislativa que permita la aplicación irrestricta de la medida, aun cuando persiguiera un fin plenamente legítimo. Así, respecto de la intervención de

⁷⁶ Un contenido definido desde los primeros pronunciamientos del Tribunal Constitucional a partir de dos aproximaciones. Por un lado, identificando la naturaleza jurídica del derecho, las «facultades o posibilidades de actuación necesarias para que el derecho sea reconocible como pertinente al tipo descrito». Por otro, identificando los intereses jurídicamente protegidos por el derecho y su posible dilución mediante limitaciones que lo hagan impracticable, lo dificulten más de lo razonable o lo despojen de su necesaria protección. Cfr. STC 11/1981, de 8 de abril (FJ. 8).

comunicaciones en el proceso penal, una vez identificado su fundado objetivo en la seguridad pública, se ha considerado acertadamente que no es posible su aplicación con carácter meramente prospectivo y que, además, solo podrá afectar a quienes puedan ser tenidos razonadamente como responsables del delito investigado, «pues si el secreto pudiera alzarse sobre la base de meras hipótesis subjetivas, el derecho al secreto de las comunicaciones, tal y como la CE lo configura, quedaría materialmente vacío de contenido»⁷⁷.

Finalmente, la norma reguladora del límite no puede reiterar sin más la mera habilitación constitucional, reduciéndose a identificar los criterios de fijación del órgano jurisdiccional competente, sin previsiones complementarias dirigidas a regular el procedimiento habilitante de la intervención⁷⁸.

Esta necesidad del establecimiento de presupuestos y condiciones para la determinación del límite en el caso concreto con el mayor rigor posible deriva, como dijimos, del respeto al contenido esencial del derecho y también, de modo conexo, de las exigencias de calidad de la norma. La falta de certeza y previsibilidad de los límites, según ha afirmado el Tribunal Constitucional, «no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), [...] sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio»⁷⁹.

⁷⁷ STC 49/1999, de 5 de abril (FJ. 8).

⁷⁸ El reconocimiento del derecho sería, como ha señalado JIMÉNÉZ CAMPO, meramente retórico: «se garantizaría, sí, el derecho frente al Estado, a salvo que por uno de sus órganos —el Juzgado o Tribunal competente— se resolviera en contrario». JIMÉNÉZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 58.

⁷⁹ STC 292/2000, de 30 de noviembre (FJ. 15).

D.2. La proporcionalidad del límite como parámetro de constitucionalidad de la ley

Además del contenido esencial, se ha abogado —doctrinal y jurisprudencialmente— por utilizar el principio de proporcionalidad como parámetro para valorar la conformidad con la Constitución de los límites legalmente previstos.

En este entendimiento, el control de proporcionalidad no operaría sólo en la valoración de la aplicación judicial del límite al derecho fundamental, sino también como criterio de enjuiciamiento de la propia ley que lo establezca. La cláusula del Estado de Derecho reclamaría, para quienes defienden la aplicación en este modo del principio de proporcionalidad, una «reserva de ley proporcional»⁸⁰.

A partir de los años 90, la jurisprudencia sitúa el fundamento del principio de proporcionalidad en diversos enunciados de la Constitución —valor justicia y Estado de Derecho (art. 1.1), interdicción de la arbitrariedad de los poderes públicos (art. 9.3) o dignidad de la persona (art. 10.1)⁸¹— y va ganando sitio como canon de control en el ámbito de los derechos fundamentales.

El Tribunal Constitucional lo asume en primer lugar como herramienta para valorar la concreta aplicación de límites a los derechos fundamentales, utilizando el test de proporcionalidad en su configuración alemana, esto es, valorando los tres subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto⁸²:

⁸⁰ MEDINA GUERRERO, M., «El principio de proporcionalidad y el legislador de los derechos fundamentales», *Cuadernos de Derecho Público*, 5, 1998, págs. 120-121.

⁸¹ STC 55/1996, de 28 de marzo (FJ. 3).

⁸² Sobre la asunción de este principio en la jurisprudencia del Tribunal Constitucional español, *vid.* ROCA TRÍAS, E. y AHUMADA RUIZ, M.A., «Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española», *XV Conferencia de los Tribunales Constitucionales de Italia, Portugal y España*, 2013, págs. 1-37.

«[...] es necesario constatar si [la medida] cumple los siguientes tres requisitos o condiciones: si tal medida era susceptible de conseguir el objetivo propuesto [...]; si, además, era necesaria en el sentido de que no existía otra medida más moderada para la consecución de tal propósito con igual eficacia; y, finalmente, si la misma era proporcionada, en sentido estricto, es decir, ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto»⁸³.

Este recurso al test de proporcionalidad para enjuiciar la limitación administrativa o judicial de un derecho fundamental, hoy ampliamente aceptado y profusamente utilizado, se abrió paso también, aunque con mayores reparos, como criterio para valorar la actividad del legislador⁸⁴.

El Tribunal Constitucional advirtió desde un primer momento de la necesaria aplicación atenuada que el principio reclama cuando se trata de enjuiciar el contenido de la ley⁸⁵.

El juicio de constitucionalidad de la ley a través del principio de proporcionalidad, aun en los casos en que se ha aceptado, se ha circunscrito a rechazar lo evidentemente desproporcionado: límites «patentemente inidóneos», «sacrificio patentemente innecesario» o «desequilibrio patente y excesivo o irrazonable». En suma, como reconocen incluso los partidarios de

⁸³ STC 66/1995, de 8 de mayo (FJ. 5).

⁸⁴ El Tribunal Constitucional ha considerado que, en el ámbito de los derechos fundamentales, el principio de proporcionalidad «constituye una regla de interpretación que, por su mismo contenido, se erige en límite de toda injerencia estatal en los mismos, incorporando, *incluso frente a la ley*, exigencias positivas y negativas»; STC 49/1999, de 5 de abril (FJ. 7) —*cursiva añadida*—. En el mismo sentido, la STC 136/1999, de 20 de julio, afirma que «[e]s la ley, en una primera instancia, la que debe garantizar que el sacrificio de los derechos de los ciudadanos sea el mínimo imprescindible y que los límites y restricciones de los mismos sean proporcionados» (FJ. 21). También entre la doctrina científica encontramos autores que abogan por la aplicación del test de proporcionalidad al legislador, así, entre otros, BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, *op.cit.*, págs. 333 y ss., y MEDINA GUERRERO, M., «El principio de proporcionalidad...», *op.cit.*, pág. 119-142.

⁸⁵ STC 55/1996, de 28 de marzo (FJ. 6).

su aplicación, «frente al legislador, el principio de proporcionalidad reclama su utilización proporcionada»⁸⁶.

A ello hay que añadir que esta construcción jurisprudencial ha tenido como objeto principal la constitucionalidad de normas penales, lo que supone una diferencia cualitativa respecto de la configuración del límite al secreto de las comunicaciones que corresponde al legislador, en donde su aplicación se vería aún más aminorada⁸⁷.

La aplicación del principio de proporcionalidad como control de legalidad del límite al secreto de las comunicaciones se diluye así a términos casi homeopáticos. Por un lado, la adecuación de la medida puede ser valorada sin excesivos esfuerzos desde el respeto al contenido esencial. Y por otro, la escasa virtualidad que los subprincipios de necesidad y proporcionalidad en sentido estricto pudieran tener en relación con las normas penales —o, más generalmente, sancionadoras—, debe descartarse del todo para el caso⁸⁸.

⁸⁶ MEDINA GUERRERO, M., «El principio de proporcionalidad...», *op.cit.*, pág. 141. Existen, además, voces autorizadas entre la doctrina científica que rechazan tal modo de proceder. Enjuiciar la ley de tal forma no es congruente con el carácter abierto de la Constitución, que sólo somete la actividad del legislador de los derechos fundamentales al respeto de su contenido esencial, a la ausencia de arbitrariedad y al principio de igualdad. Una aplicación estricta del triple test de proporcionalidad resulta inconciliable, pues, con la libertad de configuración del legislador. En este sentido, JIMÉNEZ CAMPO, J., *Derechos fundamentales...*, *op.cit.*, pág. 67; y BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, págs. 184-185. Del mismo tenor es el Voto Particular del Magistrado Don Vicente Conde Martín de Hijas a la STC 136/1999, de 20 de julio, quien opina que no parece coherente la prudencia de la aplicación del Tribunal de principios expresamente enunciados (seguridad jurídica e interdicción de la arbitrariedad) con la aplicación del principio de proporcionalidad, no previsto constitucionalmente, al juicio de la ley.

⁸⁷ Se reconoce que su aplicación debe hacerse «de manera un tanto atenuada cuando no se trata del legislador penal». BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, *op.cit.*, págs. 357-359.

⁸⁸ También se mantiene este criterio en ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, *passim*, v.gr. pág. 131.

En el supuesto de normas sancionadoras, la predeterminación del legislador condiciona la actividad judicial: realizada —y probada— la conducta descrita en el tipo, el juez deberá aplicar la sanción legalmente prevista⁸⁹.

Condicionamiento que también se cumple en otras medidas no sancionadoras en cuya valoración por el Tribunal Constitucional ha tenido cierta virtualidad el principio de proporcionalidad: la imposibilidad del detenido o preso incomunicado de designar libremente abogado (STC 196/1987, de 11 de diciembre); el cierre provisional de un medio de difusión vinculado a la mera admisión de una querrela (STC 199/1987, de 16 de diciembre —FJ. 12—) o la negación automática de efectos a documentos respecto de los cuales no se justificase el pago, exención o no sujeción al impuesto de actos jurídicos documentados (STC 141/1988, de 12 de julio).

En todos estos casos, el límite dispuesto por el legislador se enuncia para el juez como una regla lógica condicionada de subsunción: «si se cumple A, se *debe* aplicar B».

Sin embargo, esta condición no se da en diligencias de investigación limitadoras de derechos fundamentales. La tarea del legislador se circunscribe aquí a poner a disposición del órgano judicial diferentes posibilidades de aplicación. No se trata sólo de que el modo de regular estas medidas forme parte de la libertad de configuración del legislador, sino que, además, una vez aprobadas, su aplicación es para el juez de carácter potestativo. Se enuncian como una regla lógica discrecional «si se cumple A, se *puede* aplicar B».

Por todo ello, el principio de proporcionalidad no constituye criterio válido para el enjuiciamiento de la ley que prevé el límite, aunque sí, según veremos, para la aplicación del límite al caso concreto.

⁸⁹ Se ha dicho que «la STC 136/1999 el Tribunal, por primera vez, declaró la inconstitucionalidad de una norma penal por imponer una pena desproporcionada (*más precisamente, por no permitir al juez imponer una pena inferior a la mínima fijada...*), cfr. ROCA TRÍAS, E. y AHUMADA RUIZ, M.A., «Los principios de razonabilidad...», *op.cit.*, pág. 16.

II.3 El juez del artículo 18.3 CE: la aplicación del límite

A. El juicio sobre la decisión de intervención

En la decisión judicial de autorizar la intervención de comunicaciones el Tribunal Constitucional ha venido exigiendo al juez competente la superación del test de proporcionalidad en su triple dimensión. Pero, además, y de forma previa a su aplicación, se ha reclamado la necesaria concurrencia de determinados presupuestos. Ambos criterios se hallan hoy expresamente previstos en la regulación de la autorización de intervención de comunicaciones en el proceso penal.

A.1. Presupuestos para la aplicación del límite

Hasta el año 2015 la LECrim permitía la intervención de comunicaciones cuando «hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa».

En conexión con tal exigencia legal, el Tribunal Constitucional, al enjuiciar en amparo pretendidas vulneraciones del art. 18.3 CE, comienza su análisis con la identificación de lo que denomina «presupuesto habilitante» para la aplicación de tal medida, que operaría como *prius* lógico necesario del juicio de proporcionalidad.

Y el presupuesto que legitima la intervención de las comunicaciones se halla en la existencia de indicios racionales de la comisión de un delito «grave» y su conexión con la persona objeto de tal medida⁹⁰.

⁹⁰ «[...] la conexión entre la causa justificativa de la limitación pretendida —la averiguación de un delito— y el sujeto afectado por ésta —aquél de quien se presume que pueda resultar autor o partícipe del delito investigado o pueda hallarse relacionado con él— es un *prius* lógico del juicio de proporcionalidad». Entre otras, SSTC 49/1999, de 5 de abril (FJ. 8); 166/1999, de 27 de septiembre (FJ. 8); 171/1999, de 27 de septiembre (FJ. 8); 14/2001, de 29 de enero (FJ. 2); 138/2001, de 17 de julio (FJ 3); 167/2002, de 18 de septiembre (FJ. 2); y 184/2003, de 23 de octubre (FJ. 11).

- Especialidad y prohibición de intervenciones prospectivas

La necesaria conexión entre persona investigada e indicios de la comisión de un delito es exigencia de lo que ahora la LECrim denomina principio de especialidad⁹¹.

Dicha conexión tiene por objeto evidenciar que la medida no tiene carácter meramente prospectivo y no se dirige, por tanto, a satisfacer la necesidad genérica de prevenir o descubrir delitos, pues tal modo de proceder se ha estimado contrario al derecho fundamental al secreto de las comunicaciones, que prohíbe pretender su desvelo sin base objetiva⁹².

Del mismo modo, se ha exigido la existencia previa de un procedimiento de investigación penal, sin que sea posible autorizar intervenciones comunicativas previamente a su iniciación⁹³.

Estos requisitos expresamente previstos en el art. 588 bis a LECrim desde la reforma de 2015, recogen determinados principios rectores de común observancia para todas las medidas de investigación tecnológica introducidas.

En concreto, su segundo apartado dispone: «El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva».

⁹¹ Vid. RODRÍGUEZ MONTAÑÉS, T., «Artículo 18.3. El secreto de las comunicaciones», *Comentarios a la Constitución Española*, RODRÍGUEZ-PIÑERO Y BRAVO FERRER, M. y CASAS BAAMONDE, M. E. (Dir.), Tomo I, Agencia Estatal Boletín Oficial del Estado, Madrid, 2018, págs. 550-552.

⁹² SSTC 184/2003, de 23 de octubre (FJ. 11), y 165/2005, de 20 de junio (FJ. 4) y SSTS, Sala de lo Penal, de 20 de mayo de 1994 (FJ. 1); 16 de diciembre de 2011 (FJ. 2); y 24 de noviembre de 2017 (FJ. 2). Vid. GÓRRIZ ROYO, «Investigaciones prospectivas y secreto de las comunicaciones: respuestas jurídicas», GONZÁLEZ CUSSAC, J.L. y CUERDA ARNAU, M.L. (Dir.), *Nuevas amenazas a la seguridad nacional: Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Tirant Lo Blanch, Valencia, 2013, págs. 243-283.

⁹³ STS, Sala de lo Penal, de 24 de noviembre de 2017 (FJ. 2).

Se trata, en definitiva, de neutralizar «el riesgo de convertir el Estado de Derecho en un Estado policial»⁹⁴.

- *Los indicios racionales de criminalidad*

Tanto el art. 579 vigente al tiempo de aprobarse la Constitución como ahora los artículos 588 bis c) y d) exigen para autorizar la intervención de comunicaciones la existencia de «indicios», «indicios de criminalidad» o «indicios racionales»⁹⁵.

La norma no explicita, sin embargo, qué deba entenderse por «indicios», y ello pese a que la motivación de su existencia constituye la *ratio decidendi* del acto de injerencia⁹⁶.

Han sido, por tanto, los pronunciamientos de la doctrina científica y jurisprudencial los que han ido dotando de un contenido cierto a este término. En el entendido de que se trata de datos externos que permiten descubrir, con la firmeza que proporciona la sospecha fundada, la responsabilidad criminal de la persona en relación con el hecho posible objeto de investigación a través de la interceptación de sus comunicaciones⁹⁷.

Sospechas, no meras conjeturas, fundadas en datos objetivos en un doble sentido: «En primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control. Y, en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o se va a cometer el delito sin que puedan consistir en valoraciones acerca de la persona»⁹⁸.

⁹⁴ ZOCO ZABALA, C., *La Intervención Judicial de las Comunicaciones ¿Privadas?*, Aranzadi, Cizur Menor, 2014, pág. 105.

⁹⁵ También exige la existencia de tales indicios el art. 188 de la Ley Orgánica Procesal Militar.

⁹⁶ ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones, op.cit.*, pág. 147.

⁹⁷ ATS, Sala de lo Penal, de 18 de junio de 1992 (FJ. 2).

⁹⁸ SSTC 49/1999, de 5 de abril (FJ. 8); 167/2002, de 18 de septiembre (FJ. 2); 184/2003, de 23 de octubre (FJ. 11); 165/2005, de 20 de junio (FJ. 4); 259/2005, de 24 de octubre (FJ. 2); y 220/2006, de 3 de julio (FJ. 3).

Es decir, se trata de valorar *ex ante* unos datos objetivos que deben ser exteriorizados con cierta concreción y que permitan, por tanto, fiscalizar *ex post* su oportunidad y racionalidad⁹⁹. Su ausencia no puede ser sanada a posteriori por el éxito de la investigación¹⁰⁰.

En todo caso, debe ser el órgano judicial competente quien lleve a cabo el «juicio ponderativo sobre el nivel cualificativo [*sic*] de los indicios que avalan las sospechas», que no puede basarse únicamente en la admisión acrítica de las sospechas de los agentes policiales, sino que deben aportar al instructor elementos objetivos que apoyen el juicio de probabilidad. Así, aun cuando no es necesario que la policía proporcione al juzgador información exhaustiva en su solicitud, ésta le debe permitir comprobar que representa objetivamente «un sustrato que racionalmente hace pensar en la probable comisión de un delito [y] en la implicación en él de las personas cuyo derecho fundamental va a ser afectado»¹⁰¹.

- La gravedad del delito investigado

Hasta la reforma operada en el año 2015 la LECrim no preveía un catálogo de delitos para cuya investigación pudiera el juez instructor recurrir a la intervención de comunicaciones del procesado, siendo una de las deficiencias puestas de manifiesto en las diversas condenas a España por el TEDH.

