

LOS DERECHOS FUNDAMENTALES A LA VIDA PRIVADA AFECTADOS POR LA INVESTIGACIÓN TECNOLÓGICA Y EL FENÓMENO DEL ENTORNO VIRTUAL

ISIDORO ESPÍN LÓPEZ

Doctor en Derecho

Ltrado de la Administración de Justicia

Resumen

Los derechos fundamentales reconocidos en la Constitución deben ser respetados en todo tipo de procedimientos. Sin embargo, es igualmente cierto que para cumplir con lo dispuesto en el artículo 299 de la Ley de Enjuiciamiento Criminal es necesario utilizar medios de investigación indefectiblemente restrictivos de ciertos derechos fundamentales, ya que su protección puede quedar eximida ante el interés público en la persecución del delito.

La ejecución de cualquiera de las novedosas medidas de investigación tecnológica reguladas en la Ley Enjuiciamiento Criminal implica una injerencia en alguno de los derechos a la vida privada reconocidos en el artículo 18 de la Constitución, que se concretan en los derechos a la intimidad, el secreto de las comunicaciones y la protección de datos de carácter personal.

Modernamente se ha invocado por la doctrina y la jurisprudencia la existencia de un nuevo derecho denominado «derecho al entorno virtual». No obstante, sin perjuicio del reconocimiento de la realidad del fenómeno del entorno virtual, no puede afirmarse categóricamente que esta constituya un derecho propiamente dicho.

Palabras clave

Derechos fundamentales, vida privada, investigación tecnológica, entorno virtual.

Abstract

The fundamental rights recognized in the Constitution must be respected in all types of proceedings. However, it is equally true that in order to comply with the provisions of article 299 of the Criminal Procedure Act it is necessary to use means of investigation that are unfailingly restrictive of certain fundamental rights, since their protection may be exempted in the public interest in the prosecution of the crime.

The execution of any of the new technological investigation measures regulated in the Criminal Procedure Law implies an interference in any of the rights to private life recognized in article 18 of the Constitution, which are specified in the rights to privacy, secrecy of communications and protection of personal data.

The existence of a new right called “right to the virtual environment” has been invoked by doctrine and jurisprudence in recent times. However, without prejudice to the recognition of the reality of the phenomenon of the virtual environment, it cannot be categorically stated that it constitutes a right as such.

Keywords

Fundamental rights, privacy, technological research, virtual environment.

ABREVIATURAS

apdo.	Apartado
art.	Artículo
AP	Audiencia Provincial
ATC	Auto Tribunal Constitucional
ATS	Auto Tribunal Supremo (Sala de lo Penal)
BOE	Boletín Oficial del Estado
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
<i>cit.</i>	Obra citada
coord.	Coordinador
CP	Código Penal
dir.	Director
DRAE	Diccionario de la Real Academia Española
FCSE	Fuerzas y cuerpos de seguridad del Estado
FGE	Fiscalía General del Estado
FJ	Fundamento jurídico
LECrím	Ley de Enjuiciamiento Criminal
LO	Ley Orgánica
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
LOPJ	Ley Orgánica del Poder Judicial
n.º	Número
p. (pp.)	Página (páginas)
RD	Real Decreto
RGPDUE	Reglamento General de Protección de Datos de la Unión Europea
ROJ	Repertorio Oficial de Jurisprudencia
SAP	Sentencia Audiencia Provincial
ss.	Siguientes
STC	Sentencia Tribunal Constitucional
STEDH	Sentencia Tribunal Europeo de Derechos Humanos
STS	Sentencia Tribunal Supremo (Sala de lo Penal)
TC	Tribunal Constitucional
TIC	Nuevas tecnologías de la información y comunicación
TEDH	Tribunal Europeo de Derechos Humanos
TJUE	Tribunal de Justicia de la Unión Europea
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea
<i>Vid.</i>	Véase
vol.	Volumen

SUMARIO

- I. INTRODUCCIÓN
- II. INVESTIGACIÓN TECNOLÓGICA Y DERECHOS FUNDAMENTALES
 1. Investigación tecnológica
 2. El principio de proporcionalidad
 - 2.1. El principio de proporcionalidad en sentido amplio
 - 2.1.1. El juicio de idoneidad
 - 2.1.2. La necesidad
 - 2.2. El principio de proporcionalidad en sentido estricto
 - 2.2.1. Concepto
 - 2.2.2. Criterios para la ponderación
 - 2.2.2.1. Entidad de las sospechas existentes
 - 2.2.2.2. Gravedad de los hechos
- III. DERECHOS FUNDAMENTALES SUSCEPTIBLES DE SER LIMITADOS POR LA INVESTIGACIÓN TECNOLÓGICA
 1. Consideraciones previas
 - 1.1. La doble naturaleza de los derechos fundamentales
 - 1.2. Los derechos fundamentales a la vida privada reconocidos en el art. 18 CE
 - 1.3. Derechos fundamentales e investigación tecnológica
 2. Derecho a la intimidad
 - 2.1. Concepto de intimidad
 - 2.2. Idea de la expectativa razonable de la privacidad
 - 2.3. Derecho a la intimidad e investigación tecnológica
 3. Derecho al secreto de las comunicaciones
 - 3.1. Delimitación entre los derechos a la intimidad y secreto de las comunicaciones
 - 3.2. Concepto de comunicación
 - 3.3. Elementos de la comunicación protegidos por el derecho
 - 3.3.1. La información compartida
 - 3.3.2. Los intervinientes en el proceso de comunicación

3.3.3. El tercero prestador del servicio

3.3.4. Los datos de tráfico o asociados

3.4. Secreto de las comunicaciones e investigación tecnológica

4. Derecho a la protección de datos de carácter personal o autodeterminación informativa

4.1. Evolución y desarrollo del derecho

4.2. Régimen jurídico básico del derecho a la protección de datos de carácter personal

4.3. Autonomía de la protección de datos frente al derecho a la intimidad

4.4. Datos de tráfico o asociados y protección de datos de carácter personal

IV. EL ENTORNO VIRTUAL

1. La existencia del llamado entorno virtual

2. La declaración jurisprudencial del entorno virtual como un derecho independiente

3. Problemas en cuanto a la efectiva existencia de un derecho. Reconducción a los derechos a la vida privada del art. 18 CE

4. Proposición de una adecuada regulación

BIBLIOGRAFÍA

I. INTRODUCCIÓN

La rápida evolución de las nuevas tecnologías, fundamentalmente por la aparición de internet y el constante progreso de los sistemas informáticos y de telecomunicaciones, provocó la aparición de nuevas formas de delincuencia organizada que, valiéndose de complejos sistemas tecnológicos, vinieron a constituir lo que ha sido denominado como el fenómeno de la «ciberdelincuencia».

Este progreso tecnológico exigió que los ordenamientos jurídicos establecieran medidas de investigación como reacción a dicho fenómeno delictivo aprovechando los avanzados sistemas de comunicación, imagen, audio, vídeo e informáticos en general. Estos medios, que hasta no hace mucho tiempo eran desconocidos, han proporcionado a los poderes públicos unas valiosísimas herramientas para la persecución, investigación y prueba de las conductas delictivas, y no solo de aquellas conductas en cuya comisión se utilizan medios relacionados con las nuevas tecnologías, sino en general de todas las conductas constitutivas de delito, y ello dado que la prueba de cualquier delito podría ser localizada en un archivo digital ubicado en cualquier sistema informático.

Estas medidas de investigación ya se venían llevando a cabo desde hace unos años bajo una legalidad precaria y al amparo de una jurisprudencia que, mediante formas de habilitación comunes, venía permitiendo estas novedosas formas de intromisión en la esfera privada. No obstante, no es menos cierto que, ya desde finales del siglo xx, se venía reclamando jurisprudencialmente el primero de los requisitos que debe cumplirse para que puedan tener lugar este tipo de injerencias, como es una previsión legal suficiente que cubra todos sus aspectos esenciales. Con ello, no se hacía otra cosa que reclamar el cumplimiento del mandato de la Constitución Española de 1978 (CE) relativo a que toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ya incida directamente sobre su desarrollo (art. 81.1 CE) o limite o condicione su ejercicio (art. 53.1 CE), se encuentre regulada legalmente.

De este modo, la reforma procesal para llenar este vacío legal resultaba inaplazable. Tras algunos intentos de una nueva Ley de Enjuiciamiento Criminal (LECrím), como los anteproyectos de 2011 y 2013 —que no prosperaron por razones políticas—, el legislador decidió finalmente incorporar a nuestro derecho positivo la regulación de las medidas de investigación tecnológica por medio de una nueva reforma de la más que centenaria LECrím, que tuvo lugar con la Ley Orgánica (LO) 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

De este modo, por fin tuvieron entrada en nuestro ordenamiento con una regulación suficiente medidas como la interceptación de las comunicaciones telefónicas y telemáticas; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; el registro de dispositivos de almacenamiento masivo de información, y los registros remotos sobre equipos informáticos.

La incorporación de estas medidas se afrontó por el legislador con un nuevo título VIII en el libro II de la LECrim, el cual lleva como rúbrica «De las medidas de investigación limitativas de los derechos reconocidos en el art. 18 de la Constitución», que ha sustituido al originario título VIII de 1882, que se dedicaba a la entrada y registro en lugar cerrado, del de libros y papeles y de la detención y apertura de la correspondencia escrita y telegráfica.

En este novedoso título se incluyen diez capítulos, de los cuales los tres primeros —con la relevante modificación del art. 579, relativo a la correspondencia escrita y telegráfica, e inclusión de un nuevo art. 579 bis, referido a la utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales— reproducen la anterior regulación¹. Es en los siguientes siete capítulos donde se produce la incorporación de las nuevas medidas, iniciándose la regulación con el capítulo IV, dedicado a unas disposiciones comunes a todas ellas, para continuar los restantes capítulos sucesivamente con cada una de las medidas de investigación, dedicándose el X y último a las medidas de aseguramiento en relación con la conservación y protección de datos o informaciones incluidas en sistemas informáticos.

Con la investigación tecnológica, resulta incuestionable la limitación de los derechos fundamentales regulados en el art. 18 de la CE, denominados doctrinalmente los derechos de la vida privada. Así, los derechos a la intimidad personal y familiar (art. 18.1 CE), inviolabilidad del domicilio (art. 18.2 CE), secreto de las comunicaciones (art. 18.3 CE) o protección de datos de carácter personal o derecho a la autodeterminación informativa (art. 18.4 CE) se ven restringidos con la práctica de alguna de las diligencias reguladas en la LECrim (arts. 588 bis-588 octies). Junto con ellos, jurisprudencialmente se ha invocado como nuevo derecho el llamado «derecho al entorno virtual», cuya efectiva existencia es muy discutible, como se verá en el último apartado de este trabajo.

1 Afirma Marchena Gómez que «son muchos los temas controvertidos abarcados por esos tres grandes bloques sistemáticos. Algunos de ellos, además, siguen necesitados de una actualización terminológica y conceptual que les despoje de su sabor decimonónico». Vid. Marchena Gómez, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el art. 18 de la CE. Proceso penal y nuevas tecnologías», en Marchena Gómez, M., González-Cuéllar Serrano, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015, p. 173.

II. INVESTIGACIÓN TECNOLÓGICA Y DERECHOS FUNDAMENTALES

1. Investigación tecnológica

No cabe duda, y así es admitido por todos, que las nuevas tecnologías de la información y comunicación (TIC), y muy especialmente la revolución tecnológica que tuvo lugar con la aparición de internet, han ido paulatinamente transformando nuestra forma de comunicarnos, así como nuestras relaciones sociales, fundamentalmente por la mayor facilidad para acceder a cualquier tipo de información y la inmediatez que ofrecen las comunicaciones telemáticas.