Esta laguna legislativa se palió jurisprudencialmente en el entendimiento de que, tratándose de una injerencia en un derecho fundamental que, además, se lleva a cabo por el Estado de modo subrepticio, su legitimidad se

⁹⁹ LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales...», *op.cit.*, págs. 109-110.

¹⁰⁰ Por todas, SSTC 299/2000, de 11 de diciembre (FJ. 5); 138/2001, de 18 de junio (FJ. 4); 167/2002, de 18 de septiembre (FJ. 3); 165/2005, de 20 de junio (FJ. 5); y 259/2005, de 24 de octubre (FJ. 4).

¹⁰¹ STS, Sala de lo Penal, de 21 de febrero de 2017 (FFJJ. 5 y 6).

encontraba condicionada a que los indicios de criminalidad lo fueran respecto de la presunta comisión de un hecho delictivo «grave»¹⁰².

No obstante, la jurisprudencia se separó tempranamente de un criterio meramente penológico en la valoración de la gravedad del delito. Así, además de los delitos castigados con penas graves (art. 33 CP), también se consideró que se podía recurrir a esta medida de investigación atendiendo a la naturaleza de los bienes jurídicos protegidos o a la relevancia social de los hechos¹⁰³.

Este criterio ha sido asumido por el legislador. La vigente LECrim incorpora en sus arts. 579.1 (comunicaciones postales y telegráficas) y 588 ter.a (comunicaciones telefónicas y telemáticas) un listado cerrado de delitos que podrá legitimar la adopción de esta medida. Y decimos podrá porque el hecho de hallarnos ante uno de estos delitos no habilita indefectiblemente el acto de injerencia, sino que se requiere el estudio del caso concreto para comprobar si supera el tamiz del juicio de proporcionalidad.

Debe entenderse, con ZOCO ZABALA, que la delimitación legal, tanto cuantitativa como cualitativa, de este catálogo —*numerus clausus*— no supone un juicio anticipado favorable de proporcionalidad, sino que es mera garantía de seguridad jurídica e igualdad en aplicación de las normas¹⁰⁴. Como

¹⁰² ATS, Sala de lo Penal, de 18 de junio de 1992 (FFJJ. 2 y 4), y STC 49/1996, de 26 de marzo (FJ. 3).

¹⁰³ STS, Sala de lo Penal, de 25 de junio de 1993 (FJ. 3), o SSTC 54/1996, de 26 de marzo (FJ. 7), y 166/1999, de 27 de septiembre (FJ. 3.a). Sobre la investigación de delitos de contrabando (con pena, al momento de los hechos, de 6 meses a 3 años de prisión), la gravedad se considera presente en la relevancia social de los hechos, plasmada por el legislador en la Exposición de Motivos de la norma: SSTC 299/2000, de 11 de diciembre (FJ. 2); 14/2001, de 29 de enero (FJ. 3); y 82/2002, de 22 de abril (FJ. 4). En el caso de delitos de cohecho y falsedad documental cometidos por un funcionario público, dice la STC 184/2003, de 23 de octubre (FJ. 10): «la importancia del bien jurídico protegido cuando los hechos delictivos se conectan con el ejercicio de sus cargos por funcionarios públicos, su relevancia estructural para el funcionamiento del Estado y la trascendencia social de los mismos al producir el socavamiento de la confianza de los ciudadanos en aquél y en sus instituciones, entre las cuales los partidos políticos son esencialmente relevantes en el marco de un sistema democrático y pluralista, avalan, sin duda, su gravedad».

¹⁰⁴ ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, págs. 175 y ss.

acertadamente se ha señalado, «son presupuestos necesarios, pero nunca suficientes»¹⁰⁵.

Los delitos en cuya investigación se puede acordar la intervención de comunicaciones postales y telegráficas (art. 579.1 LECrim), son los siguientes:

En primer lugar, los «delitos dolosos castigados con pena límite máximo de, al menos, tres años de prisión». Presupuesto que se fija en atención tanto a la naturaleza del delito investigado, permitiéndose adoptar la medida sólo para delitos dolosos, como a la gravedad de la pena, tomando como referencia el límite máximo de la horquilla, que debe ser de, al menos, tres años de prisión, incluyéndose, por tanto, un buen número de delitos que, desde un criterio estrictamente penológico, son considerados menos graves.

Por otro lado, y en atención a la relevancia social de su comisión, se prevé la activación de esta diligencia para investigar tanto «delitos cometidos en el seno de un grupo u organización criminal», como «delitos de terrorismo»¹⁰⁶.

Por su parte, para la intervención de las comunicaciones telefónicas y telemáticas el art. 588 ter a) añade a los anteriores un nuevo tipo delictivo, atendiendo en este caso al medio de ejecución: aquellos cometidos «a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación».

¹⁰⁵ GONZÁLEZ-CUÉLLAR SERRANO, N. y MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna, Madrid, 2015, pág. 216.

¹⁰⁶ La comisión grupal del delito ya se había revelado jurisprudencialmente como criterio de gravedad que avalase la intervención de las comunicaciones. La STC 299/2000, de 11 de diciembre (FJ. 2), afirma: «A la hora de ponderar la relevancia social de los hechos y su gravedad, el elemento de que sean organizaciones complejas las que se dedican a su comisión es, sin duda, un factor de suma importancia a atender, por la potencial eficacia de dichas organizaciones en su embate contra los intereses sociales y públicos garantizados por la legalidad que atacan».

Este último presupuesto vendría justificado por la necesidad de buscar un cierto equilibrio entre los medios con que cuenta el delincuente y aquellos de los que debe poder valerse el Estado para tratar de reprimir sus conductas.

El legislador ha asumido, por tanto, los criterios ya establecidos previamente por la jurisprudencia, considerando la gravedad del delito no sólo a partir de la pena prevista, sino también de la trascendencia social de determinados delitos, su naturaleza o el ámbito en que se producen¹⁰⁷.

A.2. El test de proporcionalidad

Satisfechos los presupuestos tratados, el juez instructor debe todavía aplicar en el caso concreto el test de proporcionalidad antes de autorizar su práctica.

Como se dijo, desde principios de los años 90, el test de proporcionalidad, en su construcción alemana de triple juicio, se ha venido utilizando en la jurisprudencia como herramienta habitual para evaluar las injerencias en los derechos fundamentales¹⁰⁸.

Sabemos también que, para el caso que nos ocupa y ante la ausencia de norma que fijase los criterios específicos de intervención, la correcta aplicación del juicio de proporcionalidad y su oportuna exteriorización fueron utilizados como criterios sanadores, en el caso concreto, de los defectos de calidad de la ley¹⁰⁹.

¹⁰⁷ LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales...», *op.cit.*, pág. 105.

¹⁰⁸ El principio de proporcionalidad también ha sido utilizado frecuentemente por el TEDH para valorar la conformidad con el Convenio de restricciones operadas sobre determinados derechos, lo que ha tenido incidencia, *vía* 10.2 CE, en nuestra jurisprudencia interna. Pese a que este principio no se halla expresamente previsto en el CEDH, se ha inferido de la exigencia explícita en diversos preceptos de que las medidas restrictivas de los derechos sean «necesarias en una sociedad democrática» para la consecución de determinados fines. Sobre esta cuestión, *vid.* FASSBENDER, B., «El principio de proporcionalidad en la jurisprudencia del Tribunal Europeo de Derechos Humanos», *Cuadernos de Derecho Público*, 5, 1998, págs. 51-73; y ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, págs. 135 y ss.

¹⁰⁹ Por todas, STC 49/1999, de 5 de abril.

Mediante su aplicación se trata de valorar si la medida es adecuada para alcanzar el objetivo pretendido, si es necesaria por no existir otras más moderadas y de similar eficacia, y si la relación entre sacrificio y objetivo perseguido es proporcionada¹¹⁰.

Estos criterios, que constituyen el triple test de adecuación, necesidad y proporcionalidad se encuentran hoy expresamente previstos como principios de aplicación común a todas las medidas de investigación tecnológica incorporadas a la LECrim por la Ley Orgánica 13/2015, de 5 de octubre¹¹¹.

- Idoneidad o adecuación

El test de idoneidad o adecuación se dirige a verificar si la intervención de comunicaciones es una medida adecuada para alcanzar el fin pretendido (la averiguación de hechos relevantes para la causa).

Se ha dicho, por un lado, que opera como criterio negativo, destinado a comprobar principalmente que la medida no sea inadecuada para alcanzar el fin legítimo al que sirve¹¹².

Por otro lado, se ha propuesto que la idoneidad sea valorada desde un triple punto de vista: «1º) La medida debe ser por su naturaleza la más apta para la consecución del fin previsto; 2º) Su duración debe estar en estrecha relación con su finalidad; 3º) El sujeto al que se dirija la medida ha de estar debidamente individualizado»¹¹³.

Este criterio parece ser asumido por el legislador, ya que el art. 588 bis.a.3 enuncia este principio con el siguiente tenor:

¹¹⁰ Entre otras, SSTC 66/1995, de 8 de mayo (FJ. 5), y 198/2003, de 10 de noviembre (FJ. 6), y STS, Sala de lo Penal, de 24 de noviembre de 2017 (FJ. 2).

¹¹¹ La observancia del principio de proporcionalidad se prevé también expresamente para la intervención de las comunicaciones del concursado (art. 1.3 Ley Orgánica 8/2003, de 9 de julio, para la Reforma Concursal).

¹¹² ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, op.cit., pág. 133.

¹¹³ NOYA FERREIRO, L., «Presupuestos constitucionales de las medidas de intervención de las comunicaciones I», *Dereito. Revista xuridica da Universidade de Santiago de Compostela*, 2, 1999, págs. 157-158.

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

Es decir, no opera simplemente como criterio para valorar la adecuación de la medida en sí —la intervención de las comunicaciones—, sino también para definir su grado de injerencia: qué medida adoptar y con qué objeto (contenido de comunicaciones o sólo datos externos) —*ámbito objetivo*—, sobre qué personas —*ámbito subjetivo*— y en qué espacio temporal —*duración*—.

- Necesidad, excepcionalidad o subsidiariedad

La aplicación de este principio supone elegir, de entre los medios que se hayan demostrado idóneos, aquel que comporte un menor perjuicio en el derecho fundamental limitado, verificando, por tanto, el carácter imprescindible de la medida a adoptar¹¹⁴.

En este sentido, el art. 588 bis.a.4 LECrim dispone que sólo podrán acordarse medidas de investigación tecnológicas bien cuando no existan medidas menos gravosas para los derechos fundamentales del investigado, bien cuando el hecho de no recurrir a las mismas dificulte gravemente «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».

- Proporcionalidad en sentido estricto

El juicio de proporcionalidad en sentido estricto tiene como objetivo determinar si la medida es equilibrada por derivarse de ella más ventajas para el interés público —la investigación delictiva— que perjuicios sobre otros bienes en conflicto —el derecho fundamental al secreto de las comunicaciones del investigado—.

¹¹⁴ ZOCO ZABALA, C., *La Intervención Judicial...*, op.cit., pág. 98.

El art. 588 bis.a.5 LECrim ofrece ahora los elementos valorativos del interés público que deben tenerse en cuenta en el juicio de ponderación: «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»¹¹⁵.

Se ha dicho que este principio se ha visto defraudado en la medida en que, según hemos visto, se fija como presupuesto habilitante que los delitos investigados estén castigados con pena cuyo límite máximo sea de, al menos, tres años de prisión, separándose del criterio penológico que considera delitos graves los castigados con pena de prisión superior a cinco años¹¹⁶.

Entendemos, sin embargo, que el hecho de fijar un criterio general atendiendo a la gravedad de la pena no conculca liminarmente el principio de proporcionalidad, pues no libera a la autoridad judicial de tener que aplicar el juicio de ponderación en el caso concreto. Esto es, debe distinguirse el cumplimiento del presupuesto objetivo —aquellos delitos sobre los que se puede aplicar el acto de injerencia— de la oportunidad de aplicar una medida concreta en un caso concreto, lo que exige superar el filtro del principio de proporcionalidad.

Finalmente, debe añadirse que, pese a que la norma solo vincula explícitamente el principio de idoneidad con el grado de extensión con que se autorice la medida —ámbito objetivo y subjetivo y duración—, consideramos

¹¹⁵ Además de los criterios que habían sido utilizados jurisprudencialmente para determinar la gravedad del delito investigado, le norma prevé ahora también como criterio a valorar la incidencia del uso de las tecnologías de la información y de la comunicación en la ejecución de la actividad delictiva. *Vid.* LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales...», *op.cit.*, pág. 105. No obstante, consideramos que es este un criterio que se compadece mejor con el juicio de necesidad que con el de proporcionalidad en sentido estricto. Si el delito se ha cometido a través de estas tecnologías es posible que el recurso a esta medida sea imprescindible para la eficacia de la investigación, pero en el juicio de proporcionalidad debieran valorarse otros parámetros como la gravedad de la pena o la entidad del bien jurídico protegido.

¹¹⁶ *Informe del Consejo General del Poder al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas*, págs. 84 y ss.

que deber ser también tenido en cuenta respecto de su necesidad y proporcionalidad. Es decir, el modo de adopción de una medida de intervención de comunicaciones en el caso concreto (su duración, su objeto...) determina también su necesidad y proporcionalidad¹¹⁷.

En conexión con esto, es necesario hacer siquiera referencia al principio, de creación jurisprudencial, de la menor injerencia en el derecho fundamental al secreto de las comunicaciones cuando la intervención tiene por objeto únicamente datos de tráfico, sin acceso, por tanto, al contenido comunicado.

El Tribunal Constitucional utilizó por primera vez este criterio en la sentencia 123/2002. Tras reconocer que los datos asociados forman parte del objeto del derecho fundamental al secreto de las comunicaciones, afirma que «no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las "escuchas telefónicas", siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad»¹¹⁸.

También el Tribunal Supremo ha aplicado esta doctrina en similar sentido, considerando que la intervención de datos asociados requiere «un nivel de exigencia y control mucho más bajo que el de una intervención de las conversaciones porque la injerencia es mucho menor»¹¹⁹.

¹¹⁷ Por ejemplo, puede no reputarse necesaria la intervención del contenido de las comunicaciones que tenga por objeto únicamente descubrir la existencia una determinada comunicación (lo que puede ser útil, por ejemplo, para comprobar el incumplimiento de una orden de incomunicación), por poder autorizar otra medida igual de eficaz, pero menos gravosa (la intervención únicamente de los datos asociados).

¹¹⁸ STC 123/2002, de 20 de mayo (FJ. 6). Este criterio es también tenido en cuenta en la STC 26/2006, de 30 de enero (FJ. 7), donde se valida el proceder del juez instructor quien, a la vista de la insuficiencia de los indicios aportados por la policía, no autoriza las escuchas solicitadas, pero sí la remisión de los listados de llamadas realizados en atención a la menor intensidad que esta injerencia supone en el objeto del derecho fundamental.

¹¹⁹ STS, Sala de lo Penal, de 3 de octubre de 2007 (FJ. 3). Sobre este principio de menor intensidad, puede verse RODRÍGUEZ LAINZ, J.L., «El principio de proporcionalidad...», *op.cit.*, págs. 32 y ss.

B. La resolución judicial

El art. 18.3 CE prevé la posibilidad de levantar el secreto de las comunicaciones mediante «resolución judicial». Sin embargo, nada dice sobre su forma ni sobre la necesidad de motivación.

Ello constituye una excepción a la regla que históricamente habían seguido las constituciones españolas al declarar el derecho que venimos considerando: en todas ellas se prevé la forma de Auto, exigiendo expresamente en algunos casos su motivación¹²⁰.

A la previsión de estas cautelas se dirigieron la mayor parte de enmiendas que recibió la redacción del 18.3 CE en su proceso de elaboración. Las cuatro enmiendas presentadas a este artículo en el Congreso (núm. 116, 339, 470 y 695) propusieron como inciso final del precepto la fórmula «salvo resolución judicial motivada»; siendo rechazadas por la oposición del Grupo Parlamentario de Unión de Centro Democrático.

En todo caso, las normas infraconstitucionales que prevén en nuestro ordenamiento la posibilidad de alzar el secreto de las comunicaciones exigen que se autorice mediante «auto motivado» (arts. 583 y 588 bis.c LECrim), «resolución motivada» (art. Único.3 LO 2/2002), «decisión judicial motivada» (art. 1.3 LO 8/2003) o simplemente mediante auto (arts. 187 y 188 LO 2/1989), que consiste, como es sabido, en una resolución motivada (arts. 208.2 LEC y 141 LECrim).

No obstante, el Tribunal Constitucional considera desde un primer momento que la necesidad de motivación, en casos de injerencia en derechos fundamentales, es exigencia directamente constitucional: «la motivación es no

¹²⁰ El art. 8 de la Constitución de 1969 señalaba que «[t]odo auto de [...] detención de la correspondencia escrita o telegráfica, será motivado», previendo incluso que la ausencia de motivación o su insuficiencia pudiera dar lugar a una indemnización «proporcionada al daño causado, pero nunca inferior a 500 pesetas». También el art. 8 de la Constitución de 1876 preveía expresamente la exigencia de auto motivado, mientras que el art. 32 de la Constitución de 1931 simplemente señalaba la forma de auto. Sobre esta cuestión, *vid.* JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 65.

sólo una elemental cortesía, sino un riguroso requisito del acto de sacrificio de los derechos»¹²¹.

El juez deberá exteriorizar razonadamente los criterios en que basa su decisión de autorizar la intervención. El Tribunal Constitucional ha considerado, además, que en el caso de resoluciones que incidan de algún modo en derechos fundamentales la exigencia de motivación posee un carácter especialmente reforzado¹²². Y, para el caso del secreto de las comunicaciones, que la motivación de las resoluciones que acuerdan su alzamiento forma parte del contenido esencial del art. 18.3 CE¹²³.

Por ello, su ausencia o insuficiencia determinará, no sólo una vulneración formal o procesal del derecho fundamental a la tutela judicial efectiva (art. 24 CE), sino también una vulneración del derecho fundamental sustantivo que la resolución limita¹²⁴.

¹²¹ STC 26/1981, de 17 de julio (FJ. 14). En similar sentido, SSTC 62/1982, de 15 de octubre (FJ. 2), y 13/1985, de 31 de enero (FJ. 2). Para el caso de la autorización judicial del art. 18.3, el Tribunal Constitucional se pronuncia por primera vez, exigiendo la debida motivación, en la STC 85/1994, de 14 de marzo (FJ. 3). Cfr., asimismo, RODRÍGUEZ RUIZ, B., «El coste de los derechos fundamentales...», *op.cit.*, pág. 326; y JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 66. También la jurisprudencia constitucional italiana, desde la Sentenza n. 34 del 1973, ha prestado especial atención al requisito de la motivación de las resoluciones judiciales limitadoras del derecho a la libertad y al secreto de las comunicaciones.

¹²² «[C]uando el derecho a la tutela judicial efectiva se encuentra conectado con otro derecho fundamental, el estándar de las exigencias derivadas del deber de motivación es más riguroso, lo que se ha identificado con la exigencia de una tutela "reforzada"»; STC 222/2007, de 8 de octubre (FJ. 3).

¹²³ Por todas, SSTC 197/2009, de 28 de septiembre (FJ. 4); 72/2010, de 18 de octubre (FJ. 2); y 145/2014, de 22 de septiembre (FJ. 2). *Vid.* ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, págs. 120 y ss.

¹²⁴ La STC 180/2005, de 4 de julio (FJ. 6), afirma: «cuando se aduce la vulneración del derecho a la tutela judicial efectiva en relación con una resolución judicial en la cual se ventilan cuestiones que guardan conexión con derechos fundamentales sustantivos, el canon constitucional de enjuiciamiento no puede ser el de la razonabilidad y la interdicción de la arbitrariedad y el error patente, sino que es preciso enjuiciar si la resolución judicial tomó o no en consideración el derecho fundamental sustantivo concernido y realizó una interpretación constitucionalmente adecuada del mismo. Consecuentemente se produce una simbiosis entre ambos derechos fundamentales que trae consigo que la falta o defectuosa motivación suponga la vulneración del derecho sustantivo, al menos cuando el objeto de la resolución judicial es precisamente la limitación o afectación de ese derecho, o el control sobre las limitaciones o afectaciones producidas en relación con él por otros poderes públicos (casos de prisión provisional, intervención de comunicaciones, inviolabilidad del domicilio, etc.)».

En este sentido, motivación y ley se encuentran estrechamente vinculadas pues si, como dijimos, sólo a la ley corresponde prever los criterios que permitan al juez intervenir, la motivación judicial deberá referirse a los presupuestos normativamente establecidos¹²⁵.

En ausencia de ley fue la jurisprudencia quien se ocupó de determinar los requisitos de motivación que debían cumplir las autorizaciones de intervención de comunicaciones, cuya estricta observancia ocupa recurrentemente muchos casos de amparo.

Así, se consideró que la resolución debía exteriorizar las razones fácticas y jurídicas que habían llevado al juez a autorizar la intervención, dando cuenta del cumplimiento del presupuesto habilitante —la existencia de indicios racionales de delito grave—, así como de la superación del juicio de proporcionalidad, declarando la medida idónea, necesaria y proporcional. Pero, además, el Tribunal Constitucional había venido exigiendo otros contenidos: la identificación precisa de las personas y comunicaciones objeto de intervención, el tiempo de duración, las personas encargadas de su práctica o los periodos en que debiera darse cuenta al juez para controlar su ejecución¹²⁶.

Del mismo modo, en la autorización de prórrogas a la intervención inicialmente acordada, el juez debía observar las mismas exigencias de motivación, debiendo tener en cuenta para ello los datos obtenidos hasta el momento y, en su atención, exteriorizar las razones para extender la limitación,

¹²⁵ El Voto particular del Magistrado Cruz Villalón a la STC 49/1999, de 5 de abril, afirma: «la calidad de la ley formal facilita la motivación; las carencias de la misma la dificultan y, a la vez, la hacen más necesaria».

¹²⁶ Entre otras, SSTC 49/1996, de 26 de marzo (FJ. 3); 49/1999, de 5 de abril (FJ. 7); 299/2000, de 11 de diciembre (FJ. 4); 167/2002, de 18 de septiembre (FJ. 2); 184/2003, de 23 de octubre (FJ. 9); 165/2005, de 20 de junio (FJ. 4); 197/2009, de 28 de septiembre (FJ. 4); 72/2010, de 18 de octubre (FJ. 2); 25/2011, de 14 de marzo (FJ. 2); y 145/2014, de 22 de septiembre (FJ. 2).

sin que se considerase suficiente «una remisión tácita o presunta a la inicialmente obtenida»¹²⁷.

Sin embargo, resulta menos correcto que, al tiempo que el Tribunal venía exigiendo una motivación especialmente reforzada, admitiera, desde la STC 123/1997 y en no pocas ocasiones, resoluciones judiciales de intervención en forma de meros impresos-formularios o motivaciones lacónicas, siempre que pudiera ser integrada con el contenido del oficio policial:

«[...] aunque lo deseable es que la expresión de los indicios objetivos que justifiquen la intervención quede exteriorizada directamente en la resolución judicial, ésta puede considerarse suficientemente motivada si, integrada incluso con la solicitud policial, a la que puede remitirse, contiene los elementos necesarios para considerar satisfechas las exigencias para poder llevar a cabo con posterioridad la ponderación de la restricción de los derechos fundamentales que la proporcionalidad de la medida conlleva»¹²⁸.

Se ha vinculado asimismo motivación con proporcionalidad y, en atención a la doctrina de la menor intensidad de la injerencia sobre el derecho fundamental propia de los datos asociados, se ha admitido excepcionalmente que la intervención sea autorizada por providencia¹²⁹.

¹²⁷ SSTC 202/2001, de 15 de octubre (FJ. 6); 261/2005, de 24 de octubre (FJ. 4); 26/2010, de 27 de abril (FJ. 2); 25/2011, de 14 de marzo (FJ. 2); y 145/2014, de 22 de septiembre (FJ. 2).

¹²⁸ STC 167/2002, de 18 de septiembre (FJ. 2). En igual sentido, SSTC 123/1997, de 1 de julio (FJ. 5); 166/1999, de 27 de septiembre (FJ. 7); 171/1999, de 27 de septiembre (FJ. 6); 126/2000, de 16 de mayo (FJ. 7); 299/2000, de 11 de diciembre (FJ. 4); 138/2001, de 18 de junio (FJ. 3); 202/2001, de 15 de octubre (FJ. 5); 184/2003, de 23 de octubre (FJ. 9); 165/2005, de 20 de junio (FJ. 4); 205/2005, de 18 de julio (FJ. 3); 197/2009, de 28 de septiembre (FJ. 4); 5/2010, de 7 de abril (FJ. 2); y 72/2010, de 18 de octubre (FJ. 2). Asimismo, SSTS, Sala de lo Penal, de 27 de noviembre de 1998 (FJ. 1); 11 de mayo de 2001 (FJ. 1); 20 de junio de 2006 (FJ. 1); 12 de abril de 2012 (FJ. 8); y 18 de abril de 2013 (FJ. 6). En la doctrina, véase ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, págs. 125-126; y NOYA FERREIRO, L., «Presupuestos constitucionales (II)...», *op.cit.*, págs. 119-120.

¹²⁹ STC 123/2002, de 20 de mayo (FJ. 7). Afirma el ATS, Sala de lo Penal, de 18 de junio de 1992 (FJ. 4), que «en la motivación, actúa, a su vez, la proporcionalidad. A mayor transcendencia de la decisión, mayor exigencia, si cabe, respecto de la motivación».

En la actualidad, la LECrim regula expresamente el contenido de la resolución judicial que autorice la intervención de comunicaciones, exigiendo que se realice por «auto motivado» (art. 588 bis.c.1).

Los contenidos legalmente requeridos son coincidentes con los previamente construidos por la jurisprudencia (art. 588 bis.c.3).

Se debe exteriorizar, en primer lugar, el cumplimiento de los presupuestos habilitantes: existencia de indicios racionales de la comisión de alguno de los delitos cuya investigación permite activar esta medida e identificación de los investigados (apdos. a y b).

En segundo lugar, la resolución debe dar cuenta de la superación del juicio de proporcionalidad, identificando la finalidad perseguida y la extensión con que se autoriza (apdos. c y g).

Finalmente, la norma prevé el resto de los contenidos que se habían estimado como necesarios por el Tribunal Constitucional: duración de la medida (e), identificación de la unidad policial y del sujeto encargado de practicar la intervención (d y h) y modo de llevar a cabo el control judicial de su ejecución (f).

C. Práctica de la intervención y control judicial

Autorizada judicialmente la intervención dará comienzo su práctica, extendiéndose, en principio, hasta la fecha acordada en la resolución, que no podrá ser superior a tres meses, sin perjuicio de que sea sucesivamente prorrogada hasta un máximo de dieciocho (arts. 579.2 y 588 ter.g LECrim).

Respecto al comienzo del cómputo del plazo, la norma recoge ahora el criterio que, tras algunas vacilaciones iniciales, había sido jurisprudencialmente establecido: la duración de la medida se computará desde la fecha de la autorización judicial y no desde el inicio efectivo de su práctica (STC 205/2005, de 18 de julio —FJ. 5—, y art. 588 ter.g LECrim).

Por su parte, el cese se producirá una vez agotado el plazo o anticipadamente, bien porque desaparezcan las circunstancias de su adopción, bien por reputarla ineficaz.

La decisión de intervenir y el control de su práctica compete en exclusiva al órgano judicial, pudiendo recabar en la ejecución material de la medida el auxilio de otras autoridades.

La obligación de colaborar con la autoridad judicial viene impuesta para los operadores que exploten redes de telecomunicaciones tanto en el art. 39.2 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, como en el art. 588 ter.e LECrim, precepto que amplía este deber a «toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual».

Por ello, cobra especial importancia el Sistema Integrado de Interceptación Legal de Telecomunicaciones, *SITEL*. Se trata de una avanzada aplicación informática, cuya titularidad corresponde al Ministerio de Interior, que permite la identificación e interceptación de comunicaciones electrónicas, del contenido y de un gran número de datos asociados ¹³⁰.

¹³⁰ La puesta en marcha de *SITEL* generó un gran revuelo social y algunas dudas de constitucionalidad, principalmente por problemas de rango normativo, que entendemos en estos momentos superadas. Sobre esta cuestión, *vid.* ZOCO ZABALA, C., «Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de *SITEL* con el artículo 18.3 CE», *InDret*, 4, 2010, págs. 1-17; RODRÍGUEZ LAINZ, J.L., «Consideraciones jurídicas en torno a la licitud constitucional de *SITEL*», *Diario La Ley*, 7344, 2010, págs. 1-21; MARCHENA GÓMEZ, M., «La vulneración de derechos fundamentales...», *op.cit.*, págs. 1-15; FERNÁNDEZ RODRÍGUEZ, J.J., «La intervención de las comunicaciones digitales: a propósito del sistema *SITEL*», FERNÁNDEZ RODRÍGUEZ, J.J., SANSÓ-RUBERT PASCUAL, D., PULIDO GRAJERA, J., MONSALVE, R. (Coords.), *Cuestiones de inteligencia en la sociedad contemporánea*, Ministerio de Defensa, Madrid, 2012, págs. 61-75; y VIDAL MARÍN, T. y RUIZ DORADO, M., «Análisis de la constitucionalidad de *SITEL*. Breves consideraciones a partir de la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal», *Revista Aranzadi Doctrinal*, 9, 2016, págs. 135-162.

El sistema cuenta con un servidor central encargado de almacenar la información que recibe de los operadores y distribuirla, en tiempo real y de forma estanca, a las unidades periféricas responsables de la intervención.

El agente facultado, es decir, el agente de «policía judicial o personal del Centro Nacional de Inteligencia habilitado por una autoridad judicial para materializar una interceptación legal», es el encargado de realizar la supervisión del contenido y confeccionar la diligencia de información para su puesta a disposición del juez instructor. Por su parte, el servidor central realiza un volcado de todos los datos intervenidos a formato adecuado para su entrega a la autoridad judicial correspondiente¹³¹.

El control del proceso de ejecución de la intervención corresponde al juez instructor, considerándose que la fiscalización judicial de la restricción del derecho fundamental forma parte de su contenido esencial¹³².

El juez, como vimos, debe establecer en la resolución por la que autoriza la intervención la forma y plazos en que los agentes encargados de su ejecución deban informarle del desarrollo de la medida. Se trata, en definitiva, de que el juez conozca las vicisitudes de su desarrollo y los resultados que se van obteniendo para la investigación, pues sólo a partir de dicho conocimiento podrá autorizar nuevas prórrogas o decretar el cese de la intervención si se estima inadecuada por la ausencia de resultados.

La LECrim establece, en sede de control judicial de la intervención de comunicaciones, que la policía judicial ponga a disposición del juez, con la periodicidad determinada en la resolución, las grabaciones en dos soportes distintos: uno con la transcripción de los pasajes de las conversaciones que el

¹³¹ La explicación del funcionamiento del sistema se extrae de la STS, Sala de lo Penal, de 13 de marzo de 2009 (FJ. 1). La definición de agente facultado corresponde al art. 84.e) del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

¹³² Entre otras, SSTC 49/1996, de 26 de marzo (FJ. 3); 121/1998, de 15 de junio (FJ. 5); 49/1999, de 5 de abril (FJ. 11); 205/2002, de 11 de noviembre (FJ. 4); y 184/2003, de 23 de octubre (FJ. 12).

agente facultado considere de interés para la investigación y otro que contenga íntegramente las grabaciones realizadas (art. 588 ter.f LECrim)¹³³.

En todo caso, la jurisprudencia del Tribunal Constitucional ha considerado reiteradamente que los defectos en la incorporación de las grabaciones al proceso no inciden en el objeto protegido por el art. 18.3 CE, sino que se trata de una injerencia en el derecho al proceso con todas las garantías del 24.1: «lo relativo a la entrega y selección de las cintas grabadas, a la custodia de los originales y a la transcripción de su contenido, no forma parte de las garantías del art. 18.3 CE, sin perjuicio de su relevancia a efectos probatorios»¹³⁴.

Por su parte, la comisión de delitos de carácter transnacional puede requerir que la intervención de comunicaciones se practique en un Estado diferente al del órgano judicial encargado de su investigación. En este sentido, cobran especial importancia los mecanismos jurídicos de cooperación judicial internacional, como el Convenio de asistencia judicial en materia penal de 20 de abril de 1959.

Para el caso de la Unión Europea, la Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, regula en su artículo 30 la intervención de telecomunicaciones con la asistencia técnica de otro Estado miembro¹³⁵.

¹³³ El mismo precepto establece determinadas cautelas para la aportación de las grabaciones: «[s]e indicará el origen y destino de cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas».

¹³⁴ STC 145/2014, de 22 de septiembre (FJ. 5). También en igual sentido, entre otras, SSTC 126/2000, de 16 de mayo (FJ. 9), y 184/2003, de 23 de octubre (FJ. 12).

¹³⁵ Sobre la intervención transfronteriza de comunicaciones, *vid.* GONZÁLEZ MONJE, A., *Cooperación jurídica internacional en materia penal e intervención de comunicaciones como técnica especial de investigación*, Comares, Granada, 2017; y GONZÁLEZ CANO, M.I. (Dir.), *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, Tirant lo Blanch, Valencia, 2019.

III. CONTENIDO OBJETIVO. EL SECRETO DE LAS COMUNICACIONES EN LAS RELACIONES ENTRE PARTICULARES

Junto al contenido jurídico-subjetivo de los derechos fundamentales, analizado en las páginas precedentes para el caso del derecho al secreto de las comunicaciones, aquéllos poseen además una dimensión objetiva a través de la cual las normas iusfundamentales actúan como principios orientadores del ordenamiento jurídico y de la que se derivan determinadas obligaciones para los poderes públicos.

Nos ocupamos ahora de esta dimensión objetiva del derecho fundamental al secreto de las comunicaciones, desde un triple punto de vista. En primer lugar, en una aproximación breve y de carácter general, tratando de hallar las normas que en nuestro sistema constitucional se han identificado como fundamento de la dimensión objetiva de los derechos fundamentales; en segundo lugar, analizando las consecuencias derivadas de este reconocimiento para el derecho que nos ocupa y, finalmente, deteniéndonos en su posible eficacia en las relaciones entre particulares.

III.1. Fundamentos constitucionales de la dimensión objetiva de los derechos fundamentales

La doctrina de la dimensión objetiva de los derechos fundamentales es construida por la jurisprudencia constitucional alemana en el asunto *Lüth*.

En el caso español, el Tribunal Constitucional no encontró grandes dificultades para hallar fundamentos en el texto constitucional que amparasen la validez de esta doctrina en nuestro ordenamiento.

Así, en el ATC 382/1996, de 18 de diciembre (FJ. 3), el Tribunal afirma que la doble dimensión de los derechos fundamentales «se infiere de un texto constitucional que, tras proclamar el Estado social y democrático de Derecho (art. 1.1 CE), y, por ende, comprometer a los poderes públicos en la promoción de la libertad y la igualdad el individuo (art. 9.2 CE), eleva el libre

desarrollo de la personalidad y el respeto a los derechos de los demás a la condición de fundamento del orden político y de la paz social (art. 10.1 CE)».

En primer lugar, por tanto, se ha entendido que la dimensión objetiva de los derechos se vincula con la fórmula del Estado social y democrático de Derecho (art. 1), en cuanto que viene a identificar la constitución de una comunidad nacional como marco de convivencia humana justa y pacífica en la que los derechos fundamentales se revelan como elementos esenciales¹³⁶.

La definición del Estado como social influye en la significación de los derechos fundamentales que, en tanto componentes básicos y estructurales de aquél, reclaman determinadas actuaciones de los poderes públicos orientadas a la defensa de su plena vigencia en la vida social¹³⁷.

También el art. 1.1 proclama la libertad y la igualdad como valores superiores del ordenamiento. Valores cuya defensa se encomienda a los poderes públicos por el art. 9.2 y que se ven concretados en los diversos derechos fundamentales que la Constitución garantiza. En este sentido se ha considerado que el art. 9.2 contiene un mandato a los poderes públicos que alberga un compromiso especialmente intenso para realizar una política permanente en materia de derechos fundamentales, pues la promoción de la igual libertad implica «asumir una política activa de favorecimiento de su ejercicio efectivo y de creación de las condiciones que lo hagan posible»¹³⁸.