Pero, del mismo modo, estos avances tecnológicos permitieron la proliferación de nuevas formas de delinquir y la aparición de un nuevo grupo de delinquentes que, teniendo en cuenta las dificultades iniciales de la investigación en la red, unidas a la volatilidad de la información que circula por esta y la falta de regulación en nuestros textos legales de estas nuevas formas delictivas, hacían muy complicada la identificación de los responsables de estos novedosos delitos. Ante tal situación, los poderes públicos, a través de las FCSE, fueron haciendo uso de las TIC para la investigación no solo de los cibercriminales sino en general de cualquier delito.

Las diligencias de investigación (también denominadas actos instructorios o actos de investigación), en general, constituyen el cauce para la aportación de hechos al proceso, con la finalidad de acreditar ante el juez de instrucción la participación del investigado en los hechos y, como señala Gimeno Sendra, sirven a las partes para instar el sobreseimiento o formular su escrito de acusación, pero no permiten fundar una sentencia de condena. Por ello, no deben confundirse las diligencias de investigación con los actos de prueba, los cuales sí están dirigidos a poder fundar, en su día, una sentencia de condena².

En cuanto a la intromisión o injerencia en los derechos fundamentales llevada a cabo con la investigación penal en general, «resulta innecesario destacar», como así lo afirma Castillo Rigabert, «que los principios y derechos reconocidos en la Constitución han de ser respetados en todo tipo de procedimientos»³. No obstante, es igualmente cierto que, para poder dar cumplimiento al art. 299 de la LECrim⁴ y, en consecuencia,

2 Afirma Gimeno Sendra que, «debido a la función esencial de la fase instructoria, consistente en preparar adecuadamente el juicio oral (art. 299), el juez ha de realizar toda una serie de actos instructorios o de investigación a fin de comprobar la existencia y tipicidad de la “notitia criminis”, así como la de su autoría [...]. Los actos de investigación sirven, como se ha dicho, para facilitar a las partes la fundamentación fáctica de sus respectivos escritos de calificación o acusación, pero no permiten al juez o Tribunal sentenciador extender sobre ellos su conocimiento en la declaración de hechos probados de la sentencia». Vid. Gimeno Sendra, J. V., *Manual de Derecho Procesal Penal*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015, pp. 239 y 307.

3 Castillo Rigabert, F., «Derechos fundamentales e investigación en las diligencias previas (Estudio de la reciente jurisprudencia de la Sala II del TS)», *Anales de Derecho (Universidad de Murcia)*, n.º 13, 1995, p. 14.

4 Dispone el art. 299 de la LECrim: «Constituyen el sumario las actuaciones encaminadas a

descubrir la comisión de los delitos y la culpabilidad de los presuntos autores, se hace necesario el uso de medios de investigación indefectiblemente limitativos de determinados derechos fundamentales proclamados en la CE, por cuanto no tratándose de derechos absolutos, conforme precisa Moreno Catena, «cabe que su protección resulte exceptuada al enfrentarse al interés público por la persecución de los delitos»⁵.

Pues bien, esta inevitable injerencia, conforme se ha mencionado anteriormente, se vio incrementada con el desarrollo de las TIC y el crecimiento de su uso por la sociedad para fines de todo tipo, incluido lamentablemente el delictivo. En este sentido, las novedosas medidas de investigación tecnológica han originado un incremento del grado de intromisión en los llamados derechos a la vida privada, que fueron declarados con dicha rúbrica en el art. 8 del Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950⁶, y que en nuestro derecho se concretan en el art. 18 de la CE.

En todo caso, dicha injerencia será legítima, siempre que se respeten las garantías procesales y principios rectores establecidos para este tipo de medidas de investigación establecidos en la LECrim tras la reforma operada por la LO 13/2015 y que se concretan, conforme a lo dispuesto en el art. 588 bis a), en los de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

No obstante, en el contexto que nos ocupa, es de destacar que, con anterioridad a dicha reforma, el principal criterio para estimar necesaria la intromisión se concretaba en la valoración acerca de si su adopción suponía un beneficio al interés público y de terceros superior al perjuicio que pudiera sufrir el investigado con la intromisión en sus derechos fundamentales, es decir, cuando se diese cumplimiento al principio de proporcionalidad.

2. El principio de proporcionalidad

Resulta necesaria, al menos, una exposición resumida de las ideas fundamentales en virtud de las que se conformó la teoría de este trascendental principio, examinado

preparar el juicio y practicadas para averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en su calificación, y la culpabilidad de los delincuentes, asegurando sus personas y las responsabilidades pecuniarias de los mismos».

5 Moreno Catena, V., Cortés Domínguez, V., *Derecho Procesal Penal*, Valencia, Tirant lo Blanch, 2019, p. 265.

6 El art. 8 del CEDH, bajo la rúbrica «Derecho al respeto a la vida privada y familiar», dispone: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No 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 y constituya una medida que, en una sociedad democrática, sea necesaria para 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, o la protección de los derechos y las libertades de los demás».

desde el punto de vista del derecho procesal, con anterioridad a su incorporación a la ley mediante la LO 13/2015, en lo que a las medidas restrictivas de derechos fundamentales se refiere⁷.

En cuanto al fundamento del principio de proporcionalidad, puede situarse este en el respeto de la dignidad humana, como así se encargó de señalarlo el TS en la primera resolución en la que —desde el punto de vista de la injerencia en los derechos fundamentales como consecuencia de las diligencias de investigación del delito— exigió el reconocimiento del principio⁸.

Doctrinalmente, autores como Barnes, han señalado que la cláusula del Estado de derecho y los propios derechos fundamentales representan el fundamento último en el que descansa la proporcionalidad de la injerencia en el derecho fundamental, lo cual expresa de forma abreviada que el principio de proporcionalidad «encarna una idea elemental de justicia material: la proscripción de todo sacrificio de la libertad inútil, innecesario o desproporcionado»⁹.

Puede añadirse que el principio de proporcionalidad constituye una garantía para el efectivo cumplimiento del principio constitucional de la «interdicción de la arbitrariedad de los poderes públicos» (art. 9.3 CE).

Este principio, también denominado «prohibición de exceso», nace en el seno del derecho penal y, aunque sus orígenes más remotos de este se pueden encontrar en el derecho romano y en las reflexiones sobre la justicia de la filosofía práctica griega, sus primeras formulaciones se remontan al siglo XVIII, en el que autores como Beccaría se refirieron a la pena proporcional a la culpabilidad, siendo destacable que ya en la Declaración de los Derechos del Hombre y del Ciudadano de 1789 se disponía en su art. 8 que «la Ley solo debe establecer penas estricta y evidentemente necesarias»¹⁰.

7 Para ser estrictos, debe señalarse que la primera incorporación del principio de proporcionalidad en la LECrim se produce en relación con las intervenciones corporales, con la LO 15/2003, de 25 de noviembre, modificadora del CP, que en su disposición final 1.1.c) añadió un párrafo segundo al art. 363 LECrim, el cual dispone que «siempre que concurren acreditadas razones que lo justifiquen, el juez de instrucción podrá acordar, en resolución motivada, la obtención de muestras biológicas del sospechoso que resulten indispensables para la determinación de su perfil de ADN. A tal fin, podrá decidir la práctica de aquellos actos de inspección, reconocimiento o intervención corporal que resulten adecuados a los principios de proporcionalidad y razonabilidad».

8 Se trata del importante ATS de 18 de junio de 1992, ROJ: ATS 3773/1992, FJ 1, que declaró que «uno de los presupuestos fundamentales de nuestro Estado de Derecho, democrático y social, establecido en la Constitución, es el del respeto a la dignidad e intimidad de la persona humana, esencialmente libre, como base de la convivencia. Por ello existe o debe existir un obligado correlato, una proporcionalidad, entre el reconocimiento de la plenitud de estos derechos y las intromisiones en la vida privada de la persona que, en principio, son ilegítimas».

9 Barnes, J., «El principio de proporcionalidad. Estudio preliminar», *Cuadernos de Derecho Público*, vol. 5, 1998, p. 19.

10 En cuanto a las referidas menciones de los orígenes históricos del principio de proporcionali-

En nuestro país, al no tener reconocimiento expreso en la CE de 1978¹¹, la proporcionalidad se erigió en el ámbito del derecho penal, en un principio general del derecho íntimamente relacionado con el principio de intervención mínima, y que, con base en el valor superior de la libertad proclamado en el art. 1 CE, persigue como objetivo principal evitar una aplicación desmesurada de las penas privativas de libertad y, posteriormente, de todas las penas en general. Conforme a este, la pena que imponer por la comisión de un delito deberá guardar una correlación con el ilícito cometido, sin que quepa imponer una pena que no sea estrictamente necesaria para alcanzar los fines que la justifican.

En cualquier caso, y sin perjuicio de lo anterior, ha de señalarse que, con carácter general para todas las ramas del derecho, la construcción moderna del principio de proporcionalidad tiene su origen en la jurisprudencia alemana¹², país en el que, como señala Kluth, se alude normalmente, tanto por la doctrina como por la jurisprudencia, al «principio de prohibición de exceso» y no al «principio de proporcionalidad», al entenderse que la prohibición de exceso tiene un contenido más amplio del que formaría parte la proporcionalidad, afirmando este autor que con su reconocimiento por el TC alemán «se ponía fin a una discusión desarrollada en Alemania durante más de cien años».

dad, *vid.* Perelló Domenech, I., «El principio de proporcionalidad y la jurisprudencia constitucional», *Jueces para la Democracia. Información y Debate*, n.º 28, 1997, p. 69; Ruiz Ruiz, R., De la Torre Martínez, L., «Algunas aplicaciones e implicaciones del principio de proporcionalidad», *Revista Telemática de Filosofía del Derecho*, n.º 14, 2011, pp. 30-31, y Kluth, W., «Prohibición de exceso y principio de proporcionalidad en Derecho alemán», *Cuadernos de Derecho Público*, n.º 5, 1998, pp. 220-221.

11 Aun cuando no se menciona expresamente en la CE, Gimeno Sendra considera que el principio de proporcionalidad «se encuentra implícitamente contenido en el art. 25 (que, al consagrar el principio de “legalidad”, no solo establece el de “tipicidad”, sino también el de “proporcionalidad” entre la medida y la sanción) y más concretamente en cada uno de los preceptos que establecen los límites del ejercicio de los derechos fundamentales». *Vid.* Gimeno Sendra, J. V., *Manual de Derecho Procesal Penal*, *cit.*, p. 57.

12 Así lo señalan Ruiz Ruiz y De la Torre Martínez, indicando que «la construcción de este principio, tal y como se entiende en la actualidad, es obra fundamentalmente de la doctrina y la jurisprudencia constitucionales y administrativas alemanas, a quienes se debe la elaboración técnica del mismo. Así, el Tribunal Constitucional alemán reconoció expresamente en 1968 que la “prohibición de exceso” (Übermaßverbot) y el “principio de proporcionalidad” (Verhältnismäßigkeitsprinzip) eran reglas generales aplicables en todos los ámbitos de la actividad estatal, cuyo rango constitucional deriva del principio constitucional del Estado de Derecho del que aquellas reglas se deducen. Y, desde entonces, el alto Tribunal alemán ha realizado mediante sus sentencias aportaciones importantes en el reconocimiento del principio, las cuales han ayudado a asentar el concepto de que “en la República Federal de Alemania el principio de proporcionalidad tiene rango jurídico constitucional. Ese reconocimiento deriva del principio de Estado de Derecho, teniendo como sustrato esencial los derechos fundamentales”. Esta concepción se ha mantenido hasta la actualidad por la jurisprudencia y la doctrina alemana». *Vid.* Ruiz Ruiz, R., De la Torre Martínez, L., «Algunas aplicaciones e implicaciones del principio de proporcionalidad», *cit.*, p. 31.