Finalmente, esta dimensión se infiere del art. 10.1 CE, que designa a los derechos fundamentales como «fundamento del orden político y de la paz social» y, en tal medida, sus contenidos irradian todo el ordenamiento.

¹³⁶ STC 25/1981, de 14 de julio (FJ. 5).

¹³⁷ *Vid.*, STC 18/1984, de 7 de febrero (FJ. 6), y CASTILLO CÓRDOVA, L., «Principales consecuencias de la aplicación del principio de la doble dimensión de los derechos fundamentales», *Anuario da Facultade de Dereito da Universidade da Coruña*, 7, 2003, pág. 185.

¹³⁸ MARTÍNEZ PUJALTE, A.L., «El art. 9.2 CE y su significación en el sistema constitucional de derechos fundamentales», *Revista de las Cortes Generales*, 40, 1997, págs. 111-112. En similar sentido, BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 183.

Esta consideración de los derechos no es, por lo demás, exclusiva de nuestro sistema iusfundamental nacional, sino que el sistema de valores que subyace a los mismos se identifica en diversos instrumentos internacionales, pudiendo encontrar afirmaciones similares a la contenida en nuestro art. 10.1 en los preámbulos tanto de la Declaración Universal de Derechos Humanos como del Convenio Europeo de Derechos Humanos¹³⁹.

III.2. Dimensión objetiva del derecho fundamental al secreto de las comunicaciones

De los preceptos citados se induce, así, la consideración de los derechos fundamentales como rasgos esenciales del sistema democrático, de forma que, conjuntamente considerados, trascienden una concepción meramente subjetiva añadiendo a ella una dimensión objetiva¹⁴⁰.

Los derechos fundamentales operan, desde esta significación, como elementos estructurales básicos del ordenamiento objetivo que deben, por ello, ser tenidos en cuenta por los poderes públicos, en un doble sentido.

Por un lado, en tanto que expresión jurídica de un sistema de valores, los derechos fundamentales deben informar el conjunto de la organización jurídica y política. Por otro, su posición principal fundamenta, además de la obligación negativa del Estado de no vulneración, una positiva de promover su eficacia¹⁴¹.

Ambos mecanismos constituyen las dos principales consecuencias del reconocimiento de la dimensión objetiva: el efecto irradiante de los derechos

¹³⁹ SSTC 25/1981, de 14 de julio (FJ. 5), y 21/1981, de 15 de junio (FJ. 10).

¹⁴⁰ STC 245/1991, de 16 de diciembre (FJ. 5). FERNÁNDEZ SEGADO, F., «La teoría jurídica...», *op.cit.*, pág. 207.

¹⁴¹ STC 53/1985, de 11 de abril (FJ. 4).

fundamentales y el deber de su protección por parte de los poderes públicos¹⁴².

A. El efecto irradiante de los derechos fundamentales

Los derechos fundamentales como sistema de principios y valores objetivos poseen una pretensión singular de validez que se proyecta sobre el ordenamiento jurídico en su totalidad¹⁴³.

De esta manera, el derecho fundamental tiñe de su contenido todo el sistema normativo. Como norma de principio, el derecho fundamental debe ser realizado en todas las ramas del ordenamiento, quedando así en cierto modo «constitucionalmente conformadas»¹⁴⁴.

Ello afecta a las labores normativa y aplicativa del Derecho. El legislador debe tener en cuenta el derecho fundamental no sólo para no contravenir su contenido esencial, sino también para tratar de ordenar las relaciones jurídicas de la forma más favorable a su eficacia. Los jueces y magistrados, por su parte, deben controlar que las concretas normas no desconozcan esta dimensión objetiva de los derechos e interpretarlas a favor de los derechos fundamentales en presencia¹⁴⁵.

B. El deber de protección de los derechos fundamentales

El Tribunal Constitucional consideró tempranamente que, del sometimiento de los poderes públicos a la Constitución (art. 9.1) se deriva, además de la obligación negativa de no vulnerar los derechos fundamentales,

¹⁴² SALVADOR MARTÍNEZ, M., «Sobre el contenido objetivo...», *op.cit.*, págs. 202-203.

¹⁴³ GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva...*, *op.cit.*, pág. 73.

¹⁴⁴ SALVADOR MARTÍNEZ, M., «Sobre el contenido objetivo...», *op.cit.*, pág. 203. En similar sentido, CASTILLO CÓRDOVA, L., «Principales consecuencias...», *op.cit.*, pág. 185.

¹⁴⁵ BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, págs. 53-54.

«la obligación positiva de contribuir a la efectividad de tales derechos, y de los valores que representan»¹⁴⁶.

La dimensión positiva obliga, así, al Estado a proteger su contenido jurídico-objetivo y efectividad para que puedan tener vigencia en las relaciones privadas y en la vida social¹⁴⁷.

Ello es propio del carácter de principio objetivo de las normas iusfundamentales¹⁴⁸: mandatos de optimización o normas que ordenan su cumplimiento «en la mayor medida posible»¹⁴⁹.

Como principios objetivos, están dotadas de un alto grado de abstracción a concretar por los poderes públicos a partir de las indicaciones generales deducidas del texto constitucional. De modo que los poderes públicos encuentran en los derechos fundamentales impulsos de actuación en forma de directrices constitucionales disponibles para su concreción normativa o jurisprudencial¹⁵⁰.

¹⁴⁶ SSTC 53/1985, de 11 de abril (FJ. 4), y 26/2018, de 5 de marzo (FJ. 2). «[D]eber que afecta al legislador, al ejecutivo y a los Jueces y Tribunales, en el ámbito de sus funciones respectivas»; STC 18/1984, de 7 de febrero (FJ. 6).

¹⁴⁷ GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva...*, *op.cit.*, pág. 83. Este deber de protección también ha sido reconocido en el ámbito del CEDH a través de las denominadas «obligaciones positivas». El TEDH ha considerado, a partir de una interpretación dinámica de los derechos declarados en el Convenio, que del mismo se derivan determinadas obligaciones positivas para los Estados, consistentes en un deber de actuar para garantizar la efectividad de los derechos incluso en las relaciones entre individuos. Aunque reconoce que, en este aspecto, se debe otorgar a los Estados un amplio margen de discrecionalidad, ha afirmado que «en determinadas circunstancias, el Estado no cumple adecuadamente sus obligaciones positivas [...] a menos que garantice el respeto de las relaciones entre los individuos mediante el establecimiento de un marco normativo que tenga en cuenta los diversos intereses que han de protegerse en un contexto determinado». Cfr. STEDH de 5 de septiembre de 2017 (asunto *Barbulescu c. Rumania*, §118 y 119). *Vid.* igualmente SSTEDH de 26 de marzo de 1985 (asunto *X e Y c. Países Bajos*, §23); 7 de febrero de 2012 (asunto *Von Hannover c. Alemania*, §98); y 16 de julio de 2014 (asunto *Hämäläinen c. Finlandia*, §62); y SALAMANCA AGUADO, E., «El respeto a la vida privada...», *op.cit.*, págs. 20-21, y DI MARTINO, A., «La doppia dimensione...», *op.cit.*, págs. 48 y ss.

¹⁴⁸ SALVADOR MARTÍNEZ, M., «Sobre el contenido objetivo...», *op.cit.*, pág. 204.

¹⁴⁹ ALEXY, R., *Teoría de los derechos fundamentales*, Centro de Estudios Políticos y Constitucionales, Madrid, 1993, pág. 86. También en similar sentido, BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 50.

¹⁵⁰ FERNÁNDEZ SEGADO, F., «La teoría jurídica...», *op.cit.*, pág. 208 y GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva...*, *op.cit.*, págs. 12-13.

Corresponde a los poderes públicos, por tanto, determinar el modo y grado de actuación para la consecución del mandato en las cotas más altas posibles de eficacia del derecho fundamental¹⁵¹.

El legislador, en atención a las competencias que constitucionalmente se le atribuyen, es el principal obligado por este mandato, que debe esforzarse especialmente «allí donde un derecho o valor fundamental quedaría vacío de no establecerse los supuestos para su defensa»¹⁵². Deber que puede, en ocasiones, llevar al legislador a proteger el derecho incluso penalmente, en cuyo caso el Tribunal ha reconocido que «la protección penal forma parte del derecho fundamental mismo»¹⁵³.

El deber de protección también vincula al resto de los poderes públicos en su proceder, debiendo orientarse a la máxima protección posible de los derechos fundamentales en disputa, aunque debe tenerse en cuenta que, sometidos al principio de legalidad, su actuación se halla en ocasiones condicionada a la previa tarea del legislador¹⁵⁴.

Se trata ahora de comprobar en qué medida los poderes públicos han cumplido, para el caso del ordenamiento jurídico español, la obligación de protección respecto del derecho fundamental al secreto de las comunicaciones.

¹⁵¹ BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 183.

¹⁵² STC 53/1985, de 11 de abril (FJ. 4).

¹⁵³ STC 71/1984, de 12 de junio (FJ.2). Se deben hacer dos breves consideraciones. Por un lado, la protección penal no constituye la única solución posible — STEDH de 26 de marzo de 1985 (asunto *X e Y c. Países Bajos*, §24)—, sino que, de preverse, se reserva para los casos más graves, de manera que los derechos fundamentales sustantivos «no encuentran en la acción penal su único ámbito de protección» —STC 26/2018, de 5 de marzo (FJ. 8)—. Por otro lado, no existe para el titular del derecho fundamental vulnerado un derecho a la condena penal del sujeto responsable de la injerencia, sino que simplemente es titular del *ius ut procedatur*, pues «no forma parte del contenido de derecho fundamental alguno la condena penal de quien lo vulnere con su comportamiento»; STC 26/2018, de 5 de marzo (FJ. 3), y las allí citadas.

¹⁵⁴ BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 184.

Esta tarea requiere una consideración previa. La relación entre la dimensión subjetiva y objetiva de los derechos fundamentales, también en el caso del 18.3 CE, es de carácter asimétrico¹⁵⁵.

Cuando el derecho fundamental opera como derecho subjetivo posee un objeto y un contenido estrictamente delimitados, tal y como hemos visto en los capítulos precedentes de este trabajo. Sin embargo, en su dimensión objetiva el contenido del derecho se cifra en un deber genérico de protección, mientras que su objeto, dada la amplitud del precepto constitucional, adquiere una virtualidad muy diversa de su configuración subjetiva¹⁵⁶.

Los ordenamientos contienen normas dirigidas a proteger, conjuntamente, situaciones que frente a los poderes públicos se hallarían protegidas por derechos diversos —como la intimidad y el secreto de las comunicaciones—, o a tutelar escenarios que sobrepasan de algún modo los ámbitos de protección objetivo, subjetivo y temporal del secreto de las comunicaciones tal y como los hemos delimitado *supra*.

Doctrinalmente se ha propuesto una clasificación tripartita del deber de protección de los derechos fundamentales que integraría una obligación de prohibición, una obligación de garantía y una obligación de prevención¹⁵⁷.

La *obligación de prohibición* se dirige a que los poderes públicos impidan vulneraciones de derechos fundamentales por parte de terceros, principalmente mediante la creación y aplicación de normas sancionadoras¹⁵⁸.

A esta finalidad se prestan, en primer lugar, la tipificación penal de los delitos de descubrimiento y revelación de secretos y de determinados delitos

¹⁵⁵ GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva...*, *op.cit.*, pág. 91.

¹⁵⁶ *Vid.* sobre esta cuestión BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, págs. 50-51.

¹⁵⁷ GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva...*, *op.cit.*, pág. 89.

¹⁵⁸ *Ibid.*

cometidos por los funcionarios públicos «contra la inviolabilidad domiciliaria y demás garantías de la intimidad».

Entre los primeros se hallan los previstos en los arts. 197 y siguientes del Código Penal. El tipo básico del art. 197 castiga a quien «para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación». Por su parte, el art. 198 sanciona estas mismas conductas cuando sean cometidas por autoridad o funcionario público «fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo»¹⁵⁹.

En estos casos se aprecia con claridad la aludida asimetría entre las dimensiones subjetiva y objetiva de los derechos. Estos delitos, al igual que el resto de los previstos en el mismo capítulo, se dirigen a proteger conductas que, en su dimensión subjetiva, son subsumibles en los supuestos de hecho que identifican tanto el objeto del derecho a la intimidad como del secreto de las comunicaciones¹⁶⁰. Sin embargo, la dimensión objetiva de ambos reclama simplemente que se prevean mecanismos para su protección frente a vulneraciones de terceros, sin que sea estrictamente necesario realizar una configuración sistemática de los objetos protegidos por los arts. 18.1 y 18.3 CE¹⁶¹.

¹⁵⁹ Vid. ROMEO CASABONA, C.M., *Los delitos de descubrimiento...*, *op.cit.*; OLMO FERNÁNDEZ-DELGADO, L., *El descubrimiento y revelación de secretos...*, *op.cit.*; y RODRÍGUEZ MARÍN, F., «Los delitos de escuchas ilegales y el derecho a la intimidad», *Anuario de derecho penal y ciencias penales*, 43, 1990, págs. 197-240.

¹⁶⁰ FERNÁNDEZ RODRÍGUEZ, J.J., *Secreto e intervención de las comunicaciones...*, *op.cit.*, pág. 168.

¹⁶¹ Da también cuenta de esta protección conjunta la rúbrica del Título bajo la que tales delitos se agrupan: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio».

En similar situación se encuentran los tipos penales previstos en los arts. 535 y 536 CP, que castigan a la autoridad o funcionario público que, mediando causa por delito, pero con violación de las garantías constitucionales o legales, bien intercepte «cualquier clase de correspondencia privada, postal o telegráfica» (art. 535), bien intercepte telecomunicaciones o utilice «artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación» (art. 536), previéndose en ambos casos una agravación de la pena en caso de divulgación de la información obtenida.

También a cumplir esta obligación de prohibición se dirigen las infracciones y sanciones prevista para garantizar la confidencialidad del proceso comunicativo por parte de los prestadores de servicios de comunicaciones.

Así, el art. 59.a) de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal, califica como infracción muy grave el incumplimiento de las obligaciones impuestas a los operadores para garantizar el secreto (art. 5) y la inviolabilidad (art. 6) de la correspondencia.

Igualmente, el art. 76.10 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones considera como infracción muy grave «[l]a interceptación, sin autorización, de telecomunicaciones no destinadas al público en general, así como la divulgación del contenido».

Por su parte, la *obligación de garantía* exige la previsión de mecanismos para evitar perjuicios en los derechos fundamentales, resolviendo colisiones entre derechos o bienes constitucionales o disponiendo acciones judiciales para su protección¹⁶².

¹⁶² GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva...*, op.cit., pág. 89.

Teniendo en cuenta la diferente protección dispensada en el caso de la dimensión objetiva, podría tener cierta virtualidad también en la tutela de los principios que latan en el derecho fundamental al secreto de las comunicaciones, el art. 7.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Este precepto considera como intromisión ilegítima:

«La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción».

La misma consideración podría hacerse sobre el artículo 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que reconoce a los trabajadores el derecho «a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador».

Aunque se refiere expresamente al derecho a la intimidad, no establece diferenciación alguna sobre los contenidos protegidos de entre los albergados por esos dispositivos digitales, siendo este, como es sabido, un escenario de especial conflictividad respecto del derecho fundamental al secreto de las comunicaciones en el ámbito de las relaciones laborales¹⁶³.

Por otro lado, y más allá de lo estrictamente circunscrito al secreto de las comunicaciones, en el ordenamiento jurídico español existen otras normas dirigidas a prever acciones judiciales para garantizar la general indemnidad de los derechos fundamentales.

Este es el caso de la exclusión procesal de las pruebas obtenidas con vulneración de derechos fundamentales. Previsión contenida en el art. 11

¹⁶³ SSTC 241/2012, de 17 de diciembre, y 170/2013, de 7 de octubre.

LOPJ¹⁶⁴, y completada por el art. 287 LEC —aplicable supletoriamente al resto de órdenes procesales—, que regula el procedimiento para declarar la ilicitud de las pruebas de tal modo obtenidas.

También debe considerarse como mecanismo que atiende a la obligación de garantía, en este caso circunscrita al ámbito laboral, la previsión del art. 108.2 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social, que dispone que «[s]erá nulo el despido que [...] se produzca con violación de derechos fundamentales y libertades públicas del trabajador».

Finalmente, la *obligación de prevención* se cumple mediante la adopción de condiciones sobre determinadas conductas con el objetivo de permitir el pleno disfrute del derecho antes de que se produzca lesiones o perjuicios¹⁶⁵.

Para el caso del derecho al secreto de las comunicaciones, en esta obligación, interpretada a contrario, redundaría la permisión del uso de tecnologías de cifrado de procesos comunicativos en la medida en que supone, según se dijo, una garantía técnica para la protección anticipada del objeto del derecho.

III.3. El derecho fundamental al secreto de las comunicaciones en las relaciones entre particulares

Resulta evidente, según vemos, la conexión sucesiva que existe entre dimensión objetiva, deber de protección y eficacia de los derechos fundamentales en las relaciones entre particulares.

Mediante la puesta en marcha de los mecanismos jurídicos dirigidos a cumplir su obligación de protección de los derechos fundamentales propia de

¹⁶⁴ «No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales». Esta norma se reproduce para el proceso laboral en el art. 90.2 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social.

¹⁶⁵ GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva...*, *op.cit.*, pág. 90.

su dimensión objetiva, los poderes públicos garantizan la aplicación de los derechos fundamentales en las relaciones privadas de los individuos.

Tanto las normas de prohibición —tutela penal del secreto de las comunicaciones— como las de garantía —nulidad de pruebas ilícitas o del despido— constituyen mecanismos jurídicos válidos para reaccionar frente a conductas de particulares.

No cabe duda, así, de que el secreto de las comunicaciones está garantizado en nuestro ordenamiento también para el caso de que las injerencias en el mismo provengan de sujetos privados.

En atención a la naturaleza del derecho, a su aptitud para operar en el ámbito de las relaciones privadas y a las posibilidades de su potencial vulneración por los particulares, el derecho fundamental al secreto de las comunicaciones posee una eficacia polivalente o pluridireccional, siendo oponible tanto frente al actuar público como privado¹⁶⁶.

El tenor literal con que la norma iusfundamental se expresa —«se garantiza el secreto de las comunicaciones...»— parece disponer que nadie puede libremente violar el secreto garantizado. Postula una eficacia frente a todos tutelada por el Estado¹⁶⁷.

Esta parece ser también la opción asumida por el Tribunal Constitucional en la Sentencia 114/1984, de 29 de noviembre (FJ. 7), cuando afirma: «la norma constitucional se dirige inequívocamente a garantizar su

¹⁶⁶ Vid. BILBAO UBILLOS, J.M., *La eficacia de los derechos fundamentales frente a particulares. Análisis de la jurisprudencia del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 1997, pág. 355, y, más recientemente, BILBAO UBILLOS, J.M., «La consolidación dogmática y jurisprudencial de la *Drittwirkung*: una visión de conjunto», *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, 21, 2017, pág. 60.

¹⁶⁷ GUTIÉRREZ GUTIÉRREZ, I., «Criterios de eficacia de los derechos fundamentales en las relaciones entre particulares», *Teoría y Realidad Constitucional*, 3, 1999, pág. 198. La eficacia del derecho fundamental al secreto de las comunicaciones frente a particulares es defendida, entre otros autores, por ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 244; y RIDAURA MARTÍNEZ, M.J., «El legislador ausente del artículo 18.3...», *op.cit.*, págs. 355-356. En contra, JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, págs. 56-57.

impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia *erga omnes*) ajenos a la comunicación misma».

No se opone a este entendimiento el hecho de que el inciso final de la norma —«salvo resolución judicial»— se dirija exclusivamente a los poderes públicos¹⁶⁸.

Que el art. 18.3 CE permita que el derecho pueda ser restringido únicamente por un poder público (salvo resolución judicial) no significa que el objeto protegido (el secreto de las comunicaciones) lo sea solo frente a ellos, sino que la Constitución atribuye una competencia a la autoridad pública que no se reconoce a los sujetos privados¹⁶⁹.

El problema de la eficacia del derecho al secreto de las comunicaciones entre particulares es por tanto un problema de límites en sentido amplio¹⁷⁰.

Como vimos, cuando opera como derecho público subjetivo la Constitución habilita al poder público para excepcionar la garantía de secreto mediante resolución judicial. Y en tal caso, el límite —ahora en sentido estricto— encuentra fundamento en bienes constitucionalmente protegidos de interés público.

¹⁶⁸ Así parece entenderlo el Tribunal Constitucional pues, cuando ha enjuiciado injerencias en este derecho provenientes de particulares —SSTC 241/2012, de 17 de diciembre y 170/2013, de 7 de octubre— ni siquiera se ha planteado la ausencia de resolución judicial, que en caso de intervención de un poder público supondría la concesión casi automática del amparo, sino que ha entrado directamente a ponderar los derechos en conflicto. De la misma opinión es JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *op.cit.*, pág. 56. Por el contrario, ZOCO ZABALA considera que la garantía de resolución judicial también opera en las relaciones privadas; cfr. ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, *op.cit.*, pág. 239. También en similares términos se expresa la STS, Sala de lo Penal, de 16 de junio de 2014 (FJ. 1). Considera que el art. 18.3 es claro y tajante en la exigencia de resolución judicial y «[n]o contempla, por tanto, ninguna posibilidad ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado ("*correo corporativo*")», para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia». Cursivas en el original.

¹⁶⁹ PACE, A., *Problematika delle libertà costituzionali. Parte Generale*, CEDAM, Padova, 2003, pág. 19.

¹⁷⁰ BILBAO UBILLOS, J.M., «La consolidación dogmática...», *op.cit.*, pág. 61.

Por el contrario, los particulares no se hallan habilitados para limitar de tal modo el derecho, por lo que, en las relaciones jurídico privadas, el problema se presenta como una colisión de derechos fundamentales, que se ven mutuamente *delimitados*¹⁷¹.

De esta forma ha venido resolviendo el Tribunal Constitucional la injerencia del empresario en el secreto de las comunicaciones del trabajador:

«La controversia a resolver versa, por tanto, sobre la necesaria delimitación de bienes e intereses de relevancia constitucional en el marco de las relaciones laborales: los derechos del trabajador a la intimidad y al secreto de las comunicaciones (arts. 18.1 y 18.3 CE) y el poder de dirección del empresario»¹⁷².

Pero también ha transitado este camino en otros casos. La STC 34/1996, de 11 de marzo, resuelve la alegada vulneración de distintos derechos fundamentales en un proceso penal por un delito de revelación de secretos. El recurrente, periodista, había interceptado determinadas comunicaciones telefónicas mantenidas entre un empresario y un funcionario cuyo contenido fue publicado en prensa al día siguiente. La solución pasa, para el Tribunal Constitucional, por la ponderación:

«Una vez despejadas las dos incógnitas previas, que no eran sino la identificación de los derechos fundamentales en juego [*libertades informativas y secreto de las comunicaciones*], el paso siguiente habrá de ser la ponderación de uno y otro, en el ámbito de nuestra Constitución»¹⁷³.

¹⁷¹ «[...] en un conflicto jurídico entre privados todos los interesados gozan de la protección de los derechos fundamentales, mientras que en la relación del ciudadano con el Estado tal tutela no corresponde al poder público. Pero si los derechos fundamentales actúan en favor y en contra de todos los que toman parte en una relación jurídico-privada, se producirá ordinariamente una colisión de derechos fundamentales. En caso de conflicto, al Derecho Civil le corresponde así la tarea, sumamente complicada, de encontrar por sí mismo el modo y la intensidad de la influencia de los derechos fundamentales mediante el equilibrio o la ponderación de los derechos fundamentales que entran en consideración». *Vid.* HESSE, K., *Derecho Constitucional y Derecho Privado*, Civitas, Madrid, 1995, págs. 45 y ss.

¹⁷² STC 170/2013, de 7 de octubre (FJ. 3).

¹⁷³ STC 34/1996, de 11 de marzo (FJ. 4).

Además, los particulares se desenvuelven en el tráfico privado en una multitud de relaciones jurídicas en las que ocupan diversas posiciones que no son siempre igualitarias. En tal medida, no parece apropiado considerar que la eficacia de los derechos fundamentales deba ser homogénea en todas ellas¹⁷⁴. Así, los derechos fundamentales tienden a reequilibrar una relación que es, en principio, asimétrica¹⁷⁵.

Por ello, se ha propuesto una aplicación de la *Drittwirkung* que tenga en cuenta el desequilibrio en que las partes se encuentran en las relaciones jurídico-privadas, con fundamento análogo al origen del reconocimiento de los derechos fundamentales como derechos públicos subjetivos. Los derechos fundamentales no desplegarían, así, su eficacia únicamente frente al poder público, sino frente a todo tipo de poder¹⁷⁶.

En tal medida, se trata de distinguir entre una eficacia horizontal genérica más limitada y una eficacia específica, y de mayor intensidad, en aquellos casos en que una de las partes ostente una posición claramente dominante. De este modo, la eficacia de los derechos fundamentales frente a particulares, aun modulada por la autonomía privada de los individuos, deberá ser más intensa cuando operen en relaciones no igualitarias¹⁷⁷. Un escenario, por lo demás, propio de las relaciones laborales, lo que explica que éste haya sido el escenario más fecundo de aplicación de la doctrina de la *Drittwirkung*¹⁷⁸.

¹⁷⁴ Así, GUTIÉRREZ GUTIÉRREZ, I., «Criterios de eficacia...», *op.cit.*, pág. 194; y BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 102.

¹⁷⁵ QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T., *El recurso de amparo y los derechos fundamentales en las relaciones entre particulares*, Civitas, Madrid, 1981, págs. 70 y ss.; y BILBAO UBILLOS, J.M., «La consolidación dogmática...», *op.cit.*, pág. 50.

¹⁷⁶ BILBAO UBILLOS, J.M., *La eficacia de los derechos fundamentales...*, *op.cit.*, págs. 368-369; y GUTIÉRREZ GUTIÉRREZ, I., «Criterios de eficacia...», *op.cit.*, pág. 204.

¹⁷⁷ BILBAO UBILLOS, J.M., «La consolidación dogmática...», *op.cit.*, pág. 63; y BASTIDA FREIJEDO, F. *et al.*, *Teoría general de los derechos fundamentales...*, *op.cit.*, pág. 193.

¹⁷⁸ «[...] la jurisprudencia de este Tribunal ha insistido reiteradamente en la plena efectividad de los derechos fundamentales del trabajador en el marco de la relación laboral, ya que ésta no puede implicar en modo alguno la privación de tales derechos para quienes prestan servicio en las organizaciones productivas, que no son ajenas a los principios y derechos constitucionales que informan el sistema de relaciones de trabajo»; STC 98/2000, de 10 de abril (FJ. 6).

En la relación laboral, el empresario es titular de los derechos fundamentales a la propiedad privada (art. 33) y la libertad de empresa (art. 38). Derechos que, en ambos casos, están vinculados expresamente *ex constitutione* a determinados intereses generales: la función social en el caso del primero y el modelo constitucional de economía en el segundo¹⁷⁹.

Por ello, en la medida en que estos derechos sirven a una función constitucionalmente relevante o a otros derechos fundamentales —la libertad de empresa sirve también al derecho al trabajo— pueden configurarse como poderes y afectar a derechos ajenos: el poder de dirección del empresario, normativamente reconocido, puede afectar a los derechos fundamentales del trabajador¹⁸⁰.

La colisión de derechos que se produce en estos casos es especialmente importante en la medida en que uno de los sujetos de la relación está habilitado para imponer sanciones (el despido disciplinario) y para imponer reglas que pueden incidir en derechos fundamentales y cuyo incumplimiento puede determinar la imposición de sanciones¹⁸¹.

Este ha sido el escenario de mayor conflictividad del derecho fundamental al secreto de las comunicaciones en la empresa: el desvelo del secreto por parte del empresario para comprobar el cumplimiento de las reglas de uso de los dispositivos de titularidad empresarial (ordenadores, teléfonos, ...) ¹⁸².

¹⁷⁹ También en el caso de las asociaciones, el derecho de la asociación sirve al derecho de los socios y a los fines de la misma, que en ocasiones se hallan a su vez vinculados con otros derechos fundamentales, como sucede con los derechos de participación en el caso de los partidos políticos. Por ello, la misma solución de ponderación entre derechos se ha dado en estos casos. *Vid.* STC 26/2018, de 5 de marzo, en la que se analiza la intervención de comunicaciones de correo electrónico de un afiliado por parte del partido.

¹⁸⁰ GUTIÉRREZ GUTIÉRREZ, I., «Criterios de eficacia...», *op.cit.*, págs. 204-205.

¹⁸¹ *Ibid.*, pág. 206.

¹⁸² *Vid.* OCÓN GARCÍA, J., «La incidencia de las resoluciones del TEDH...», *op.cit.*, págs. 267 y ss.; ELVIRA PERALES, A., «¿Qué hay de nuevo en torno al derecho ...?», *op.cit.*, págs. 607 y ss.; VILLALBA SÁNCHEZ, A., «Los derechos fundamentales del trabajador frente a los nuevos instrumentos de control empresarial», *Revista Derecho Social y Empresa*, 6, 2016, págs. 86-105; y MARTÍNEZ ALARCÓN, M. L., «El control de las comunicaciones electrónicas

que los trabajadores realizan a través de las herramientas informáticas de la empresa», RUBIO LLORENTE, F., JIMÉNEZ CAMPO, J., SOLOZABAL ECHAVARRÍA, J. J., BIGLINO CAMPOS, P. y GÓMEZ MONTORO, A. (Coords.), *La Constitución política de España. Estudios en homenaje a Manuel Aragón Reyes*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, págs. 725-745.

CONCLUSIONES

PRIMERA

El artículo 18.3 de la Constitución española de 1978 garantiza el derecho fundamental al secreto de las comunicaciones.

Un derecho autónomo al servicio de bienes y valores jurídicos que encuentran garantía y protección en objetos de diversos derechos fundamentales próximos, pero diversos.

Se trata de un derecho dirigido a descartar los riesgos propios de los procesos comunicativos a través de medios técnicos y, en su caso, de la necesaria participación de un tercero. El derecho tutela la privacidad, el buen curso de la comunicación y, muy principalmente, la confianza de su titular en el tercero prestador del servicio.

La garantía iusfundamental se disocia así del contenido comunicado. De modo que el secreto posee naturaleza formal. Y protege el proceso comunicativo en su totalidad: conocimiento de su existencia, contenido u otras circunstancias del proceso.

SEGUNDA

El objeto del derecho fundamental se configura como prohibición a los poderes públicos. El art. 18.3 CE veda la intervención de las comunicaciones mediante su secreto y, de este modo, las asegura exentas de injerencias no autorizadas o consentidas.

Tal prohibición no es absoluta, sino sujeta a excepciones.

La norma se estructura a partir de dos proposiciones típicas comunes a todos los ordenamientos: garantía de secreto y posibilidad de su levantamiento judicial.

El contenido del derecho consiste en la facultad de reaccionar frente al incumplimiento de la prohibición o frente a la inobservancia de las condiciones constitucionalmente previstas para excepcionarla.

TERCERA

El espacio de autodeterminación viene delimitado por los conceptos de «comunicación» y «secreto».

A falta de definición expresa, el concepto de comunicación del art. 18.3 CE resulta de la concurrencia del concepto de secreto, de las características comunes a los medios expresamente aludidos en el precepto, y de los bienes y valores jurídicos fundamento del derecho.

Las comunicaciones con garantía de secreto consisten en un intercambio de expresiones de sentido, entre personas determinadas y mediante soportes que permiten su transmisión en canal cerrado.

CUARTA

La determinabilidad de los destinatarios es precondition del secreto y distingue los procesos comunicativos del 18.3 CE de otros dirigidos a audiencias no determinables, objeto de las libertades comunicativas del art. 20 CE.

En otros casos, el encaje iusfundamental se alcanzará mediante las reglas de conmutabilidad de roles en la relación comunicativa y capacidad de selección del destinatario o direccionamiento de la comunicación.

Las comunicaciones protegidas son las soportadas por medio técnico, únicas en que la garantía formal de secreto cobra sentido, neutralizando los riesgos asociados a la función del tercero intermediario.

QUINTA

La eficacia temporal del derecho no alcanza a todas las fases del proceso comunicativo: se ciñe a aquellas en que la vulnerabilidad asociada a la dependencia técnica del tercero requiere la garantía formal de secreto.

En comunicaciones bidireccionales simultáneas, la garantía de secreto nace con la activación del soporte por el emisor y cesa con su desactivación por ambos intervinientes.

En comunicaciones unidireccionales de tracto alternativo, el secreto opera desde que el emisor cede el control de la comunicación al tercero prestador y hasta su recuperación por el destinatario con la recepción del mensaje. Esta regla opera como variable independiente de la toma de conocimiento del contenido: no considera el momento de su acceso al contenido ni el de la apertura de la comunicación.

Desactivado el soporte o recibido el mensaje los registros resultantes del proceso comunicativo devienen datos estáticos ajenos al objeto de este derecho.

SEXTA

El concepto de secreto de nuestro ordenamiento jurídico reconoce un dominio del conocimiento y una facultad de exclusión de acceso de terceros: siempre al servicio de bienes y valores jurídicos constitucionales.

En el art. 18.3 CE el secreto es un atributo jurídico de los procesos comunicativos a través de medio técnico. Por ello no es posible condicionar el secreto a contenido material alguno, pues su comprobación requeriría

desactivarlo. El secreto posee carácter formal y se protege con independencia de que el mensaje sea íntimo, no exista o no llegue a ser transmitido.

El ámbito objetivo del secreto se predica del proceso comunicativo en todos sus aspectos: existencia, contenido y datos asociados (circunstancias del proceso, fecha, duración o identificación de los medios utilizados).

Desde un punto de vista subjetivo, el secreto, como límite al conocimiento ajeno, no opera entre los comunicantes. Tampoco frente al prestador del servicio en los datos precisos a su función, sobre los que rige un deber de confidencialidad del que, no obstante, puede ser dispensado con arreglo a norma jurídica habilitante.

SÉPTIMA

El bien protegido por el secreto en el art. 18.3 CE es la libertad de las comunicaciones. Pero tal libertad no se identifica con un derecho prestacional al medio o servicio ni con una libertad universal y general de comunicación, más próxima al objeto del derecho a la libre expresión.

Invocar una pretendida libertad de las comunicaciones como cláusula de prohibición de alterar su normal curso sólo sería eficaz previa desactivación de dicho secreto, incurriendo en una injerencia en el derecho fundamental. Así concebida impondría vulnerar el derecho como precondition de su protección.

La libertad de las comunicaciones, como bien jurídico tutelado por el art. 18.3 CE, consiste llanamente en asegurar el secreto. La garantía formal de inmunidad frente a indagaciones ajenas permite a los comunicantes entablar procesos comunicativos libres: ese es, cabalmente, el único modo posible.

OCTAVA

La generalización del uso de técnicas de cifrado en procesos comunicativos supone un reto para el derecho fundamental al secreto de las comunicaciones.

Criptografía y derecho fundamental mantienen una relación ambivalente: refuerza el secreto mediante la garantía técnica de inaccesibilidad al contenido comunicado, pero dificulta su legítima desactivación en los casos constitucionalmente habilitados.

El cifrado no forma parte del contenido esencial del derecho fundamental al tratarse de un instrumento más al servicio de la eficacia del secreto preservado.

Por tanto, la decisión política sobre la regulación del recurso a la criptografía es de oportunidad; y hasta el límite del respeto de la dimensión objetiva del sistema iusfundamental que la Constitución configura.