Situándonos ya en el ámbito del derecho procesal, el principio de proporcionalidad surge como un criterio necesario para una adecuada protección de los derechos fundamentales frente a las injerencias en ellos como consecuencia de cualquier acto procesal, adquiriendo especial relevancia dentro de estos, los de investigación.

El principio cobró especial fuerza en nuestro país en los años ochenta del siglo pasado, señalando González-Cuéllar Serrano que en el derecho procesal el principio de prohibición de exceso o proporcionalidad en sentido amplio comenzó a ser objeto de estudio doctrinal a finales de dicha década, sin que con anterioridad hubiese merecido, con carácter general y salvo algunas excepciones, la atención de los estudiosos del derecho procesal¹³.

Con anterioridad, la proporcionalidad había sido proclamada en el CEDH, que, en el apartado segundo de los arts. 8, 9, 10 y 11, dispone de una forma similar en todos ellos que las restricciones a dichos derechos solo podrán tener lugar cuando la injerencia constituya una medida que, en una sociedad democrática, sea necesaria para 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, o la protección de los derechos y las libertades de los demás.

Estos postulados fueron aplicados en distintos supuestos por la jurisprudencia del TEDH, la cual tuvo indudable influencia para el desarrollo del principio en nuestro país. El primer referente lo constituye la STEDH de 7 de diciembre de 1976, caso *Handyside c. Reino Unido*, en la que se determinó que, si bien corresponde a cada Estado adoptar, conforme a sus leyes, los casos en los que resulta posible la restricción de los derechos y libertades, el ejercicio de tal margen de apreciación habrá de ser proporcionado a la finalidad perseguida¹⁴, situando el criterio fundamental para estimar que la medida ha sido proporcionada en la circunstancia de que esta fuese «necesaria para obtener el fin perseguido»¹⁵.

Por su parte, la STEDH de 22 de octubre de 1981, caso *Dudgeon c. Reino Unido*, declaró en su apdo. 53 que, «finalmente, en el artículo 8, al igual que en otros varios artículos del Convenio, el concepto de “necesidad” está vinculado al de “sociedad democrática”».

13 Señala González-Cuéllar Serrano que entre las excepciones relativas a los autores que sí trataron el principio de proporcionalidad con anterioridad a los años finales de la década de los ochenta del siglo pasado, en los que comenzó a ser objeto de estudio este principio, cabe destacar a Gimeno Sendra, que incluía la proporcionalidad entre los principios del proceso penal en sus manuales. *Vid.* González-Cuéllar Serrano, N., «El principio de proporcionalidad en el Derecho procesal español», *Cuadernos de Derecho Público*, n.º 5, 1998, p. 191.

14 En el apdo. 49 de la citada sentencia, el Alto Tribunal Europeo enjuiciaba unos hechos en relación con el derecho a la «libertad de expresión» y destacó que «toda formalidad, condición, restricción o sanción impuesta en la materia debe ser proporcionada al fin legítimo que se persigue».

15 En el apdo. 58, la misma STEDH declaró que el Reino Unido habría violado «el principio de proporcionalidad inherente al adjetivo “necesario”».

Por lo que respecta a nuestro TC, inició la afirmación del principio de una forma fragmentaria al referirse a este, no de una manera unitaria, sino en relación con diversos derechos constitucionales, como, por ejemplo, a los derechos a la igualdad¹⁶, a la intimidad¹⁷, a la libertad de expresión¹⁸ o a la tutela judicial efectiva¹⁹, llegándose a una definitiva construcción de la teoría del principio y su paralela consolidación jurisprudencial con la STC 207/1996, de 16 de diciembre²⁰, la cual, pese a resolver acerca de una intervención corporal, establece una doctrina del principio totalmente válida para las diligencias de investigación tecnológica, y que, en palabras de González-Cuéllar Serrano, «constituye un magnífico ejemplo de rigor conceptual en el tratamiento del principio que nos ocupa»²¹.

En definitiva, como señala Barnes, «se trata, pues, de un principio general que, aunque no escrito, está reconocido al máximo nivel, y, por tanto, vincula a todos los poderes

16 *Vid.* STC 22/1981, de 2 de julio, FJ 3, que declaró que «la igualdad es solo violada si la desigualdad está desprovista de una justificación objetiva y razonable, y la existencia de dicha justificación debe apreciarse en relación a la finalidad y efectos de la medida considerada, debiendo darse una relación razonable de proporcionalidad entre los medios empleados y la finalidad perseguida».

17 *Vid.* STC 37/1989, de 15 de febrero, FJ 7, que declaró que «la protección de la intimidad reclama [...] la razonable apreciación, por la autoridad actuante, de la situación en que se halle el sujeto [...] pues no se acomodaría, ciertamente, al derecho fundamental la resolución que constriñese el ámbito de intimidad de quienes no se hallan en una posición o situación específica respecto de aquella actuación, como tampoco respetaría la garantía que consideramos, la medida desatenta a toda estimación de proporcionalidad entre el sacrificio del derecho y la situación en que se halla aquel a quien se le impone».

18 *Vid.* STC 62/1982, de 15 de octubre, FJ 5, que al enjuiciar si se había infringido el principio de proporcionalidad en relación con el derecho a la libertad de expresión, declaró que «el Tribunal Constitucional ha de circunscribirse a determinar si el principio de proporcionalidad ha quedado infringido, desde la perspectiva del derecho fundamental y del bien jurídico que ha venido a limitar su ejercicio, por ser las medidas adoptadas desproporcionadas para la defensa del bien que da origen a la restricción».

19 *Vid.* STC 36/1986, de 12 de marzo, FJ 2, que, al examinar la proporcionalidad que ha de existir entre un defecto procesal en el que incurra una de las partes en el proceso y la sanción que se establezca legalmente por dicho defecto, declaró que «debe procederse a la subsanación del defecto, más que a eliminar los derechos o facultades que se vinculan a su cauce formal, lo que, con mayor razón, debe sostenerse cuando el efecto que pueda producir la inobservancia de un requisito formal sea precisamente el cierre de la vía de recurso. Esta interpretación finalista y su corolario, la proporcionalidad entre la sanción jurídica y la entidad real del defecto, no es sino una consecuencia más de la necesaria interpretación de la legalidad ordinaria en el sentido más favorable a la efectividad de un derecho fundamental».

20 La construcción doctrinal que la STC 207/1996 realiza acerca de la proporcionalidad se lleva a cabo en el FJ 4, al cual se remitirán las sucesivas menciones que se hagan de esta resolución en este apartado.

21 González-Cuéllar Serrano, N., «El principio de proporcionalidad en el Derecho procesal español», *cit.*, p. 192.

públicos», añadiendo en relación con los numerosos pronunciamientos del TC reafirmando el principio que, «siendo reconducibles a una concepción sistemática y unitaria de la acción del Estado y de la dignidad de la persona a la que aquella se dirige, se resuelven en afirmar que el principio de proporcionalidad es inherente al Estado de Derecho y al valor justicia proclamado en el art. 1.1 CE»²².

Cabe señalar, finalmente, que el principio de proporcionalidad se encuentra proclamado en la Carta de los Derechos Fundamentales de la Unión Europea, que dispone en su art. 52.1 que «cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Solo se podrán introducir limitaciones, respetando el “principio de proporcionalidad”, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás»²³.

En cuanto al contenido del principio, la STC 207/1996 —que conforme a lo expuesto anteriormente puede ser considerada el *leading case* en lo que respecta a la doctrina constitucional respecto del principio de proporcionalidad en el derecho procesal— declara que el principio de proporcionalidad será respetado cuando, en relación con la medida, se cumplan los requisitos de idoneidad, necesidad y proporcionalidad en relación con un fin constitucionalmente legítimo²⁴.

Con base en ello, el estudio del principio que nos ocupa ha sido sistematizado en un doble sentido: amplio y estricto, aspectos que se tratarán a continuación.

22 Barnes, J., «El principio de proporcionalidad. Estudio preliminar», *cit.*, p. 19.

23 Ha de tenerse en cuenta que el art. 2 de la LO 1/2008, de 30 de julio, por la que se autoriza la ratificación por España del Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, firmado el 13 de diciembre de 2007, ya establecía que, «a tenor de lo dispuesto en el párrafo segundo del artículo 10 de la Constitución española y en el apartado 8 del artículo 1 del Tratado de Lisboa, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán también de conformidad con lo dispuesto en la Carta de los Derechos Fundamentales publicada en el “Diario Oficial de la Unión Europea” de 14 de diciembre de 2007».

24 En relación con el «fin constitucionalmente legítimo cabe señalar, como así lo ha hecho Gimeno Sendra, que «el *ius puniendi* del Estado y la tutela judicial de la víctima integran bienes constitucionales que posibilitan la lícita instauración de correlativas obligaciones del inculgado a fin de garantizar el cumplimiento de los fines del proceso penal». *Vid.* Gimeno Sendra, J. V., «Medidas limitadoras de derechos fundamentales en el proceso penal», en Pérez-Cruz Martín, A. J., Ferreiro Baamonde, X. (dirs.), Neira Pena, A. (coord.), *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional)*, A Coruña, 2 y 3 de junio de 2011, A Coruña, Universidade da Coruña, 2012, p. 82.

2.1. El principio de proporcionalidad en sentido amplio

El principio de proporcionalidad es considerado, en primer lugar, en un sentido amplio al estar comprendidos dentro de este tres subprincipios como son el principio de idoneidad, el de necesidad y el de proporcionalidad en sentido estricto.

Así lo establece la STC 207/1996 al declarar que «para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: “si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)”».

2.1.1. El juicio de idoneidad

Al ocuparnos del subprincipio de la idoneidad, o, quizá mejor dicho, «juicio de idoneidad», este puede ser definido como aquella valoración que ha de realizarse por el juez a fin de determinar si el objeto de la medida de investigación es apropiado para la obtención de evidencias que sirvan para la averiguación de un hecho aparentemente delictivo. Dicho de otro modo, como señala Perelló Domenech, «es preciso, por tanto, que la restricción que sufre el derecho resulte realmente útil para justificar el fin perseguido, o, dicho en negativo, que la medida restrictiva no sea desde todo punto de vista, y en principio, absolutamente inútil para alcanzar el fin»²⁵.

El CEDH proclama la exigencia del juicio de idoneidad en su art. 18, que, bajo la rúbrica «limitación de la aplicación de las restricciones de derechos», establece que «las restricciones que, en los términos del presente Convenio, se impongan a los citados derechos y libertades no podrán ser aplicadas más que con la finalidad para la cual hayan sido previstas». Cabe señalar que este precepto es mencionado por la STC 207/1996, declarando que la medida ha de ser «idónea (apta, adecuada) para alcanzar el fin constitucionalmente legítimo perseguido con ella (art. 18 CEDH), esto es, que sirva objetivamente para determinar los hechos que constituyen el objeto del proceso penal».