En tal sentido, se propone:

1. El rechazo de su prohibición absoluta como técnica de protección del secreto.
2. Su uso mediante protocolos descriptores de los supuestos de acceso y desactivación de la protección encriptada de una comunicación concreta.
3. Los supuestos podrían consistir, en el estado actual del conocimiento científico tecnológico, en el recurso a técnicas desactivadoras mediante suplantación, criptoanálisis, registro remoto y establecimiento de deberes de colaboración de terceros
4. Los instrumentos anteriores son preferibles, en atención a los bienes jurídicos en juego del art. 18.3 CE, al establecimiento de una regulación general de los elementos internos de los sistemas de cifrado, como sucede en el régimen de depósito y recuperación de claves.

NOVENA

La mera activación de un proceso comunicativo origina, con independencia de contenido y resultado, un conjunto de datos técnicos: indicativos del origen y destino de la comunicación, encaminamiento, datos temporales, volumen de la información transmitida y tipo de comunicación.

Estos datos de tráfico se suman a los que el proveedor de servicios posee como resultado de la relación contractual que mantiene con su cliente y que son ajenos al proceso de comunicación concreto.

Pues bien, sólo los primeros —datos de tráfico de la comunicación concreta— forman parte del objeto del derecho al secreto de las comunicaciones; y sólo cuando nacen y permanecen como parte indisociable del proceso comunicativo en curso.

El acceso a datos de tráfico de comunicaciones finalizadas, y por tanto obrantes en los dispositivos de los comunicantes o en poder del prestador del servicio de comunicaciones, en correcto cumplimiento del deber legal de conservación, excede del objeto del art. 18.3 CE. Su tutela podrá corresponder, en su caso, a otros derechos como la intimidad o la protección de datos de carácter personal.

DÉCIMA

El secreto de las comunicaciones no posee carácter absoluto, sino que incluye un espacio de injerencia constitucionalmente conforme.

La posibilidad de levantar el secreto de las comunicaciones constituye un límite al ejercicio del derecho fundamental previsto en el art. 18.3 CE. Pese a que la literalidad del precepto solo alude al órgano judicial, se trata de una habilitación de segundo grado que requiere previa intervención del legislador para regular su procedimiento y presupuestos.

Además del respeto al contenido esencial del derecho, la ley debe satisfacer criterios de previsibilidad y precisión en el desarrollo del límite, con fundamento en un bien o interés jurídico constitucionalmente legítimo.

Por su parte, la decisión judicial de intervención de comunicaciones deberá atender, además de a los presupuestos normativos dispuestos, a un escrutinio de proporcionalidad.

UNDÉCIMA

La obligación de contribuir a la eficacia del derecho fundamental al secreto de las comunicaciones, derivada de su dimensión objetiva, exige de los poderes públicos la protección de su contenido jurídico-objetivo en la vida social.

Se despliega a través de normas que sancionan penal, civil y administrativamente la intervención de comunicaciones privadas por parte de particulares, incluida la nulidad radical del acto vulnerador y sus efectos.

Los particulares no están habilitados para limitar el secreto de las comunicaciones, por lo que, en las relaciones privadas, el acceso a comunicaciones ajenas se presenta como un problema de colisión de derechos fundamentales o bienes constitucionalmente protegidos que se ven mutuamente delimitados (propiedad privada, libertad de empresa, patria potestad, ...).

La eficacia del derecho fundamental al secreto de las comunicaciones en las relaciones entre particulares deberá ser mayor en aquellas donde una parte ostenta una posición dominante, como sucede especialmente en la relación laboral.

BIBLIOGRAFÍA

ALÁEZ CORRAL, B., *Minoría de edad y derechos fundamentales*, Tecnos, Madrid, 2003.

ALEXY, R., *Teoría de los derechos fundamentales*, Centro de Estudios Políticos y Constitucionales, Madrid, 1993.

ALONSO PÉREZ, F., *Intervención de las comunicaciones postales, telegráficas y telefónicas*, Dykinson, Madrid, 2001.

ANCOS FRANCO, H., «El tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones. Comentario a la Consulta 1/1999 de la Fiscalía General del Estado», *Diario La Ley*, 4812, 1999, págs. 1-9.

ASSCHER, L.F., *Communicatiegrondrechten: een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, University of Amsterdam, Amsterdam, 2002 (*Tesis Doctoral. Summary*).

BAHAMONDE, A., *Las comunicaciones del siglo XIX al XX. Correo, telégrafo y teléfono*, Santillana, Madrid, 1996.

- BALLESTEROS MOFFA, L.A., «La difícil situación de la Ley 25/2007 de conservación y cesión de datos de tráfico y localización en las comunicaciones electrónicas: la “tala” de su base comunitaria y los desfavorables vientos desde sus homólogas europeas», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 44, 2017, págs. 1-26.
- BAJO FERNÁNDEZ, M., «El secreto profesional en el proyecto de Código penal», *Anuario de derecho penal y ciencias penales*, Tomo 33, 3, 1980, págs. 595-610.
- BASTIDA FREIJEDO, F., VILLAVERDE MENÉNDEZ, I., REQUEJO RODRÍGUEZ, P., PRESNO LINERA, M.A., ALÁEZ CORRAL, B., FERNÁNDEZ SARASOLA, I., *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, 2004.
- BELDA PÉREZ-PEDRERO, E., «El derecho al secreto de las comunicaciones», *Parlamento y Constitución*, 2, 1998, págs. 169-194.
- BILBAO UBILLOS, J.M., *La eficacia de los derechos fundamentales frente a particulares. Análisis de la jurisprudencia del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 1997.
- BILBAO UBILLOS, J.M., «La consolidación dogmática y jurisprudencial de la *Drittwirkung*: una visión de conjunto», *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, 21, 2017, págs. 43-74.
- BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, Dykinson, Madrid, 2004.

- CARRILLO, M., «Los ámbitos del derecho a la intimidad en la sociedad de la comunicación», AA.VV., *El derecho a la privacidad en un nuevo entorno tecnológico*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, págs. 11-70.
- CARUSO, C., «La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale», *Forum di Quaderni Costituzionali*, 10, 2013, págs. 1-24.
- CASANOVA MARTÍ, R., «La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos», *Diario La Ley*, 8674, 2016, págs. 1-14.
- CASARES SÁNCHEZ, J., *Diccionario Ideológico de la Lengua Española*, Editorial Gustavo Gili, Barcelona, 1990.
- CASTILLO CÓRDOVA, L., «Principales consecuencias de la aplicación del principio de la doble dimensión de los derechos fundamentales», *Anuario da Facultade de Dereito da Universidade da Coruña*, 7, 2003, págs. 183-195.
- CATALÁ I BAS, A., «La problemática adecuación de la legislación española sobre escuchas telefónicas a las exigencias del Convenio Europeo de Derechos Humanos y sus consecuencias», *Revista del Poder Judicial*, 66, 2002, págs. 13-71.
- CATALÁ I BAS, A., «Sentencia del Tribunal Europeo de Derechos Humanos Prado Bugallo c. España de 18 de febrero de 2003», *Revista Europea de Derechos Fundamentales*, 1, 2003, págs. 127-135.
- CATALÁ I BAS, A., «Escuchas telefónicas: un encuentro con el Tribunal Constitucional y un desencuentro con el legislador español», *Revista Europea de Derechos Fundamentales*, 15, 2010, págs. 279-294.

- CATALÁ I BAS, A., «Diálogo entre tribunales y creación de un sistema europeo de derechos humanos abierto en red», *Revista Europea de Derechos Fundamentales*, 28, 2016, págs. 13-47.
- CERVINI, R., «El elemento estatutario del secreto como instrumento de efectiva realización de las garantías», *Revista de Derecho: Publicación de la Facultad de Derecho de la Universidad Católica de Uruguay*, 1, 2006, págs. 55-81.
- CHUECA RODRÍGUEZ, R., «Debilidades estructurales del derecho fundamental», CHUECA RODRÍGUEZ, R. (Dir.), *Las fronteras de los derechos fundamentales en la constitución normativa*, Centro de Estudios Políticos y Constitucionales, Madrid, 2019, págs. 23-52.
- CLEMENTE GALLARDO, J., «Computación y comunicación cuánticas», *Matematicalia. Revista digital de divulgación matemática*, 4-5, 2007, págs. 1-8.
- COLOMER HERNÁNDEZ, I., «Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016», RUDA GONZÁLEZ, A. y JEREZ DELGADO, C. (Dir.), *Estudios sobre Jurisprudencia Europea. Materiales del I y II Encuentro anual del Centro español del European Law Institute*, Sepin, Madrid, 2018, págs. 767-781.
- COSTANZO, P., «Le intercettazioni delle comunicazioni interpersonali (un vademecum costituzionale)», *Consulta Online*, 2, 2016, págs. 231-240.
- CRUZ VILLALÓN, P., «Formación y evolución de los derechos fundamentales», *Revista Española de Derecho Constitucional*, 25, 1989, págs. 35-62.

- CRUZ VILLALÓN, P., «Dos cuestiones de titularidad de derechos: los extranjeros, las personas jurídicas», *Revista Española de Derecho Constitucional*, 35, 1992, págs. 63-83.
- CRUZ VILLALÓN, P. y PARDO FALCÓN, J., «Los derechos fundamentales en la Constitución Española de 1978», *Boletín Mexicano de Derecho Comparado*, 97, 2000, págs. 65-154.
- DE ASÍS ROIG, A.E., «Artículo 36», GARCÍA DE ENTERRÍA, E. y DE LA QUADRA-SALCEDO, T. (Coords.), *Comentarios a la Ley General de Telecomunicaciones. Ley 32/2003, de 3 de noviembre*, Civitas, Madrid, 2004, págs. 560-602.
- DI MARTINO, A., «La doppia dimensione dei diritti fondamentali», *Rivista del Gruppo di Pisa*, 2, 2016, págs. 1-63.
- DÍAZ LEMA, J.M., «¿Tienen derechos fundamentales las personas jurídico-públicas?», *Revista de Administración Pública*, 120, 1989, págs. 79-126.
- DÍAZ MARTÍNEZ, M., «La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos», DÍAZ MARTÍNEZ, M. y LÓPEZ-BARAJAS PEREA, I. (Coords.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant Lo Blanch, Valencia, 2018, págs. 85-112.
- DÍAZ REVORIO, F.J., «El derecho fundamental al secreto de las comunicaciones», *Derecho PUCP. Revista de la Facultad de Derecho*, 59, 2006, págs. 159-175.
- ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, Iustel, Madrid, 2007.

ELVIRA PERALES, A., «¿Qué hay de nuevo en torno al derecho al secreto de las comunicaciones?», AA.VV., *La Constitución política de España. Estudios en homenaje a Manuel Aragón Reyes*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, págs. 601-615.

ELVIRA PERALES, A., «Derecho al secreto de las comunicaciones», MATÍA PORTILLA, F.J. y LÓPEZ DE LA FUENTE, G. (Dirs.), *De la intimidad a la vida privada y familiar. Un derecho en construcción*, Tirant Lo Blanch, Valencia, 2019, págs. 115-140.

ETXEBERRÍA GURIDI, J.F., «La previsión legal y las diligencias de investigación restrictivas de derechos fundamentales (A propósito de la STC 49/1999 de 5 de abril)», *Diario La Ley*, 4215, 1999, págs. 1-27.

ETZIONI, A., «Apple: Good Business, Poor Citizen?», *Journal of Business Ethics*, 151, 2018, págs. 1-11.

FASSBENDER, B., «El principio de proporcionalidad en la jurisprudencia del Tribunal Europeo de Derechos Humanos», *Cuadernos de Derecho Público*, 5, 1998, págs. 51-73.

FERNÁNDEZ GARCÍA, J.J., «Inviolabilidad y secreto de la correspondencia», *Revista Española de Derecho Administrativo*, 39, 1983, págs. 557-574.

FERNÁNDEZ RODRÍGUEZ, J.J., *Secreto e intervención de las comunicaciones en internet*, Civitas, Madrid, 2004.

FERNÁNDEZ RODRÍGUEZ, J.J., «La intervención de las comunicaciones digitales: a propósito del sistema SITEL», FERNÁNDEZ RODRÍGUEZ, J.J., SANSÓ-RUBERT PASCUAL, D., PULIDO GRAJERA, J., MONSALVE, R. (Coords.), *Cuestiones de inteligencia en la sociedad contemporánea*, Ministerio de Defensa, Madrid, 2012, págs. 61-75.

- FERNÁNDEZ RODRÍGUEZ, J.J., «Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente», *Revista Española de Derecho Constitucional*, 108, 2016, págs. 93-122.
- FERNÁNDEZ SEGADO, F., «Naturaleza y régimen legal de la suspensión general de los derechos fundamentales», *Revista de derecho político*, 18-19, 1983, págs. 31-58.
- FERNÁNDEZ SEGADO, F., «La teoría jurídica de los derechos fundamentales en la doctrina constitucional», *Revista Española de Derecho Constitucional*, 39, 1993, págs. 195-250.
- FRÍGOLS BRINES, E., «La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías», BOIX REIG, J. (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, págs. 37-91.
- GALINDO AYUDA, F., «La conveniencia de una regulación española del cifrado de las comunicaciones electrónicas», *Diario La Ley*, 4708, 1999, págs. 1-6.
- GARCÍA RUÍZ, J.M., «Correo electrónico y proceso penal», *Diario La Ley*, 5805, 2003, págs. 1-19.
- GAVARA DE CARA, J.C., *La proyección interna de la dimensión objetiva de los derechos fundamentales: el art. 10.1 CE*, Bosch, Barcelona, 2011.
- GIANFRANCESCO, E., «Profili ricostruttivi della libertà e segretezza di corrispondenza e comunicazione», *Diritto e società*, 2, 2008, págs. 219-249.

- GÓMEZ DE LIAÑO FONSECA-HERRERO, M., «El uso de dispositivos electrónicos de captación de comunicaciones en operaciones de infiltración policial», DÍAZ MARTÍNEZ, M. y LÓPEZ-BARAJAS PEREA, I. (Coords.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant Lo Blanch, Valencia, 2018, págs. 205-233.
- GÓMEZ DE SILVA, G., *Breve diccionario etimológico de la lengua española*, México: Fondo de Cultura Económica, México D.F., 1998.
- GÓMEZ MONTORO, A.J., «La titularidad de derechos fundamentales por personas jurídicas (análisis de la jurisprudencia del Tribunal Constitucional español)», *Cuestiones constitucionales*, 2, 2000, págs. 23-71.
- GÓMEZ MONTORO, A.J., «Artículo 39», REQUEJO PAGÉS, J.L. (Coord.), *Comentarios a la Ley Orgánica del Tribunal Constitucional*, Tribunal Constitucional – Boletín Oficial del Estado, Madrid, 2001, págs. 578-608.
- GONZÁLEZ CANO, M.I. (Dir.), *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, Tirant lo Blanch, Valencia, 2019.
- GONZÁLEZ-CUÉLLAR SERRANO, N. y MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna, Madrid, 2015.
- GONZÁLEZ LÓPEZ, J.J., «La retención de datos de tráfico de las comunicaciones en la Unión Europea: una aproximación crítica», *Diario La Ley*, 6456, 2006, págs. 1-13.
- GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal*, La Ley, Madrid, 2007.

- GONZÁLEZ LÓPEZ, J.J., «Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones», *Revista General de Derecho Procesal*, 16, 2008, págs. 1-38.
- GONZÁLEZ LÓPEZ, J.J., «Consideraciones acerca de las dificultades conceptual e iusfundamental planteadas por los datos de las comunicaciones electrónicas en la investigación penal», CABEZUDO RODRÍGUEZ, N. (Coord.), *Inclusión digital: perspectivas y experiencias*, 2011, Universidad de Zaragoza, Zaragoza, págs. 151-180.
- GONZÁLEZ MONJE, A., *Cooperación jurídica internacional en materia penal e intervención de comunicaciones como técnica especial de investigación*, Comares, Granada, 2017.
- GONZÁLEZ NAVARRO, B.A., «Criptología y libertades públicas», *Cuadernos de Derecho Judicial. Internet y derecho penal*, 10, 2001, págs. 145-237.
- GONZÁLEZ NAVARRO, A., «Medios tecnológicos de investigación en el proceso penal alemán: una visión comparada», DÍAZ MARTÍNEZ, M. y LÓPEZ-BARAJAS PEREA, I. (Coords.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant Lo Blanch, Valencia, 2018, págs. 234-283.
- GÓRRIZ ROYO, «Investigaciones prospectivas y secreto de las comunicaciones: respuestas jurídicas», GONZÁLEZ CUSSAC, J.L. y CUERDA ARNAU, M.L. (Dir.), *Nuevas amenazas a la seguridad nacional: Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Tirant Lo Blanch, Valencia, 2013, págs. 243-283.

- GRIMA LIZANDRA, V., «Secreto profesional del abogado y derecho de defensa penal», BOIX REIG, J. (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, págs. 199-229.
- GUERRERO PICÓ, M.C., «Protección de datos personales e Internet: la conservación indiscriminada de los datos de tráfico», *Revista de la Facultad de Derecho de la Universidad de Granada*, 8, 2005, págs. 109-139.
- GUTIÉRREZ GUTIÉRREZ, I., «Criterios de eficacia de los derechos fundamentales en las relaciones entre particulares», *Teoría y Realidad Constitucional*, 3, 1999, págs. 193-211.
- HERNÁNDEZ DOMÍNGUEZ, J.J., «Apertura de paquetes postales. Alcance del secreto de las comunicaciones», *Diario La Ley*, 8265, 2014, págs. 1-12.
- HERNÁNDEZ DOMÍNGUEZ, J.J. y MARTÍNEZ MARTÍN J.I., *Secreto de las Comunicaciones. Alcance de protección constitucional de su interpretación y casuística*, Dilex, Madrid, 2015.
- HERNÁNDEZ GUERRERO, F.J., «La intervención de las comunicaciones electrónicas», *Estudios Jurídicos del Ministerio Fiscal*, 3, 2001, págs. 313-461.
- HESSE, K., *Derecho Constitucional y Derecho Privado*, Civitas, Madrid, 1995.
- ITALIA, V., *Libertà e segretezza della corrispondenza e delle comunicazioni*, Giuffrè, Milán, 1963.

- JIMÉNEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», *Revista Española de Derecho Constitucional*, 20, 1987, págs. 35-82.
- JIMÉNEZ CAMPO, J., «Qué hacer con la ley inconstitucional», AA.VV., *La sentencia sobre la constitucionalidad de la Ley. Actas de las II Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Tribunal Constitucional – Centro de Estudios Constitucionales, Madrid, 1997, págs. 15-79.
- JIMÉNEZ CAMPO, J., *Derechos fundamentales. Concepto y garantías*, Trotta, Madrid, 1999.
- JOVE VILLARES, D., «*Quo vadis*, intimidad?», AA.VV., *Setenta años de Constitución Italiana y cuarenta años de Constitución Española*, Vol. II, Boletín Oficial del Estado – Centro de Estudios Políticos y Constitucionales, Madrid, 2020, págs. 151-165.
- LASAGABASTER, I., «Derechos fundamentales y personas jurídicas de derecho público», AA.VV., *Estudios sobre la Constitución Española. Homenaje al profesor Eduardo García de Enterría*, Vol. 2, Civitas, Madrid, 1991, págs. 651-674.
- LAZCANO BROTONS, I., *El secreto profesional en el periodismo*, Lete Argitaletxea, Bilbao, 2007.
- LLORIA GARCÍA, P., «El secreto de las comunicaciones: su interpretación en el ámbito de los delitos cometidos a través de Internet. Algunas consideraciones», BOIX REIG, J. (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, págs. 171-198.

LÓPEZ-BARAJAS PEREA, I., «El deber de conservación de datos en la Unión Europea y sus límites», *Revista de Derecho de la Unión Europea*, 16, 2009, págs. 195-220.

LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, La Ley, Madrid, 2011.

LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la medida», *Revista de Derecho Político*, 98, 2017, págs. 91-119.

LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», DÍAZ MARTÍNEZ, M. y LÓPEZ-BARAJAS PEREA, I. (Coords.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant Lo Blanch, Valencia, 2018, págs. 135-167.

LUCAS MURILLO DE LA CUEVA, P., «Notas sobre el derecho fundamental al secreto de las comunicaciones», AA.VV., *Constitución, Estado de las Autonomías y justicia constitucional (Libro homenaje al profesor Gumersindo Trujillo)*, Tirant Lo Blanch, Valencia, 2005, págs. 601-685.

MARCHENA GÓMEZ, M., «La vulneración de derechos fundamentales por ministerio de la Ley (a propósito del art. 33 de la Ley General de Telecomunicaciones)», *Diario La Ley*, 7572, 2011, págs. 1-15.

MARTÍN MORALES, R., *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid, 1995.

- MARTÍNEZ ALARCÓN, M. L., «El control de las comunicaciones electrónicas que los trabajadores realizan a través de las herramientas informáticas de la empresa», RUBIO LLORENTE, F., JIMÉNEZ CAMPO, J., SOLOZABAL ECHAVARRÍA, J. J., BIGLINO CAMPOS, P. y GÓMEZ MONTORO, A. (Coords.), *La Constitución política de España. Estudios en homenaje a Manuel Aragón Reyes*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, págs. 725-745.
- MARTÍNEZ PUJALTE, A.L., «El art. 9.2 CE y su significación en el sistema constitucional de derechos fundamentales», *Revista de las Cortes Generales*, 40, 1997, págs. 111-128.
- MARTÍN-RETORTILLO BAQUER, L., «La calidad de la ley según la jurisprudencia del Tribunal Europeo de Derechos Humanos (Especial referencia a los casos “Valenzuela Contreras” y “Prado Bugallo”, ambos contra España)», *Derecho Privado y Constitución*, 17, 2003, págs. 377-406.
- MAS BADÍA, M.D., «El alcance temporal de la declaración de inconstitucionalidad de las leyes civiles. Especial referencia a las valencianas», *Derecho Privado y Constitución*, 31, 2017, págs. 317-386.
- MATALLIN EVANGELIO, A., «El efecto expansivo de los derechos fundamentales a la intimidad y al secreto de las comunicaciones telefónicas», GONZÁLEZ CUSSAC, J.L. y CUERDA ARNAU, M.L. (Dir.), *Nuevas amenazas a la seguridad nacional: Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Tirant Lo Blanch, Valencia, 2013, págs. 379-407.
- MATIA PORTILLA, F.J., *El derecho fundamental a la inviolabilidad del domicilio*, McGraw-Hill, Madrid, 1997.

- MEDINA GUERRERO, M., «El principio de proporcionalidad y el legislador de los derechos fundamentales», *Cuadernos de Derecho Público*, 5, 1998, págs. 119-142.
- MELGAR MARTÍNEZ, L., «4Cs: Ciberseguridad, Confidencialidad, Criptografía y Computación cuántica», *Diario La Ley*, 10, 2017, págs. 1-7.
- MOLINER RUÍZ, M., *Diccionario del uso del español*, Tomo II, Gredos, Madrid, 2004.
- MONSTESQUIEU, *Considérations sur les causes de la grandeur des Romains et de leur décadence*, 1734.
- MONTAÑÉS PARDO, M.A., *La intervención de las comunicaciones. Doctrina jurisprudencial*, Aranzadi, Pamplona, 1999.
- MORALES LUNA, G., «Computabilidad y computación cuántica: revisión de modelos alternativos de computación», *Ingeniería Industrial*, 2, 2011, págs. 49-63.
- MORENO CATENA, V.M., *El secreto en la prueba de testigos del proceso penal*, Montecorvo, Madrid, 1980.
- MORENO FONTELA, J.L., «Servicios cifrados de extremo a extremo e investigación penal bajo derecho español», VALLS PRIETO, J. (Coord.), *Retos jurídicos por la sociedad digital*, Aranzadi, Cizur Menor, 2018, págs. 269-299.
- MORÓN LERMA, E., *El Secreto de Empresa: Protección Penal y Retos que Plantea ante las Nuevas Tecnologías*, Aranzadi, Cizur Menor, 2002.

- MURRAY, D. y FUSSEY, P., «Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data», *Israel Law Review*, Vol. 52, 1, 2019, págs. 31–60.
- NEIRA PENA, A.M., «La interceptación de las comunicaciones de la persona jurídica investigada», *Justicia: revista de derecho procesal*, 2, 2016, págs. 421-460.
- NOYA FERREIRO, L., «Presupuestos constitucionales de las medidas de intervención de las comunicaciones I», *Dereito. Revista xuridica da Universidade de Santiago de Compostela*, 2, 1999, págs. 145-166.
- NOYA FERREIRO, L., «Presupuestos constitucionales de las medidas de intervención de las comunicaciones II», *Dereito. Revista xuridica da Universidade de Santiago de Compostela*, 1, 2000, págs. 101-120.
- OCÓN GARCÍA, J., «La incidencia de las resoluciones del TEDH en la configuración del derecho fundamental al secreto de las comunicaciones», AA.VV., *Diálogos judiciales en el sistema europeo de protección de derechos: una mirada interdisciplinar*, Tirant Lo Blanch, Valencia, 2018, págs. 259-272.
- OCÓN GARCÍA, J., «Derecho a la intimidad y registro de dispositivos informáticos: a propósito del asunto Trabajo Rueda c. España», *Revista Española de Derecho Constitucional*, 113, 2018, págs. 327-343.
- OLMO FERNÁNDEZ-DELGADO, L., *El descubrimiento y revelación de secretos documentales y de las telecomunicaciones. Estudio del artículo 197.1º del Código Penal*, Dykinson, Madrid, 2009.

- ORTIZ PRADILLO, J.C., «Tecnología versus proporcionalidad en la investigación penal: la nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas», *La Ley Penal*, 75, 2010, págs. 1-14.
- ORTIZ PRADILLO, J.C., «Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos», BAUZÁ REILLY, M. y BUENO DE MATA, F. (Coords.), *El derecho en la sociedad telemática. Estudios en homenaje al profesor Valentín Carrascosa López*, Andavira, Santiago de Compostela, 2012, págs. 57-86.
- PACE, A., *Problematica delle libertà costituzionali. Parte Generale*, CEDAM, Padova, 2003.
- PASCUAL MEDRANO, A., «Los derechos fundamentales y la Ley de Protección del Menor», *Revista jurídica de Navarra*, 22, 1996, págs. 249-264.
- PASCUAL MEDRANO, A., *El Derecho Fundamental a la Propia Imagen. Fundamento, Contenido, Titularidad y Límites*, Aranzadi, Cizur Menor, 2003.
- PASCUAL MEDRANO, A., «La dignidad humana como principio jurídico del ordenamiento constitucional español», CHUECA RODRÍGUEZ, R. (Dir.), *Dignidad humana y derecho fundamental*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015, págs. 295-333.
- PERALTA GUTIÉRREZ, A. y AGUIRRE ALLENDE, P., «El TJUE y el acceso a los datos de abonado en el seno de la instrucción penal», *Diario La Ley*, 9420, 2019, págs. 1-11.

- PÉREZ PEREIRA, M., «La evolución de los sistemas de cifrado», *Revista de la Contratación Electrónica*, 75, 2006, págs. 93-99.
- POLLICINO, O., «La tutela de la *privacy* digital: el diálogo entre el Tribunal de Justicia de la Unión Europea y las jurisdicciones nacionales», *Revista de Estudios Políticos*, 173, 2016, págs. 195-244.
- PONS PORTELLA, M., «La nulidad diferida de las leyes en caso de omisión de informes autonómicos preceptivos», *Anales de la Facultad de Derecho*, 35, 2018, págs. 29-45.
- PRESNO LINERA, M.A., *El derecho de voto*, Tecnos, Madrid, 2003.
- PUNSET BLANCO, R., «Las sentencias declaratorias de la inconstitucionalidad de las leyes: consideraciones sobre la posible reforma de los artículos 39.1 y 40.1 de la LOTC», *Anuario de Derecho Constitucional y Parlamentario*, 7, 1995, págs. 33-48.
- QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T., *El recurso de amparo y los derechos fundamentales en las relaciones entre particulares*, Civitas, Madrid, 1981.
- REBOLLO DELGADO, L., «El secreto de las comunicaciones: problemas actuales», *Revista de Derecho Político*, 48-49, 2000, págs. 351-382.
- REQUEJO RODRÍGUEZ, P., «¿Suspensión o supresión de los derechos fundamentales?», *Revista de Derecho Político*, 51, 2001, págs. 105-137.
- RICARD, J.D., *Droit et jurisprudence en matière de postes, télégraphes, téléphones*, Recueil Sirey, París, 1931.

- RICHARD GONZÁLEZ, M., *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*, La Ley, Madrid, 2017.
- RIDAURA MARTÍNEZ, M.J., «El legislador ausente del artículo 18.3 de la Constitución (la construcción pretoriana del derecho al secreto de las comunicaciones)», *Revista de Derecho Político*, 100, 2017, págs. 347-404.
- RIVERA, A., «Computación cuántica: nuevas reglas del juego para los ordenadores», *Alfa. Revista de seguridad nuclear y protección radiológica*, 27, 2015, págs. 35-41.
- RIVERO SÁNCHEZ-COVISA, F.J., *Revisión del concepto constitucional del secreto de las comunicaciones*, Dykinson, Madrid, 2017.
- RIVEST, R.L., «The Case against Regulating Encryption Technology», *Scientific American*, 279, 1998, págs. 116-117.
- ROCA TRÍAS, E. y AHUMADA RUIZ, M.A., «Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española», *XV Conferencia de los Tribunales Constitucionales de Italia, Portugal y España*, 2013, págs. 1-37.
- RODOTÁ, S., «La conservación de los datos de tráfico en las comunicaciones electrónicas», *IDP. Revista de Internet, Derecho y Política*, 3, 2006, págs. 53-60.
- RODRÍGUEZ LAINZ, J.L., «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», *Diario La Ley*, 6859 y 6860, 2008, págs. 1-41.

- RODRÍGUEZ LAINZ, J.L., «Consideraciones jurídicas en torno a la licitud constitucional de SITEL», *Diario La Ley*, 7344, 2010, págs. 1-21.
- RODRÍGUEZ LAINZ, J.L., «Sobre la naturaleza formal del derecho al secreto de las comunicaciones: dimensión constitucional e histórica», *Diario La Ley*, 7647, 2011, págs. 1-15.
- RODRÍGUEZ LAINZ, J.L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», *Diario La Ley*, 8142, 2013, págs. 1-12.
- RODRÍGUEZ LAINZ, J.L., «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones», *Diario La Ley*, 8308, 2014, págs. 1-15.
- RODRÍGUEZ LAINZ, J.L., «Sobre la inconstitucionalidad de las vigilancias policiales mediante micrófonos ocultos (A propósito de la STC 145/2014, de 22 de septiembre)», *Diario La Ley*, 8438, 2014, págs. 1-14.
- RODRÍGUEZ LAINZ, J.L., *El secreto de las telecomunicaciones y su interceptación legal*, Sepín, Madrid, 2016.
- RODRÍGUEZ LAINZ, J.L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», *Diario La Ley*, 8896, 2017, págs. 1-14.
- RODRÍGUEZ LAINZ, J.L., «La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones», *Diario La Ley*, 8901, 2017, págs. 1-24.

- RODRÍGUEZ LAINZ, J.L., «La jurisprudencia del tribunal de Luxemburgo sobre regímenes de conservación preventiva de datos en la Doctrina del Tribunal Supremo», *Diario La Ley*, 9087, 2017, págs. 1-9.
- RODRÍGUEZ MARÍN, F., «Los delitos de escuchas ilegales y el derecho a la intimidad», *Anuario de derecho penal y ciencias penales*, 43, 1990, págs. 197-240.
- RODRÍGUEZ MONTAÑÉS, T., «Artículo 18.3. El secreto de las comunicaciones», *Comentarios a la Constitución Española*, RODRÍGUEZ-PIÑERO Y BRAVO FERRER, M. y CASAS BAAMONDE, M. E. (Dirs.), Tomo I, Agencia Estatal Boletín Oficial del Estado, Madrid, 2018, págs. 544-561.
- RODRÍGUEZ RUBIO, C., «La injerencia en el derecho al secreto de las comunicaciones a través de la regulación de las medidas de investigación tecnológica», *Revista Europea de Derechos Fundamentales*, 28, 2016, págs. 267-285.
- RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones: tecnología e intimidad*, McGraw-Hill, Madrid, 1998.
- RODRÍGUEZ RUIZ, B., «El coste de los derechos fundamentales. Un comentario de la STC 49/1999, de 5 de abril», *Teoría y Realidad Constitucional*, 3, 1999, págs. 315-340.
- RODRÍGUEZ RUIZ, B., «El caso *Valenzuela Contreras* y nuestro sistema de derechos fundamentales», *Revista Española de Derecho Constitucional*, 56, 1999, págs. 223-250.
- ROMEO CASABONA, C.M., *Los delitos de descubrimiento y revelación de secretos*, Tirant Lo Blanch, Valencia, 2004.

- ROSALES LEAL, M.A., «Captación y grabación de comunicaciones orales directas», *Revista de Derecho Constitucional Europeo*, 30, 2018.
- ROSOUX, G., «Au cœur de la protection “multi-niveaux” et du dialogue juridictionnel: la “dématérialisation” des droits fondamentaux comme clé de lecture du raisonnement actuel dans le domaine des droits fondamentaux», *Fundamentos. Cuadernos monográficos de teoría del estado, derecho público e historia constitucional*, 9, 2016, págs. 71-99.
- SALAMANCA AGUADO, E., «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones», *Revista del Instituto Español de Estudios Estratégicos*, 4, 2014, págs. 1-26.
- SALVADOR MARTÍNEZ, M., «El doble contenido de los derechos fundamentales en la doctrina alemana», *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, 7, 1997-1998, págs. 115-142.
- SALVADOR MARTÍNEZ, M., «Sobre el contenido objetivo de los derechos fundamentales», APARICIO PÉREZ, M.A. (Coord.), *Derechos Constitucionales y Formas Políticas. Actas del Congreso sobre derechos Constitucionales y Estado autonómico*, Cedecs, Barcelona, 2001, págs. 199-218.
- SÁNCHEZ ALMEIDA, C., «España: La Criptografía como derecho», *Revista Electrónica de Derecho Informático*, 23, 2000, págs. 1-3.
- SÁNCHEZ BARRILAO, J.F., «Servicios de inteligencia, secreto y garantía judicial de los derechos», *Teoría y Realidad Constitucional*, 44, 2019, págs. 309-339.

SÁNCHEZ YLLERA, I., «Valenzuela Contreras c. España (STEDH de 30 de julio de 1998): La deficiente calidad de las normas que habilitan la intervención de las comunicaciones telefónicas», ALCÁCER GUIRAO, R., BELADIEZ ROJO, M. y SÁNCHEZ TOMÁS, J.M., *Conflicto y diálogo con Europa. Las condenas a España del Tribunal Europeo de Derechos Humanos*, Civitas, Madrid, 2013, págs. 443-470.

SANTA TERESA, M. (trad.), *Compendio Moral Salmaticense según la mente del angélico doctor*, Tomo I, Madrid, 1808.

SEMPERE RODRÍGUEZ, C., «Artículo 18: Derecho al honor, a la intimidad y a la propia imagen», ALZAGA VILLAAMIL, O (Dir.), *Comentarios a la Constitución Española de 1978*, Tomo II, Edersa, Madrid, 1996, págs. 383-482.

SERRANO ALBERCA, M., «Artículo 18», GARRIDO FALLA, F. (Dir.), *Comentarios a la Constitución*, Civitas, Madrid, 1985, págs. 351-381.

SINGH, S., *Los códigos secretos. El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era de Internet*, Editorial Debate, Barcelona, 2000.

SOLOZÁBAL ECHEVARRÍA, «Aspectos constitucionales de la libertad de expresión y el derecho a la información», *Revista Española de Derecho Constitucional*, 23, 1988, págs. 139-155.

SOLOZÁBAL ECHEVARRÍA, «La libertad de expresión desde la teoría de los derechos fundamentales», *Revista Española de Derecho Constitucional*, 32, 1991, págs. 73-113.