Para un correcto juicio de idoneidad, González-Cuéllar Serrano, partiendo de la base de que este criterio hace referencia, desde una perspectiva tanto objetiva como subjetiva, a la causalidad de las medidas en relación con sus fines y exige que las injerencias faciliten el éxito perseguido en virtud de su adecuación cualitativa, cuantitativa y de su ámbito subjetivo de aplicación, considera en tal sentido que la idoneidad se encuentra compuesta por tres elementos como son «la adecuación

25 Perelló Domenech, I., «El principio de proporcionalidad y la jurisprudencia constitucional», *cit.*, p. 70.

cualitativa y cuantitativa, la adecuación de su ámbito subjetivo de aplicación y la prohibición de la desviación de poder»²⁶.

a) En cuanto a la adecuación cualitativa y cuantitativa, una medida será adecuada cualitativamente cuando sea apta por su propia naturaleza y no de una forma abstracta. Así, por ejemplo, un registro de dispositivos de almacenamiento masivo o un registro remoto sobre equipos informáticos es adecuado para encontrar archivos que acrediten la comisión de un delito de pornografía infantil.

Por su parte, el aspecto cuantitativo se refiere a la duración o intensidad de la medida. De este modo, un registro remoto de un equipo informático no sería adecuado cuantitativamente una vez que haya transcurrido cierto tiempo desde que se inició la intervención y los resultados hubiesen resultado infructuosos.

b) Respecto a la adecuación del ámbito subjetivo de aplicación, será estrictamente necesaria la individualización de los sujetos pasivos de las medidas que adoptar, sin que sea posible someter a un conjunto indeterminado de ciudadanos. Para la individualización de las personas, las circunstancias que permiten llevar a cabo esta son las mismas que fundamentan la sospecha acerca de la participación del imputado en la comisión del hecho punible.

c) Y, finalmente, por lo que se refiere a la prohibición de la desviación de poder, esta se traduce en la particularidad de que el órgano de persecución penal no podrá pretender una finalidad distinta de la prevista por la ley, por lo que será inconstitucional toda medida dirigida a la consecución de fines no previstos legalmente.

2.1.2. La necesidad

El requisito de la necesidad, como su propio nombre indica, se centra en la circunstancia de que la medida ha de ser indispensable para conseguir el objetivo propuesto. Ello se producirá cuando no exista otra medida menos gravosa, entendiéndose por tanto que, en general, para cualquier acto de investigación limitativo de un derecho fundamental, el juzgador deberá llevar a cabo un «juicio de necesidad», en virtud del cual determine cuál es la medida que, siendo la menos restrictiva del derecho fundamental de que se trate, resulta suficiente para alcanzar el fin perseguido.

Como declara la STC 207/1996, de 16 de diciembre, para que la medida limitativa del derecho fundamental satisfaga las exigencias del principio de proporcionalidad, es preciso que esta «sea necesaria o imprescindible para ello, esto es, que no existan otras medidas menos gravosas que, sin imponer sacrificio alguno de los derechos fundamentales a la integridad física y a la intimidad, o con un menor grado de sacrificio, sean igualmente aptas para conseguir dicho fin». La necesidad, por tanto, supone la aplicación de una regla de subsidiariedad, en virtud de la cual se aplicará una medida

²⁶ González-Cuéllar Serrano, N., «El principio de proporcionalidad en el Derecho procesal español», *cit.*, pp. 199-206.

limitativa de derechos fundamentales, en defecto de otra medida con menor grado de lesividad de un derecho fundamental.

Ante la dificultad que en algunos casos puede suponer la elección de la medida menos gravosa²⁷, tal y como puso de manifiesto González-Cuéllar Serrano con anterioridad a la LO 13/2015, refiriéndose a aquellos supuestos en los que se localizasen dispositivos de almacenamiento en un registro domiciliario, debería otorgarse preferencia a las medidas de colaboración del imputado que evitasen búsquedas coactivas de las que pudiera prescindirse, concediendo prioridad a la inspección y copia *in situ* de los datos, de tal forma que no fuese necesaria la recogida de los dispositivos o soportes que los contengan. De todos modos, de acuerdo con lo expresado por el referido autor, serían las circunstancias del caso concreto las que condujesen a la elección de un modo de actuar u otro, siendo posiblemente la mejor opción en la mayoría de las ocasiones la recogida para el posterior análisis del equipo informático; por ejemplo, en aquellos casos en los que el interesado se negase a proporcionar la clave de acceso al disco duro del ordenador o ante el riesgo de que un intento de acceso y copia de los datos sin introducción de un determinado código provoque la destrucción de la información²⁸.

2.2. El principio de proporcionalidad en sentido estricto

2.2.1. Concepto

La STC 207/1996, de 16 de diciembre, declara que para que la medida restrictiva del derecho fundamental cumpla con las exigencias del principio de proporcionalidad es necesario que, «aun siendo idónea y necesaria, el sacrificio que imponga de tales derechos no resulte desmedido en comparación con la gravedad de los hechos y de las sospechas existentes».

En dicha afirmación, queda perfectamente condensado el subprincipio de la «proporcionalidad en sentido estricto», desprendiéndose de esta una obligada comparación, o, como dice Alexy, ponderación²⁹ entre el derecho sacrificado y el beneficio obtenido para el conjunto de la ciudadanía, en el entendimiento de que la adopción de la medida respetará el principio de proporcionalidad si el citado beneficio social supera desde una perspectiva axiológica al perjuicio sufrido por la persona investigada. Por tanto, y conforme señaló la STC 49/1999, de 5 de abril, «la

27 Afirma Kluth que, «pese a que, en abstracto, los criterios señalados pueden parecer claros, lo cierto es que su aplicación práctica resulta con frecuencia muy complicada». *Vid.* Kluth, W., «Prohibición de exceso y principio de proporcionalidad en Derecho alemán», *cit.*, p. 228.

28 González-Cuéllar Serrano, N., «Garantías constitucionales de la persecución penal en el entorno digital», en Díaz Maroto y Villarejo, J. y otros, *Derecho y Justicia Penal en el Siglo XXI*, Madrid, Colex, 2006, p. 898.

29 Afirma Alexy que la ponderación «es el tema del tercer subprincipio del principio de proporcionalidad, esto es, el principio de proporcionalidad en sentido estricto». *Vid.* Alexy, R., «Los derechos fundamentales y el principio de proporcionalidad», *Revista Española de Derecho Constitucional*, n.º 91, 2011, p. 15.

desproporción entre el fin perseguido y los medios empleados para conseguirlo puede dar lugar a un enjuiciamiento desde la perspectiva constitucional cuando esa falta de proporción implica un sacrificio excesivo e innecesario de los derechos que la Constitución garantiza»³⁰.

2.2.2. Criterios para la ponderación

Por lo que se refiere a los criterios para llevar a cabo la ponderación, conforme declara el inciso anteriormente citado de la meritada STC 207/1996, de 16 de diciembre, estos se concretan en la entidad de las sospechas existentes y en la gravedad de los hechos.

2.2.2.1. Entidad de las sospechas existentes

La entidad de las sospechas se identifica con la existencia de indicios suficientes, siendo de destacar lo mencionado por la Circular 1/2013 de la FGE cuando señala que «los indicios suficientes para acordar la intervención son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento», así como que «las sospechas no han de ser tan solo circunstancias meramente anímicas, sino que precisan hallarse apoyadas en datos objetivos»³¹.

En el mismo sentido se había pronunciado la jurisprudencia del TC, declarando que la exteriorización en la resolución judicial de los indicios que permiten la intervención es indispensable, habida cuenta de que «el juicio sobre la legitimidad constitucional de la medida exige verificar si la decisión judicial apreció razonadamente la conexión entre el sujeto o sujetos que iban a verse afectados por la medida y el delito investigado», así como que «la relación entre la persona investigada y el delito se manifiesta en las sospechas que, como tiene declarado este Tribunal, no son tan solo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas hallarse apoyadas en datos objetivos, que han de serlo 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 que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona»³².

También el TS ha tenido la oportunidad de pronunciarse en relación con la entidad de las sospechas como criterio para la resolución de la proporcionalidad en sentido estricto, al señalar que «la sospecha acerca de la comisión del delito o de la participación del sospechoso no puede ser considerada un indicio, por más contundente que sea su expresión, ni tampoco, consecuentemente, puede serlo la afirmación de la existencia del delito y de la participación; o de su posibilidad o

30 Vid. STC 49/1999, de 5 de abril, FJ 7, que cita diversas sentencias anteriores.

31 Fiscalía General del Estado, Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, 2013, p. 134.

32 Vid. STC 167/2002, de 18 de septiembre, FJ 2.

probabilidad», así como que «el juez, en el cumplimiento de su función de protección del derecho fundamental, no puede operar sobre el valor que otorgue o la confianza que le proporcione la sospecha policial en sí misma considerada, sino sobre el significado razonable de los datos objetivos que se le aportan, valorados como indicios, obtenidos por la policía en el intento inicial de verificación de la consistencia de sus sospechas»³³.

Por tanto, puede concluirse que en nuestro derecho se impone la necesidad de que la convicción del juez se manifieste en la resolución judicial, haciendo constar los factores que permitieron llegar a esta, sin que estos factores constituyan meras suposiciones o conjeturas de la existencia del delito.

2.2.2.2. Gravedad de los hechos

Una vez determinada la suficiencia de los indicios, habrá que estar a que los presuntos hechos delictivos sobre los que se tienen sospechas fundadas tengan una gravedad que permita la injerencia en los derechos fundamentales. Cabe señalar que el TS ha declarado que «el interés del Estado y de la Sociedad en la persecución y descubrimiento de los hechos delictivos es directamente proporcional a la gravedad de estos», por lo que «solo en relación a la investigación de delitos graves, que son los que mayor interés despiertan su persecución y castigo, será adecuado el sacrificio de la vulneración de derechos fundamentales para facilitar su descubrimiento, pues en otro caso, el juicio de ponderación de los intereses en conflicto desaparecería si por delitos menores, incluso faltas se generalizase este medio excepcional de investigación, que desembocaría en el generalizado quebranto de derechos fundamentales de la persona sin justificación posible»³⁴.

33 *Vid.* STS 775/2014, de 20 de noviembre, FJ 1, la cual también señala que «en consecuencia no es suficiente que quien solicita la medida comunique, sobre la base de sus noticias o informaciones, que sabe o cree saber que el sospechoso ha cometido, está cometiendo, o va a cometer un delito; o que ha practicado una investigación y que exponga a continuación sus conclusiones. Por el contrario, es preciso que traslade al juez las razones de tal afirmación, o el contenido de aquella indagación en su integridad, identificando las diligencias practicadas y los datos objetivos relevantes alcanzados como su resultado, pues precisamente esos elementos son los que deben ser valorados por el juez para decidir acerca de la consistencia de los indicios y, en consecuencia, de la necesidad y proporcionalidad de la restricción del derecho fundamental que le es solicitada».

34 *Vid.* STS 297/2006, de 6 de marzo, FJ 2, que, al referirse a la intervención de las comunicaciones telefónicas como un medio de investigación excepcional, declaró, asimismo, que, «frente a otras legislaciones que establecen un catálogo de delitos para cuya investigación está previsto este medio excepcional, la legislación española guarda un silencio que ha sido interpretado por la jurisprudencia en el sentido de exigir la investigación de hechos delictivos graves, y desde luego, aquellos que revisten la forma de delincuencia organizada; de alguna manera, puede decirse que en un riguroso juicio de ponderación concretado a cada caso, la derogación del principio de intangibilidad de los derechos fundamentales, debe ser proporcionado a la legítima finalidad perseguida».

Por otra parte, autores como Subijana Zunzunegui afirman que «el enorme sacrificio que para la plenitud de los derechos fundamentales supone su limitación conlleva que la misma solo encuentre justificación cuando el interés estatal en la investigación penal tenga una especial relevancia, en atención a la gravedad del delito investigado, utilizando para determinar la gravedad tanto un criterio cuantitativo (importancia de la pena asignada al delito) como cualitativo (trascendencia social de los hechos investigados)»³⁵.

Por tanto, de acuerdo con lo indicado por este autor, atendiendo a los aspectos cuantitativo y cualitativo que han de tenerse en cuenta para fijar la mayor o menor gravedad de los hechos, las medidas limitativas de derechos fundamentales podrán acordarse para la investigación de los delitos graves contemplados en el CP según los arts. 13 y 33 de este en función de la pena que imponer. Pero, además, podrán acordarse para la investigación de delitos que, aun sin alcanzar la pena prevista para los delitos graves previstos por el CP, estén ocasionados por unos hechos cuya gravedad tenga una trascendencia social que exija la intervención.

Tal y como apuntó Velasco Núñez con anterioridad a la promulgación de la reforma operada por la LO 13/2015, «a diferencia de los países que señalan el tipo de delitos concretos que permiten la investigación a través de intervenciones telecomunicativas (Alemania, Bélgica) y de aquellos otros que la modulan en función de la pena (Reino Unido, Francia)», España mantenía un esquema abierto en que la ponderación se hacía «en función no solo del tipo de delito sino sobre todo de las circunstancias que en el caso concreto explican la afección a la relevancia jurídico penal de los hechos, su bien jurídico protegido y la trascendencia social del mismo (SSTC 166/99, de 27 de septiembre, 299/2000, de 11 de diciembre, 104/2006, de 3 de abril)»³⁶, criterio que se ha mantenido por la jurisprudencia hasta fechas más recientes³⁷.

35 Subijana Zunzunegui, I. J., «Policía judicial y derecho a la intimidad en el seno de la investigación criminal», *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, n.º 10, 1997, p. 148.

36 Menciona este autor algunos casos en los que la jurisprudencia del TC y TS permitió la injerencia en la investigación de delitos que, no siendo graves conforme a los arts. 13 y 33 del CP, así fueron considerados por su repercusión social, señalando resoluciones de los altos tribunales en que se admitió la injerencia al tratarse de delitos cometidos por funcionarios (STS 14/06/1993); contrabando, por afectar a intereses fiscales y a la vez a costes sociales sanitarios; contra la propiedad intelectual, por la potencialidad lesiva y rápida difusión del uso de instrumentos como los informáticos que facilitan su comisión en masa (STC 104/2006, de 3 de abril), o por versar sobre organizaciones criminales complejas con posibilidad de atacar intereses sociales y públicos (SSTC 299/2000, de 11 de diciembre, 14/2001, de 29 de enero, 202/2001, de 15 de octubre, 82/2002, de 22 de abril). *Vid.* Velasco Núñez, E., «Correo electrónico, SMS y virus troyanos: aspectos procesales penales», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 22, 2009, p. 15.

37 *Vid.* STS 513/2014, de 24 de junio, FJ 1, que declara que, «en el momento de adoptar su decisión, el juez ha de atender, necesariamente a varios aspectos. En primer lugar, a la proporcionalidad, en el sentido de que ha de tratarse de la investigación de un delito grave. Para valorar la gravedad no solo es preciso atender a la previsión legal de una pena privativa de libertad grave,

Con carácter general, el TC se ha pronunciado en relación con la gravedad del delito declarando que «la infracción punible no puede estar determinada únicamente por la calificación de la pena legalmente prevista, aunque indudablemente es un factor que debe de ser considerado, sino que también deben tenerse en cuenta otros factores, como los bienes jurídicos protegidos y la relevancia social de aquella»³⁸, existiendo algún pronunciamiento del TS a favor de la determinación de la gravedad del delito según la trascendencia social del delito que se trata de investigar³⁹.

Por otro lado, se ha planteado si las medidas de investigación han de considerarse proporcionadas cuando se acuerden para la investigación de delitos cometidos por medios informáticos, en relación con lo que, de acuerdo con el TS en una de las últimas sentencias en que se refirió a este tema atendiendo a la regulación anterior a la LO 13/2015, declaró que las medidas de investigación tecnológica de derechos fundamentales, en la investigación de delitos cometidos por medios informáticos, han de considerarse proporcionadas «no tanto en función de la pena eventualmente aplicable sino de la propia naturaleza de los hechos investigados, de su mecánica comisiva y de las inevitables necesidades para su ulterior probanza»⁴⁰.

Esta doctrina ha tenido finalmente entrada en la LECrim tras la reforma operada por la LO 13/2015, al disponer el art. 588 bis a.5 que «las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el

sino además debe valorarse la trascendencia social del delito que se trata de investigar».

38 *Vid.* STC 299/2000, de 11 de diciembre, FJ 2, que declaró que «en este sentido no cabe sostener que, cuando el contrabando de tabaco se realiza a gran escala a través de una organización, lo que constituía objeto de la investigación policial en este caso, merece un reproche social muy escaso, dada la incidencia de tal actividad, no solo sobre los intereses recaudatorios de la Hacienda Pública, sino también sobre la finalidad extrafiscal inherente a la imposición específica sobre consumos, justificada en el caso del tabaco por los costes sociales, sanitarios en concreto, que genera por tratarse de un producto perjudicial para la salud [...] 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».

39 *Vid.* Auto del Tribunal Supremo (ATS) 353/2017, de 2 de febrero, FJ 1, que declaró que «para valorar la gravedad no solo es preciso atender a la previsión legal de una pena privativa de libertad grave, sino además debe valorarse la trascendencia social del delito que se trata de investigar».

40 *Vid.* STS 811/2015, de 9 de diciembre, FJ 1, la cual justifica la proporcionalidad de las diligencias de investigación tecnológica cuando se trate de investigación de los delitos cometidos por medios informáticos de forma independiente a la nueva regulación. Además, declara que, «en esta clase de delitos, la posible volatilidad de las pruebas documentales puede aconsejar claramente en numerosos supuestos una rápida intervención tendente a su más pronta ocupación, sin las demoras que produciría una investigación más amplia».

interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho».

III. DERECHOS FUNDAMENTALES SUSCEPTIBLES DE SER LIMITADOS POR LA INVESTIGACIÓN TECNOLÓGICA

1. Consideraciones previas

Previamente al estudio de los derechos fundamentales a la vida privada afectados por la investigación tecnológica, se realizarán unas breves consideraciones acerca de los derechos fundamentales con carácter general, para lo cual se hace necesario examinar, en primer lugar, la doble naturaleza de los derechos fundamentales.

1.1. La doble naturaleza de los derechos fundamentales

Una de las primeras sentencias del TC ya se refirió a la doble naturaleza de los derechos fundamentales al declarar que, «en primer lugar, los derechos fundamentales son derechos subjetivos, derechos de los individuos no solo 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»⁴¹.

Así, desde el punto de vista subjetivo, siguiendo a García-Atance y García de Mora, «su carácter público les confiere la condición de que son exigibles frente al Estado y frente a los poderes públicos»⁴², mientras que, en relación con el aspecto objetivo de estos ha señalado Álvarez Conde que «los derechos fundamentales, además de su condición de derechos subjetivos, cumplen una función unificadora del ordenamiento jurídico, al que dotan de sus contenidos básicos, estableciendo una vinculación directa entre los individuos y el Estado»⁴³, refiriéndose a una obligación negativa del Estado de no lesionar la esfera individual o institucional protegida por los derechos fundamentales e igualmente a una obligación positiva de contribuir a la efectividad de los derechos fundamentales aun cuando no exista una pretensión subjetiva por parte del ciudadano⁴⁴.

41 STC 25/1981, de 14 de julio, FJ 5.

42 García-Atance y García de Mora, M. V., «La Constitución Dogmática (I). Estado de Derecho y naturaleza de los derechos», en García-Atance y García de Mora, M. V., Gutiérrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, p. 41.

43 Álvarez Conde, E., «El sistema constitucional español de derechos fundamentales», *Corts: Anuario de derecho parlamentario*, n.º 15, 2004, p. 118.

44 Álvarez Conde, E., «El sistema constitucional español de derechos fundamentales», *cit.*, pp. 119-120.

1.2. Los derechos fundamentales a la vida privada reconocidos en el art. 18 CE

Cuando, por medio de las diligencias de investigación tecnológica, el Estado lleva a cabo determinadas injerencias en la esfera de los derechos fundamentales, si ello es necesario para la investigación del delito, los derechos que resultan limitados se concretan en los derechos fundamentales reconocidos en el art. 18 CE.

En relación con estos, señala Díez-Picazo Giménez que «el artículo 18 CE consagra una pluralidad de derechos cuya finalidad última común es proteger la vida privada»⁴⁵. Esta denominación fue dada por la rúbrica del art. 8 del CEDH, al referirse al respeto a los derechos a la vida privada y familiar, con la única salvedad de que en este precepto no se contempla, al menos de manera expresa, el derecho al honor ni tampoco el derecho a la protección de datos. Esta última carencia se explica por la época en la que fue adoptado el CEDH, siendo prueba de ello que no se produjo tal circunstancia en la Carta de Derechos Fundamentales, aprobada por el Parlamento Europeo, el Consejo de la Unión y la Comisión Europea el 7 de diciembre de 2000 en Niza, la cual sí establece en su art. 7 el respeto a la vida privada y familiar y en su art. 8 reconoce el derecho a la protección de datos de carácter personal⁴⁶.

Los derechos a la vida privada reconocidos en el art. 18 CE que pueden resultar restringidos por las medidas de investigación tecnológica son el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la protección de datos de carácter personal⁴⁷.

1.3. Derechos fundamentales e investigación tecnológica

En cuanto a la confrontación de los derechos fundamentales a la vida privada y la investigación tecnológica, todas las diligencias de este tipo, incorporadas por la LO 13/2015 a la LECrim, es decir, la interceptación de comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización

45 Dice este autor que «se trata de lo que Louis Brandeis, un gran jurista norteamericano que llegó a ser miembro del Tribunal Supremo, bautizó hace cien años como la *privacy*. Esta privacidad consistiría, sintéticamente, en el derecho "a ser dejado en paz" (*to be let alone*). La existencia de una esfera privada, en la que los demás (poderes públicos o particulares) no pueden entrar sin el consentimiento de la persona, no implica solo un reconocimiento del altísimo valor que tiene la faceta privada de la vida humana, sino que constituye también una garantía básica de libertad: en un mundo donde toda la actividad de los hombres fuera pública, no cabría la autodeterminación individual. El constitucionalismo, así, exige diferenciar entre las esferas pública y privada y, por tanto, entre lo visible y lo reservado». *Vid.* Díez-Picazo Giménez, L. M., *Sistema de Derechos Fundamentales*, Cizur Menor (Navarra), Editorial Aranzadi, 2013, p. 279.

46 *Vid.* Díez-Picazo Giménez, L. M., «Sistema de Derechos Fundamentales», *cit.*, pp. 279-280.

47 Podría plantearse desde una perspectiva crítica la no inclusión en este estudio de los derechos al honor y a la propia imagen proclamados en el art. 18.1 CE. Sin embargo, en el contexto de las diligencias de investigación tecnológica y teniendo en cuenta la contextualización que se lleva a cabo de los derechos del art. 18 CE dentro del genérico derecho a la vida privada del art. 8 CEDH, únicamente será estudiado en este trabajo el derecho a la intimidad.

de dispositivos electrónicos, la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, el registro de dispositivos de almacenamiento masivo de información y el registro remoto sobre equipos informáticos, pueden resultar limitativas de los derechos a la vida privada reconocidos en el artículo 18 CE, como así se establece en la rúbrica del título VIII del libro II de la LECrim.