- STORMS, S., VALCKE, P. y KINDT, E., «Rage against the machine: does machine-to-machine communication fall within the scope of the confidentiality principle?», *International Journal of Law and Information Technology*, 27, 2019, págs. 372-408.
- TEJERINA RODRÍGUEZ, O., *Seguridad del Estado y privacidad*, Editorial Reus, Madrid, 2014.
- TINTO GIMBERNAT, M., «El secreto de las comunicaciones electrónicas en los ordenamientos jurídicos español y norteamericano», DAVARA RODRÍGUEZ, M.A. (coord.), *III Jornadas sobre informática y sociedad*, Universidad Pontificia Comillas, Madrid, 2001, págs. 251-257.
- USAI, S., «Registrazione di conversazione tra privati: per attività di PG necessaria l'autorizzazione», *Sigurezza e Giustizia*, 2, 2015, págs. 14-15.
- VAINIO, N. y MIETTINEN, S., «Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States», *International Journal of Law and Information Technology*, 23, 2015, págs. 290-309.
- VALVERDE MEGÍAS, R., «Intervención de comunicaciones telemáticas y registro remoto», *La interceptación de las comunicaciones telefónicas y telemáticas*, Jornadas de Formación del Centro de Estudios Jurídicos, 27 de abril de 2016, págs. 1-44.
- VEGAS TORRES, J., «Detención y apertura de paquetes postales. Especial consideración de la apertura de paquetes en el marco de las entregas vigiladas», *Tribunales de Justicia*, 8-9, 1997, págs. 849-864.

- VEGAS TORRES, J., «Sobre el alcance del secreto de las comunicaciones», HERMIDA, C. y SANTOS, J.A. (Coords.), *Una Filosofía del Derecho en acción. Homenaje al profesor Andrés Ollero*, Congreso de los Diputados, Madrid, 2015, págs. 1609-1626.
- VIDAL, G. y MORENO, J.L., «Cryptography and Communications Privacy: An Introduction», ALHAJJ, R. y ROKNE, J. (Eds.), *Encyclopedia of Social Network Analysis and Mining*, Springer, Nueva York, 2018, págs. 513-533.
- VIDAL FUEYO, M.C., «Juez y pasividad del legislador. Las intervenciones corporales», *Revista Española de Derecho Constitucional*, 74, 2005, págs. 361-394.
- VIDAL MARÍN, T. y RUIZ DORADO, M., «Análisis de la constitucionalidad de SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal», *Revista Aranzadi Doctrinal*, 9, 2016, págs. 135-162.
- VILASAU SOLANA, M., «La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad», *IDP. Revista de Internet, Derecho y Política*, 3, 2006, págs. 1-15.
- VILLALBA SÁNCHEZ, A., «Los derechos fundamentales del trabajador frente a los nuevos instrumentos de control empresarial», *Revista Derecho Social y Empresa*, 6, 2016, págs. 86-105.
- VILLAVERDE MENÉNDEZ, I., «Concepto, contenido, objeto y límites de los derechos fundamentales», AA.VV., *La democracia constitucional. Estudios en homenaje al Profesor Francisco Rubio Llorente*, Congreso de los Diputados, Madrid, 2002, págs. 317-363.

- VÍRGALA FORURIA, E., «La suspensión de derechos por terrorismo en el ordenamiento español», *Revista Española de Derecho Constitucional*, 40, 1994, págs. 61-132.
- ZOCO ZABALA, C., «Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de SITEL con el artículo 18.3 CE», *InDret*, 4, 2010, págs. 1-17.
- ZOCO ZABALA, C., *La Intervención Judicial de las Comunicaciones ¿Privadas?*, Aranzadi, Cizur Menor, 2014.
- ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones*, Aranzadi, Cizur Menor, 2015.
- ZOCO ZABALA, C., «Intervención de las comunicaciones e intervención de las conversaciones: una misma protección *iusfundamental*», HERRERO GUTIÉRREZ, F.J. y MATEOS MARTÍN, C. (Coords.), *Del verbo al bit*, Sociedad Latina de Comunicación Social, La Laguna, 2017, págs. 344-363.
- ZOCO ZABALA, C., «Secreto de las comunicaciones en la frontera de la revolución tecnológica», CHUECA RODRÍGUEZ, R. (Dir.), *Las fronteras de los derechos fundamentales en la constitución normativa*, Centro de Estudios Políticos y Constitucionales, Madrid, 2019, págs. 311-338.
- ZUIDERVEEN BORGESIU, F.J., y STEENBRUGGEN, W., «The right to communications confidentiality in Europe: protecting privacy, freedom of expression, and trust», *Theoretical Inquiries in Law*, Vol. 20, 1, 2019, págs. 291-322.

JURISPRUDENCIA

TRIBUNAL EUROPEO DE DERECHOS HUMANOS

Decisión de 26 de septiembre de 2006 (*Abdulkadir Coban c. España*)

Decisión de 7 de septiembre de 2010 (*Fernández Saavedra c. España*)

STEDH de 21 de febrero de 1975 (*Golder c. Reino Unido*)

STEDH de 6 de septiembre de 1978 (*Klass y otros c. Alemania*)

STEDH de 26 de abril de 1979 (*Sunday Times c. Reino Unido*)

STEDH de 2 de agosto de 1984 (*Malone c. Reino Unido*)

STEDH de 26 de marzo de 1985 (*X e Y c. Países Bajos*)

STEDH de 24 de abril de 1990 (*Huvig c. Francia*)

STEDH de 24 de abril de 1990 (*Kruslin c. Francia*)

STEDH de 23 de noviembre de 1993 (*A. c. Francia*)

STEDH de 30 de julio de 1998 (*Valenzuela Contreras c. España*)

STEDH de 16 de febrero de 2000 (*Amann c. Suiza*)

STEDH de 12 de mayo de 2000 (*Khan c. Reino Unido*)

STEDH de 25 de septiembre de 2001 (*P.G. y J.H. c. Reino Unido*)

STEDH de 18 de febrero de 2003 (*Prado Bugallo c. España*)

STEDH de 8 de abril de 2003 (*M.M. c. Países Bajos*)

STEDH de 31 de mayo de 2005 (*Vetter c. Francia*)

STEDH de 3 de abril de 2007 (*Copland c. Reino Unido*)

STEDH de 7 de febrero de 2012 (*Von Hannover c. Alemania*)

STEDH de 16 de julio de 2014 (*Hämäläinen c. Finlandia*)

STEDH de 30 de mayo de 2017 (*Trabajo Rueda c. España*)

STEDH de 5 de septiembre de 2017 (*Barbulescu c. Rumania*)

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

STJUE, Gran Sala, de 8 de abril de 2014 (asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd*)

STJUE, Gran Sala, de 21 de diciembre de 2016 (asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB*)

STJUE, Gran Sala, de 2 de octubre de 2018 (asunto C-207/16, *Ministerio Fiscal*)

TRIBUNAL CONSTITUCIONAL

ATC 257/1985, de 17 de abril

ATC 344/1990, de 1 de octubre

ATC 382/1996, de 18 de diciembre

STC 11/1981, de 8 de abril

STC 21/1981, de 15 de junio

STC 25/1981, de 14 de julio

STC 26/1981, de 17 de julio

STC 2/1982, de 29 de enero

STC 24/1982, de 13 de mayo

STC 62/1982, de 15 de octubre

STC 101/1983, de 18 de noviembre

STC 18/1984, de 7 de febrero

STC 22/1984, de 17 de febrero

STC 71/1984, de 12 de junio

STC 107/1984, de 23 de noviembre

STC 110/1984, de 26 de noviembre

STC 114/1984, de 29 de noviembre

STC 13/1985, de 31 de enero

STC 53/1985, de 11 de abril

STC 137/1985, de 17 de octubre

STC 159/1986, de 16 de diciembre

STC 196/1987, de 11 de diciembre

STC 199/1987, de 16 de diciembre

STC 64/1988, de 12 de abril

STC 141/1988, de 12 de julio

STC 177/1988, de 10 de octubre

STC 231/1988, de 2 de diciembre
STC 254/1988, de 21 de diciembre
STC 23/1989, de 2 de febrero
STC 45/1989, de 20 de febrero
STC 129/1989, de 17 de julio
STC 36/1991, de 14 de febrero
STC 245/1991, de 16 de diciembre
STC 222/1992, de 11 de diciembre
STC 100/1993, de 22 de marzo
STC 85/1994, de 14 de marzo
STC 117/1994, de 25 de abril
STC 66/1995, de 8 de mayo
STC 139/1995, de 26 de septiembre
STC 181/1995, de 11 de diciembre
STC 34/1996, de 11 de marzo
STC 46/1996, de 26 de marzo
STC 49/1996, de 26 de marzo
STC 54/1996, de 26 de marzo
STC 55/1996, de 28 de marzo
STC 96/1996, de 30 de mayo
STC 207/1996, de 16 de diciembre
STC 123/1997, de 1 de julio
STC 121/1998, de 15 de junio
STC 177/1998, de 14 de septiembre
STC 195/1998, de 1 de octubre
STC 49/1999, de 5 de abril
STC 69/1999, de 26 de abril
STC 136/1999, de 20 de julio
STC 166/1999, de 27 de septiembre
STC 171/1999, de 27 de septiembre
STC 208/1999, de 11 de noviembre
STC 235/1999, de 20 de diciembre
STC 98/2000, de 10 de abril
STC 126/2000, de 16 de mayo

STC 141/2000, de 29 de mayo
STC 292/2000, de 30 de noviembre
STC 299/2000, de 11 de diciembre
STC 14/2001, de 29 de enero
STC 138/2001, de 18 de junio
STC 169/2001, de 16 de julio
STC 202/2001, de 15 de octubre
STC 70/2002, de 3 de abril
STC 82/2002, de 22 de abril
STC 83/2002, de 22 de abril
STC 123/2002, de 20 de mayo
STC 137/2002, de 3 de junio
STC 167/2002, de 18 de septiembre
STC 205/2002, de 11 de noviembre
STC 14/2003, de 28 de enero
STC 33/2003, de 13 de febrero
STC 56/2003, de 24 de marzo
STC 184/2003, de 23 de octubre
STC 198/2003, de 10 de noviembre
STC 138/2005, de 26 de mayo
STC 165/2005, de 20 de junio
STC 180/2005, de 4 de julio
STC 205/2005, de 18 de julio
STC 259/2005, de 24 de octubre
STC 261/2005, de 24 de octubre
STC 273/2005, de 27 de octubre
STC 26/2006, de 30 de enero
STC 104/2006, de 3 de abril
STC 136/2006, de 8 de mayo
STC 146/2006, de 8 de mayo
STC 150/2006, de 22 de mayo
STC 219/2006, de 3 de julio
STC 220/2006, de 3 de julio
STC 239/2006, de 17 de julio

STC 253/2006, de 11 de septiembre
STC 281/2006, de 9 de octubre
STC 222/2007, de 8 de octubre
STC 230/2007, de 5 de noviembre
STC 148/2009, de 15 de junio
STC 197/2009, de 28 de septiembre
STC 219/2009, de 21 de diciembre
STC 220/2009, de 21 de diciembre
STC 5/2010, de 7 de abril
STC 26/2010, de 27 de abril
STC 68/2010, de 18 de octubre
STC 72/2010, de 18 de octubre
STC 87/2010, de 3 de noviembre
STC 9/2011, de 28 de febrero
STC 15/2011, de 28 de febrero
STC 25/2011, de 14 de marzo
STC 173/2011, de 7 de noviembre
STC 12/2012, de 30 de enero
STC 142/2012, de 2 de julio
STC 241/2012, de 17 de diciembre
STC 115/2013, de 9 de mayo
STC 164/2013, de 26 de septiembre
STC 170/2013, de 7 de octubre
STC 145/2014, de 22 de septiembre
STC 164/2014, de 7 de octubre
STC 13/2015, de 5 de febrero
STC 151/2017, de 21 de diciembre
STC 26/2018, de 5 de marzo
STC 25/2019, de 25 de febrero
STC 76/2019, de 22 de mayo

TRIBUNAL SUPREMO

ATS, Sala de lo Penal, de 18 de junio de 1992 (recurso núm. 610/1990)
STS, Sala de lo Civil, de 3 de noviembre de 1988
STS, Sala de lo Penal, de 10 de marzo de 1989
STS, Sala de lo Penal, de 21 de febrero de 1991
STS, Sala de lo Penal, de 25 de junio de 1993
STS, Sala de lo Penal, de 20 de mayo de 1994 (recurso núm. 2946/1993)
STS, Sala de lo Penal, de 19 de noviembre de 1994 (recurso núm. 1827/1994)
STS, Sala de lo Penal, de 23 de diciembre de 1994 (recurso núm. 936/1993)
STS, Sala de lo Penal, de 13 de marzo de 1995 (recurso núm. 241/1994)
STS, Sala de lo Penal, de 23 de marzo de 1995 (recurso núm. 3063/1994)
STS, Sala de lo Penal, de 1 de febrero de 1996 (recurso núm. 849/1995)
STS, Sala de lo Penal, de 20 de diciembre de 1996 (recurso núm. 3369/1995)
STS, Sala de lo Penal, de 7 de noviembre de 1997 (recurso núm. 2596/1995)
STS, Sala de lo Penal, de 27 de noviembre de 1998 (recurso núm. 802/1997)
STS, Sala de lo Penal, de 8 de febrero de 1999 (recurso núm. 1224/1998)
STS, Sala de lo Penal, de 22 de marzo de 1999 (recurso núm. 1528/1998)
STS, Sala de lo Penal, de 11 de mayo de 2001 (recurso núm. 2188/1999)
STS, Sala de lo Penal de 7 de diciembre de 2001 (recurso núm. 865/2000)
STS, Sala de lo Penal, de 27 de junio de 2002 (recurso núm. 4174/2000)
STS, Sala de lo Penal, de 30 de noviembre de 2005 (recurso núm. 2135/2004)
STS, Sala de lo Penal, de 6 de marzo de 2006 (recurso núm. 1285/2004)
STS, Sala de lo Penal, de 20 de junio de 2006 (recurso núm. 1004/2005)
STS, Sala de lo Penal, de 20 de febrero de 2007 (recurso núm. 1647/2006)
STS, Sala de lo Penal, de 3 de octubre de 2007 (recurso núm. 1473/2006)
STS, Sala de lo Penal, de 9 de mayo de 2008 (recurso núm. 1797/2007)
STS, Sala de lo Penal, de 20 de mayo de 2008 (recurso núm. 10983/2007)
STS, Sala de lo Penal, de 25 de noviembre de 2008 (recurso núm. 227/2008)
STS, Sala de lo Penal, de 13 de marzo de 2009 (recurso núm. 10624/2008)
STS, Sala de lo Penal, de 5 de febrero de 2010 (recurso núm. 1691/2009)
STS, Sala de lo Penal, de 11 de marzo de 2010 (recurso núm. 11238/2009)
STS, Sala de lo Penal, de 18 de marzo de 2010 (recurso núm. 121/2009)
STS, Sala de lo Penal, de 16 de diciembre de 2011 (recurso núm. 496/2011)
STS, Sala de lo Penal, de 22 de diciembre de 2011 (recurso núm. 93/2011)

STS, Sala de lo Penal, de 12 de abril de 2012 (recurso núm. 1491/2011)
STS, Sala de lo Penal, de 17 de abril de 2013 (recurso núm. 1461/2012)
STS, Sala de lo Penal, de 18 de abril de 2013 (recurso núm. 593/2012)
STS, Sala de lo Penal, de 14 de noviembre de 2013 (recurso núm. 642/2013)
STS, Sala de lo Penal, de 2 de abril de 2014 (recurso núm. 1581/2013)
STS, Sala de lo Penal, de 16 de junio de 2014 (recurso núm. 2229/2013)
STS, Sala de lo Penal, de 18 de julio de 2014 (recurso núm. 11124/2013)
STS, Sala de lo Penal, de 26 de noviembre de 2014 (recurso núm. 10269/2014)
STS, Sala de lo Penal, de 22 de diciembre de 2014 (recurso núm. 10636/2014)
STS, Sala de lo Penal, de 24 de febrero de 2015 (recurso núm. 1774/2014)
STS, Sala de lo Penal, de 14 de abril de 2015 (recurso núm. 10731/2014)
STS, Sala de lo penal, de 7 de julio de 2015 (recurso núm. 10168/2015)
STS, Sala de lo Penal, de 23 de noviembre de 2015 (recurso núm. 10386/2015)
STS, Sala de lo Penal, de 4 de diciembre de 2015 (recurso núm. 10447/2015)
STS, Sala de lo Penal, de 10 de diciembre de 2015 (recurso núm. 912/2015)
STS, Sala de lo Penal, de 10 de marzo de 2016 (recurso núm. 10633/2015)
STS, Sala de lo Penal, de 21 de febrero de 2017 (recurso núm. 1572/2016)
STS, Sala de lo Penal, de 18 de abril de 2017 (recurso núm. 815/2016)
STS, Sala de lo Penal, de 1 de junio de 2017 (recurso núm. 1642/2016)
STS, Sala de lo Penal, de 24 de noviembre de 2017 (recurso núm. 2315/2016)
STS, Sala de lo Penal, de 14 de octubre de 2019 (recurso núm. 1379/2019)
STS, Sala de lo Penal, de 3 de marzo de 2020 (recurso núm. 2277/2018)

TRIBUNAL CONSTITUCIONAL FEDERAL ALEMÁN

BVerfGE 7, 198, de 15 de enero de 1958
BVerfGE 41, 251, de 27 de enero de 1976
BVerfGE 67, 157, de 20 de junio de 1984
BVerfGE 85, 386, de 25 de marzo de 1992
BVerfGE 100, 313, de 14 de julio de 1999
BVerfGE 106, 28, de 9 de octubre de 2002
BVerfGE 109, 279, de 3 de marzo de 2004
BVerfGE 115, 166, de 2 de marzo de 2006
BVerfGE 120, 274, de 24 de febrero de 2008

CORTE COSTITUCIONAL ITALIANA

Sentenza n. 34 del 1973

Sentenza n. 366 del 1991

Sentenza n. 81 del 1993

Sentenza n. 320 del 2009

CORTE DE CASACIÓN PENAL ITALIANA

Sentenza n. 36747, de 24 de septiembre de 2003

Sentenza n. 19158, de 20 de marzo de 2015