2. Derecho a la intimidad

2.1. Concepto de intimidad

Aunque se suele afirmar que el término intimidad adolece de una vaguedad e imprecisión que lo llevan al terreno de aquellos conceptos difícilmente definibles⁴⁸, nuestro TC nos ha facilitado, a los efectos que nos interesan, una correcta definición del derecho fundamental a la intimidad al declarar que «el derecho fundamental a la intimidad reconocido por el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (art. 10.1 CE), frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares»⁴⁹. Asimismo, ha declarado que «tratándose de un derecho fundamental estrictamente vinculado a la propia personalidad [...] implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana»⁵⁰.

Este concepto ha sido tratado tanto doctrinal como jurisprudencialmente desde dos puntos de vista o criterios: objetivo y subjetivo⁵¹, también denominados material o formal⁵².

Conforme a un criterio subjetivo o formal, el derecho a la intimidad comprendería aquellos ámbitos reservados de la vida privada y familiar que conforme a la voluntad del interesado deben quedar excluidos del conocimiento e intromisiones de los demás. Desde un punto de vista objetivo o material estarán protegidas por el derecho a la intimidad todas aquellas facetas de la vida privada que según el sentimiento

48 Lucena Cid, I. V., «El concepto de la intimidad en los nuevos contextos tecnológicos», en Galán Muñoz, A. (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, Tirant lo Blanch, 2014, p. 18.

49 *Vid.* STC 115/2000, de 5 de mayo, FJ 4.

50 *Vid.* STC 186/2000, de 10 de julio, FJ 5.

51 Rebollo Delgado, L., «Derecho al honor, derecho a la intimidad y a la propia imagen. Inviolabilidad del domicilio, secreto de las comunicaciones y límites al uso de las nuevas tecnologías», en García-Atance y García de Mora, M. V., Gutiérrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado, C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, pp. 180-181.

52 Díez-Picazo Giménez, L. M., «Sistema de Derechos Fundamentales», *cit.*, p. 281.

mayoritario de una concreta sociedad sean consideradas privadas y ajenas a los demás.

El problema que resolver se centra en determinar cuál de las concepciones indicadas ha de prevalecer. Como indica Díez-Picazo Giménez, «ni que decir tiene que, si se adopta un criterio formal, la extensión de la esfera privada variará de una persona a otra, dependiendo de cuán celoso de la propia intimidad sea cada uno; si se adopta un criterio material, en cambio, la extensión de la esfera privada será tendencialmente la misma para todos»⁵³. Se plantea entonces el interrogante de si cada persona puede decidir qué aspectos de la vida privada han de quedar excluidos del conocimiento de los demás.

La jurisprudencia constitucional, aunque se ha inclinado más a favor de un criterio objetivo o material⁵⁴, se ha pronunciado a favor de ambos conceptos, entendiendo que desde el punto de vista subjetivo cada persona puede reservarse un espacio resguardado de la curiosidad ajena⁵⁵.

Doctrinalmente, se han defendido ambas posturas igualmente, existiendo autores que señalan que, en todo caso, en el derecho a la intimidad subsiste un acentuado carácter subjetivo que podría cambiar dependiendo de la persona e incluso de una sociedad a otra, llegándose a denominar a la intimidad como el elemento de la desconexión social⁵⁶. Otros autores, sin embargo, se han inclinado por un criterio objetivo o material, entendiendo que el derecho a la intimidad se ha de entender en clave predominantemente objetiva o material, considerando que una construcción de índole formal o subjetiva se encuentra llena de riesgos⁵⁷.

53 Díez-Picazo Giménez, L. M., «Sistema de Derechos Fundamentales», *cit.*, p. 281.

54 Pueden mencionarse, entre otras, las SSTC 143/1994, de 9 de mayo, FJ 6, y 207/1996, de 16 de diciembre, FJ 3, en las que con cita de otras numerosas sentencias se declaró que el derecho a la intimidad «implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de vida humana».

55 La STC 134/1999, de 15 de julio, FJ 5, con cita de numerosas sentencias declaró que «el derecho a la intimidad salvaguardado en el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean estos poderes públicos o simples particulares, que está ligado al respeto de su dignidad», así como que «el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia de una publicidad no querida. El art. 18.1 C.E. no garantiza una “intimidad” determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público».

56 *Vid.* Rebollo Delgado, L., «Derecho al honor, derecho a la intimidad y a la propia imagen. Inviolabilidad del domicilio, secreto de las comunicaciones y límites al uso de las nuevas tecnologías», *cit.*, p. 183.

57 *Vid.* Díez-Picazo Giménez, L. M., «Sistema de Derechos Fundamentales», *cit.*, p. 282.

Sin embargo, para modular ambos criterios, finalmente nuestra jurisprudencia acogió la doctrina de la «idea de la expectativa razonable de la privacidad».

2.2. Idea de la expectativa razonable de la privacidad

Ante la confrontación entre los criterios objetivo y subjetivo del derecho a la intimidad, esta teoría constituye un criterio válido para establecer si nos encontramos ante una manifestación de la vida privada que ha de ser protegida ante cualquier intromisión. Se trata de la «expectativa razonable» que toda persona tiene sobre sí se encuentra amparada ante cualquier observación ajena. Este concepto fue establecido por la jurisprudencia de EE. UU. en el caso *Katz v. United States*⁵⁸ y ha sido recogido por el TEDH⁵⁹.

El fundamento que sustenta esta doctrina radica en la circunstancia de que no pueden abrigarse expectativas razonables de privacidad cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean pueden ser claramente objeto de registro o de información pública. De este modo, la protección constitucional del derecho a la intimidad se dará en las situaciones en las no es razonable que la propia persona, o cualquier otra en similares circunstancias, considere que sus acciones se someten al conocimiento ajeno, mientras que no gozará de protección el ciudadano que sea consciente de que su actividad puede trascender a terceros.

Dicho en palabras de Rodríguez Lainz, «el enunciado de esta doctrina podía resumirse en la siguiente máxima: Un ciudadano no puede ser sometido a una injerencia sobre su privacidad con la que no pudiera contar en términos razonables»⁶⁰.

También el TC ha seguido esta doctrina, declarando qué ámbito de cobertura del derecho a la intimidad viene determinado por la existencia en el caso de una expectativa razonable de privacidad o confidencialidad⁶¹.

58 En el caso *Katz v. United States*, resuelto por Sentencia del Tribunal Supremo de EE. UU. el 18 de diciembre de 1967, quedó acreditado que Charles Katz usó una cabina telefónica pública para transmitir información sobre apuestas ilegales desde Los Ángeles a Miami y Boston. Sin que Katz lo supiera, el FBI estaba grabando sus conversaciones a través de un dispositivo de escucha electrónico conectado al exterior de la cabina. Katz fue condenado con base en estas grabaciones. Argumentó en su recurso que las grabaciones se obtuvieron con violación de los derechos de la cuarta enmienda. El Tribunal Supremo estimó el recurso considerando que hubo intromisión ilegítima por parte del FBI, dado que, al haber cerrado la puerta de la cabina, se mantenía intacta la expectativa razonable del Sr. Katz de que su intimidad se encontraba preservada.

59 *Vid.* STEDH de 25 de septiembre de 2001, P.G. y J.H. c. Reino Unido, § 57, y STEDH de 28 de enero de 2003, Peck c. Reino Unido, § 58.

60 Rodríguez Lainz, J. L., «El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre», *Diario La Ley - Sección Doctrina*, n.º 8122, 2013, p. 2.

61 STC 170/2013, de 7 de octubre, FJ 5, entre otras, la cual declara: «[...] hemos tenido ocasión de precisar que el ámbito de cobertura de este derecho fundamental viene determinado por la existencia en el caso de una expectativa razonable de privacidad o confidencialidad. En concreto,

Por su parte, el TS, en la Sentencia 610/2016, de 7 de julio, se refirió a la expectativa razonable de privacidad al realizar un completo estudio de la jurisprudencia del TEDH dictada en relación con el derecho a la intimidad, así como de la STEDH de 25 de septiembre de 2001, P.G. y J.H. c. Reino Unido, del derecho comparado y de las resoluciones del TC relativas al derecho a la intimidad⁶².

2.3. Derecho a la intimidad e investigación tecnológica

La necesidad de intervención de la sociedad y de los sistemas que gobiernan esta ya se hizo necesaria en el ámbito del derecho a la intimidad en 1890 a propósito de la publicación por Warren y Brandeis del artículo «The Right to Privacy», en el cual denunciaban la captura de imagen a distancia y sin permiso a través de fotografías y la distribución de estas en la prensa⁶³.

Un siglo después, de una forma similar, como consecuencia del desarrollo de las TIC, surgieron nuevos contenidos del derecho a la intimidad, concretados en los aspectos de la vida privada a los que eventualmente podrían tener acceso no autorizado terceras personas a través de la tecnología digital. Tales accesos indebidos a la vida privada de los demás se mostraron como consecuencia de la aparición de internet y las redes sociales, así como por otras tecnologías como la videovigilancia, el conocimiento de la ubicación de una persona a través de GPS (*global positioning systems*) y también, cómo no, en los casos de diligencias de investigación tecnológica del delito, que, como se ha venido exponiendo, hicieron necesaria igualmente la intervención de la sociedad, dando lugar a una revisión de la definición del derecho a la intimidad.

hemos afirmado que un criterio a tener en cuenta para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente a intromisiones ilegítimas es el de las expectativas razonables que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observación o del escrutinio ajeno. Así, por ejemplo, cuando se encuentra en un paraje inaccesible o en un lugar solitario debido a la hora del día, puede conducirse con plena espontaneidad en la confianza fundada de la ausencia de observadores. Por el contrario, no pueden abrigarse expectativas razonables al respecto cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean, claramente pueden ser objeto de registro o de información pública (SSTEDH de 25 de septiembre de 2001, P.G. y J.H. c. Reino Unido, § 57, y de 28 de enero de 2003, Peck c. Reino Unido, § 58)».

62 En su FJ 1, la STS 610/2016 declara: «Son la intensidad de la injerencia y el factor tiempo los que hacen que la medida afecte claramente a esa expectativa razonable de privacidad que inspira la doctrina del caso Katz».

63 Señalaron estos autores en 1890 que «es un principio tan viejo como el *common law* que el individuo debe gozar de total protección en su persona y en sus bienes, sin embargo, resulta necesario, de vez en cuando, redefinir con precisión la naturaleza y la extensión de esta protección. Los cambios políticos, sociales y económicos imponen el reconocimiento de nuevos derechos, y el *common law*, en su eterna juventud, evoluciona para dar cabida a las demandas de la sociedad». Vid. Lucena Cid, I. V., «El concepto de la intimidad en los nuevos contextos tecnológicos», *cit.*, p. 16.

En efecto, como consecuencia de la irrupción de las TIC, se produce una ampliación en el contenido del derecho a la intimidad. Como declaró el TC, al resolver un recurso de amparo en el que se planteaba la vulneración del derecho a la intimidad como consecuencia de una investigación policial, «es evidente que cuando su titular navega por internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc.»⁶⁴.

En cualquier caso, el derecho a la intimidad, tal y como ha declarado el TC, no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes siempre que el recorte que aquel haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo y proporcionado para alcanzarlo, siendo en todo caso respetuoso con el contenido esencial del derecho⁶⁵.

Respecto a los intereses constitucionalmente relevantes, el TC ha considerado incluida dentro de estos a la investigación del delito, declarando que la intromisión es imprescindible para asegurar la defensa del interés público que se pretende defender mediante el ejercicio del ius puniendi⁶⁶.

Asimismo, el TEDH ha declarado, al resolver un caso en el que se denunciaba la violación del derecho a la intimidad como consecuencia de una diligencia de investigación tecnológica, que para la legítima injerencia se han de cumplir los requisitos del apartado 2 del art. 8 del CEDH, es decir, se ha de determinar si la medida está prevista por la ley y si es necesaria en una sociedad democrática⁶⁷.

Cuando concurran tales exigencias, o, en su caso, cuando medie el consentimiento del interesado, no será ilegítima la afectación o injerencia en el derecho a la intimidad, y, como ha declarado nuestro TC, «tampoco podrá ser calificada de ilegítima aquella injerencia o intromisión en el derecho a la intimidad que encuentra su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos, siempre y cuando se respete el contenido esencial del derecho»⁶⁸.

64 *Vid.* STC 173/2011, de 7 de noviembre, FJ 3.

65 *Vid.* SSTC 57/1994, de 28 de febrero, FJ 5, y 143/1994, de 9 de mayo, FJ 6, entre muchas otras.

66 *Vid.* SSTC 37/1989, de 15 de febrero, FJ 8; y 207/1996, de 16 de diciembre, FJ 4.

67 *Vid.* STEDH de 30 de mayo de 2017, caso Trabajo Rueda c. España, apdo. 28.

68 *Vid.* STC 159/2009, de 29 de junio, FJ 3.

3. Derecho al secreto de las comunicaciones

El derecho al secreto de las comunicaciones se encuentra protegido, junto con los demás derechos que en general comprenden el derecho a la vida privada, por el art. 12 de la Declaración Universal de Derechos Humanos de 19 de diciembre de 1948, el art. 8 CEDH y el art. 17 del Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966, y ampara a toda persona física o jurídica contra cualquier injerencia en el ámbito de su libertad a comunicarse libremente con los demás, impidiendo que el contenido de la comunicación sea conocido por terceros.

Asimismo, el derecho se encuentra reconocido en el art 7 de la Carta de Derechos Fundamentales de la UE, que dispone que «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones».

El art. 18.3 de nuestra Constitución dispone que «se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

Afirma Rebollo Delgado que el texto constitucional realiza una precisión, a su juicio improcedente, al referirse, en especial, a las comunicaciones postales, telegráficas y telefónicas, señalando que «hubiera sido mejor no haber delimitado los tipos de comunicaciones, sobre todo por lo vertiginoso de la evolución de estos, y haber hecho una protección genérica del secreto de las comunicaciones o de las telecomunicaciones». No obstante, como también afirma el referido autor, el precepto constitucional ha de interpretarse de forma «amplia y flexible»⁶⁹ y, por tanto, de forma extensiva a las comunicaciones que tengan lugar a través de cualquier medio tecnológico, habiéndose pronunciado el TS en idéntico sentido⁷⁰.

En cualquier caso, de conformidad con las disposiciones citadas, es lo cierto que nos encontramos ante un derecho fundamental de todos, cuya restricción supondría una invasión en la esfera privada del afectado y, por tanto, un ataque a su intimidad. Ello lleva, en primer lugar, a indagar acerca de la delimitación entre el derecho a la intimidad y el derecho al secreto de las comunicaciones.

69 Rebollo Delgado, L., «Derecho al honor, derecho a la intimidad y a la propia imagen. Inviolabilidad del domicilio, secreto de las comunicaciones y límites al uso de las nuevas tecnologías», *cit.*, p. 193.

70 *Vid.* STS 714/2016, de 26 de septiembre, FJ 6, que declara que «el derecho al secreto de las comunicaciones puede considerarse una plasmación singular de la dignidad de la persona y del libre desarrollo de su personalidad, que constituyen el fundamento del orden político y de la paz social (STC n.º 281/2006, de 9 de octubre y STS n.º 766/2008, de 27 de noviembre), por lo que trasciende de mera garantía de la libertad individual, para constituirse en medio necesario para ejercer otros derechos fundamentales. Por ello la protección constitucional del secreto de las comunicaciones abarca todos los medios de comunicación conocidos en el momento de aprobarse la norma fundamental, y también los que han ido apareciendo o puedan aparecer en el futuro, no teniendo limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse (SSTS n.º 367/2001, de 22 de marzo y n.º 137/1999, de 8 de febrero)».

3.1. Delimitación entre los derechos a la intimidad y secreto de las comunicaciones

Como derecho, el secreto de las comunicaciones «tuvo un reconocimiento en los textos constitucionales muy anterior al derecho a la intimidad, quedando recogido por primera vez en los arts. 7 y 8 de la Constitución de 1869, y reconocido de nuevo en las de 1876 (art. 7) y 1931 (art. 32)»⁷¹. Por otra parte, «aun cuando dicho derecho claramente se relacione con el derecho fundamental a la “intimidad” [...] no se identifica absolutamente con él, sino que posee un contenido mucho más amplio»⁷².

La primera cuestión que destacar, tras el examen del art. 18 CE, radica en la circunstancia de que para que pueda producirse una injerencia en el derecho al secreto de las comunicaciones es necesaria una resolución judicial, lo cual no se produce del mismo modo ante cualquier vulneración del derecho a la intimidad. En este sentido, no todas las intervenciones de las FCSE necesitarán una orden judicial cuando se trate de una actuación que pueda vulnerar la intimidad, mientras que, si se trata de una intromisión restrictiva del derecho al secreto de las comunicaciones (a salvo de los supuestos establecidos en el art. 579.3 y 4 LECrim⁷³ para la intervención de la correspondencia escrita y telegráfica y en el art. 588 ter d.3 LECrim⁷⁴ para la

71 Vid. Rebollo Delgado, L., *El derecho fundamental a la intimidad*, Madrid, Dykinson, 2000, pp. 58-60. Citado por Megías Quirós, J. J., «Privacidad e internet: intimidad, comunicaciones y datos personales», *Anuario de Derechos Humanos - Nueva Época*, n.º 3, 2002, p. 546.

72 Gimeno Sendra, J. V., *Manual de Derecho Procesal Penal*, cit., p. 407.

73 Establecen los apartados 3 y 4 del art. 579 de la LECrim para la detención y apertura de la correspondencia escrita y telegráfica lo siguiente:

«3. 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.

4. No se requerirá autorización judicial en los siguientes casos:

- a) Envíos postales que, por sus propias características externas, no sean usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías o en cuyo exterior se haga constar su contenido.
- b) Aquellas otras formas de envío de la correspondencia bajo el formato legal de comunicación abierta, en las que resulte obligatoria una declaración externa de contenido o que incorporen la indicación expresa de que se autoriza su inspección.
- c) Cuando la inspección se lleve a cabo de acuerdo con la normativa aduanera o proceda con arreglo a las normas postales que regulan una determinada clase de envío».

74 El art. 588 ter d.3 LECrim reproduce el contenido del art. 579.3 que acaba de citarse.

interceptación de las comunicaciones telefónicas y telemáticas), exigirá en todo caso la correspondiente autorización judicial.

Efectivamente, tal y como ha declarado el TC en relación con el derecho a la intimidad, y a diferencia de otras medidas restrictivas de derechos fundamentales como la intervención de las comunicaciones, «no existe en la Constitución reserva absoluta de previa resolución judicial», señalando, asimismo, que, aun cuando previamente se había declarado que la limitación del ámbito constitucionalmente protegido del derecho a la intimidad era solo posible por decisión judicial, ello no descarta la posibilidad de que «en determinados casos y con la conveniente habilitación legislativa [...], tales actuaciones pudieran ser dispuestas por la Policía Judicial»⁷⁵.

Como segunda diferencia —con la que se delimita más nítidamente el derecho al secreto de las comunicaciones en relación con el derecho a la intimidad—, doctrinalmente se ha señalado que «estriba en el sistema adoptado para hacer efectiva la protección de cada uno de los derechos: un sistema formal (secreto) frente a un sistema material, basado en el contenido»⁷⁶. A diferencia del derecho a la intimidad, en el que debe examinarse el contenido sobre el que ha tenido lugar la injerencia para determinar si pertenece al ámbito de lo privado, en el derecho al secreto de las comunicaciones, su contenido, como su propio nombre indica, se encuentra incluido dentro del concepto de secreto, estableciéndose así un concepto formal que «no necesita en modo alguno analizar el contenido de la comunicación —o de sus circunstancias— para determinar su protección por el derecho fundamental»⁷⁷. Es lo que otros autores denominan «garantía formal de intangibilidad», dado que las comunicaciones son de acceso reservado en cuanto tales, y ello por cuanto lo decisivo no es el contenido, es decir, lo que se transmite en la comunicación, sino el continente,

75 Vid. STC 70/2002, de 3 de abril, FJ 10, la cual añadió que «la regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que solo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad».

76 Frígols i 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, Javier (dir.), Jareño Leal, A. (coord.), *La protección jurídica de la intimidad*, Madrid, Lustel, 2010, p. 42.

77 Frígols i 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», *cit.*, p. 42.

o lo que es lo mismo, poder transmitirlo sin que lo sepan los demás, incluido el Estado⁷⁸.

En otras palabras, puede afirmarse que el derecho que nos ocupa se configura en torno al concepto de secreto con la finalidad de poder comunicarse libremente, y ello independientemente de que el contenido del mensaje deba incluirse dentro de la esfera privada del individuo y de que pueda o no tener la cualidad de íntimo.

En efecto, tal y como estableció la STC 114/1984, de 29 de noviembre, FJ 7, la cual sigue siendo un referente en esta materia, «el bien constitucionalmente protegido es así—a través de la imposición a todos del “secreto”— la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje —con conocimiento o no del mismo— o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)», declarando, asimismo, que, «sea cual sea el ámbito objetivo del concepto de “comunicación”, la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia *erga omnes*) ajenos a la comunicación misma»⁷⁹.

Posteriormente, se dieron otros pronunciamientos acerca de este aspecto definitorio del derecho, entre los que cabe destacar la STC 34/1996, de 11 de marzo, FJ 4, que declaró de forma similar que, «en definitiva, se pretende garantizar así la “impenetrabilidad de la comunicación” por terceros con eficacia *erga omnes*, tanto para los ciudadanos de a pie como para los agentes de los poderes públicos y abstracción hecha de la “dimensión material del secreto”, lo que se transmite».

Finalmente, en torno a la delimitación entre el derecho al secreto de las comunicaciones y el derecho a la intimidad, ha tenido lugar una particular polémica al plantearse la cuestión de si las comunicaciones en las que el proceso comunicativo ya ha concluido se encontrarían protegidas por el derecho al secreto de las comunicaciones o por el derecho a la intimidad.

Inicialmente el TC declaró que «la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos»⁸⁰.

78 Díez-Picazo Giménez, L. M., «Sistema de Derechos Fundamentales», *cit.*, pp. 298-299.

79 La STC 114/1984, de 29 de noviembre, FJ 7, declaró 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», señalando que esta condición formal del secreto de las comunicaciones constituye una presunción *iuris et de iure* de que lo comunicado es secreto en un sentido sustancial.

80 *Vid.* STC 70/2002, de 3 de abril, FJ 9.

En la misma línea se ha pronunciado el TS, considerando que la garantía dispensada por el derecho al secreto de las comunicaciones termina con la comunicación. En este sentido, ha declarado 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. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya protección constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones»⁸¹.

Sin embargo, en otra de sus resoluciones, el TC estimó que el derecho al secreto de las comunicaciones se extiende más allá de la finalización de la comunicación, al precisar que este derecho comprende también los datos registrados durante el proceso de comunicación, «con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso»⁸². En términos similares se pronunció la STC 230/2007, de 5 de noviembre, que, con cita de la STEDH de 3 de abril de 2007, caso Copland c. Reino Unido, apdo. 43, declaró vulnerado el secreto de las comunicaciones por el acceso policial al registro de llamadas de un terminal móvil⁸³. También el TS se ha pronunciado en el mismo sentido en alguna de sus resoluciones⁸⁴.

Posteriormente, el TC ha mantenido que los mensajes ya leídos quedan protegidos por el derecho a la intimidad y no por el derecho al secreto de las comunicaciones. Concretamente, en la STC 173/2011, de 7 de noviembre, FJ 3, ha señalado que «a esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no solo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o

81 *Vid.* STS 342/2013, de 17 de abril, FJ 8.

82 *Vid.* STC 123/2002, de 20 de mayo, FJ 6.

83 La STC 230/2007, de 5 de noviembre, FJ 2, declara que, «con los antecedentes expuestos, debe concluirse, conforme también interesa el Ministerio Fiscal, que se ha vulnerado al recurrente el derecho al secreto de las comunicaciones (art. 18.3 CE), en tanto que, acreditado y reconocido por las resoluciones judiciales el presupuesto fáctico del acceso policial al registro de llamadas del terminal móvil intervenido al recurrente sin su consentimiento ni autorización judicial, 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 garantizado por el art. 18.3 CE y, por tanto, que resulta necesario para acceder a dicha información, en defecto de consentimiento del titular del terminal telefónico móvil intervenido, que se recabe la debida autorización judicial. Ello supone la imposibilidad de valoración de dicha prueba al tener que quedar excluida del material probatorio apto para enervar la presunción de inocencia, en tanto que obtenida con vulneración de derechos fundamentales del recurrente».

84 *Vid.* STS 156/2008, de 8 de abril, FJ 4.

email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado».

En cualquier caso, y no obstante la aparente discrepancia entre las resoluciones mencionadas, de la lectura de estas no se desprende estrictamente la existencia de divergencias jurisprudenciales, teniendo en cuenta que, en los casos en los que tanto el TC como el TS se han pronunciado en favor de la protección por el derecho al secreto de las comunicaciones, incluso una vez concluido el proceso comunicativo, lo ha sido cuando se ha tratado de determinados datos de tráfico y no así del contenido de la comunicación. En este sentido, la doctrina constitucional mencionada ha mantenido sin vacilaciones que la visualización de un mensaje una vez que este ha sido abierto y leído por su destinatario no vulnera el derecho al secreto de las comunicaciones sino el derecho a la intimidad.

La distinción tiene gran importancia teniendo en cuenta, fundamentalmente, que, en atención al derecho vulnerado, será necesario el requisito de la jurisdiccionalidad para la intervención policial, ya que para la injerencia en el secreto de las comunicaciones será siempre necesaria autorización judicial, pero no así en aquellos casos en los que la Policía Judicial pueda llevar a cabo una intervención que no vulnere el secreto de las comunicaciones y sí, levemente, el derecho a la intimidad.

La conclusión más congruente, tal y como se colige de la doctrina jurisprudencial citada, es aquella conforme a la que, con independencia de que un mensaje haya sido leído o una llamada haya finalizado, no lleva aparejada una desprotección del derecho al secreto de las comunicaciones en relación con los datos que han quedado almacenados o se han originado como consecuencia del proceso de comunicación, como podría ser el listado de llamadas efectuadas registrado en un teléfono.

No obstante, como se verá más adelante, los datos almacenados una vez concluido el proceso de comunicación no siempre quedarán protegidos por el derecho al secreto de las comunicaciones, pudiendo en determinados supuestos quedar protegidos por el derecho a la protección de datos de carácter personal del art. 18.4 CE.

3.2. Concepto de comunicación

Resulta necesario referirse al concepto de «comunicación», como elemento imprescindible para que el derecho al secreto de las comunicaciones despliegue su eficacia, construyéndose este concepto a partir de los elementos del proceso comunicativo que se encuentran amparados por el secreto.

Es de reseñar que, tal y como señala la STC 70/2002, de 3 de abril, FJ 9, «ciertamente 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 esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE».

De forma parecida, la Circular 1/2013 de la FGE señala que «los imparable avances tecnológicos ponen en manos no solo de los poderes públicos sino incluso de los particulares enormes poderes que potencialmente son una amenaza para el secreto de las comunicaciones, lo que exige reinterpretar este derecho y afinar el sistema de garantías para proteger la privacidad humana»⁸⁵, añadiendo que «como ha declarado el TC “en una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no solo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo”»⁸⁶.

Aceptado este nuevo entendimiento del concepto de comunicación, cabría referirse a una nueva noción que, dejando aparte la comunicación postal, comprendiese todas las comunicaciones electrónicas. 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, en su artículo 2.d definió comunicación, a los efectos de esta, como «cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público»⁸⁷.

Doctrinalmente se ha propuesto una definición más ajustada a todas las posibilidades que demanda el mundo de las nuevas tecnologías, considerando que debe concebirse la comunicación como «la transmisión, compartición o intercambio de información entre dos o más sujetos determinados o determinables, dirigida a través de determinados canales de comunicaciones que son gestionados por terceras personas o entidades, en quienes se confía no solo su buen fin, sino también la confidencialidad en su gestión frente al conocimiento ajeno»⁸⁸.

Finalmente, cabe destacar que la vulneración del secreto no se producirá cuando la intervención de la comunicación se produzca de modo directo, sin intervención técnica alguna. Como ha señalado el TC, para que se produzca la limitación del derecho se 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 comunicación⁸⁹.

85 Fiscalía General del Estado, Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, *cit.*

86 STC 123/2002, de 20 de mayo, FJ 5.

87 Esta definición se encuentra posteriormente reproducida literalmente en el art. 64.c del Real Decreto (RD) 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.

88 *Vid.* Rodríguez Lainz, J. L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», *Diario La Ley*, n.º 8143, 2013, p. 2.

89 ATC 15/2004, de 20 de enero, FJ 4.

3.3. Elementos de la comunicación protegidos por el derecho

La definición expuesta anteriormente del término comunicaciones nos muestra los cuatro elementos fundamentales que constituyen el contenido del proceso comunicativo, los que, como se dijo al inicio de este apartado, se encuentran protegidos por el secreto. Estos elementos son, el comunicador o emisor, el interlocutor o receptor, la información compartida y un tercero prestador del servicio de comunicación, quien «se encuentra unido a los interlocutores por vínculos de confidencialidad, lo que caracterizará a la comunicación amparada por el secreto»⁹⁰. A ellos hay que añadir los datos de tráfico o asociados, que son aquellos que se generan como consecuencia del establecimiento de comunicación de forma externa a esta y que pueden facilitar los elementos que la identifican.

3.3.1. La información compartida

En cuanto a la información compartida o contenido de la comunicación, aunque la información que se transmite o comparte es esencial para la existencia de una comunicación, no es menos cierto que «el carácter formal del derecho al secreto de las comunicaciones convierte a la integridad del procedimiento de comunicación en el núcleo de la cuestión»⁹¹. Por tanto, lo que se comunica no es lo más relevante a los efectos de la protección constitucional dispensada por el derecho. Sin embargo, ello no obsta para que el contenido de la comunicación se configure como el núcleo central del proceso en el que la comunicación consiste, encontrándose protegidas por el derecho todas las formas que puede tener este, tales como voz, mensajes escritos electrónicos o archivos de audio o vídeo.

3.3.2. Los intervinientes en el proceso de comunicación

Respecto del comunicador o emisor y el interlocutor o receptor, esto es, las personas que intervienen en el proceso, la jurisprudencia del TC ya declaró en la meritada STC 114/1984, de 29 de noviembre, que el término «secreto» cubre, además del contenido de la comunicación, otros aspectos de esta como, por ejemplo, la identidad subjetiva de los interlocutores o corresponsales⁹². Ha de señalarse que debe tratarse de una comunicación entre personas físicas, habiendo declarado la STC 281/2006, de 9 de octubre, FJ 3, que «las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana».

90 Rodríguez Lainz, J. L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», *cit.*, p. 2.

91 González-Cuéllar Serrano, N., «Garantías constitucionales de la persecución penal en el entorno digital», en Díaz Maroto y Villarejo, J. y otros, *Derecho y Justicia Penal en el Siglo XXI*, Madrid, Colex, 2006, p. 903.

92 Posteriormente otras SSTC lo han declarado igualmente. Así, por ejemplo, la 70/2002, de 3 de abril, FJ 9, o la 142/2012, de 2 de julio, FJ 3.

No obstante estas menciones referentes a la necesidad de que sean personas humanas las que intervienen en el proceso, no es posible negar la titularidad del derecho a las personas jurídicas, lo que ha sido afirmado por la jurisprudencia del TEDH al declarar que el domicilio «incluye también la oficina registrada de una empresa dirigida por un particular, así como la oficina registrada de una persona jurídica, sucursales y otros locales comerciales»⁹³.

Se trata de una cuestión que del mismo modo ha sido reiteradamente declarada por la jurisprudencia del TS, que, en muchas de sus sentencias, ha puesto de manifiesto que son titulares del derecho «las personas físicas y las jurídicas tanto nacionales como extranjeras, mayores y menores de edad, porque el secreto de las comunicaciones presupone la libertad, y su restricción se produce en un sentido de control y observación y no propiamente de impedimento a las comunicaciones y se extiende tanto al conocimiento del contenido de las mismas, como a la identidad de los interlocutores»⁹⁴.

Sin embargo, no se encuentran protegidos por el derecho los diálogos entre dispositivos electrónicos o informáticos que se generan de forma automática, respecto de lo que tanto el TC como el TS han declarado, que «las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana»⁹⁵, tratándose de un criterio compartido por la FGE, que se ha pronunciado en idéntico sentido⁹⁶.

Finalmente, en relación con los intervinientes en el proceso de comunicación, cabe referirse a las comunicaciones que tienen lugar a través de las redes sociales (Facebook, Twitter, YouTube, redes P2P, etc.), en las cuales no puede hablarse de privacidad, dado que la información transmitida a través de ellas es de acceso público, por lo que estas no se encuentran protegidas por el derecho fundamental, habiendo señalado el TS que «no se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma»⁹⁷.

3.3.3. El tercero prestador del servicio

En cuanto al tercero prestador del servicio de comunicación unido a los interlocutores por vínculos de confidencialidad, se trata de una intervención necesaria para la consecución de la comunicación, la cual no sería posible sin que por este se facilitasen los medios para que se llevase a efecto.

93 Vid. SSTEDH de 27 de septiembre de 2005, caso Petri Sallinen y otros c. Finlandia, apdo. 70, y de 14 de marzo de 2013, caso Bernh Larsen Holding AS y otros c. Noruega, apdo. 104.

94 Vid. SSTS 1295/1999, de 21 de septiembre, FJ 2, 132/1997, de 8 de febrero FJ 2, y 276/1996, de 2 de abril, FJ 6.

95 Vid. STC 281/2006, de 9 de octubre, FJ 3, y STS 766/2008, de 27 de noviembre, FJ 3.

96 Fiscalía General del Estado, Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, *cit.*, p. 11.

97 Vid. STS 236/2008, de 9 de mayo, FJ 2.

Respecto al vínculo de confidencialidad, es indispensable para la completa realización del derecho, encontrándose lógicamente enlazado con el secreto de la comunicación. Como señala Rodríguez Lainz, «la confidencialidad da contenido a lo que podríamos entender como dimensión interna del secreto de las comunicaciones»⁹⁸. El TC se ha referido al citado vínculo declarando que «el fundamento del carácter autónomo y separado del reconocimiento de este 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»⁹⁹.

Con base en lo anterior, y siendo necesaria la existencia de algún medio con el que se produzca la comunicación y la de un tercero que de soporte a este, para que pueda desplegar efectos el amparo constitucional ofrecido por el art. 18.3 CE, será preciso que el medio permita una comunicación secreta entre dos o más personas, por lo que están excluidas de la protección las conversaciones que tengan lugar en medios de comunicación en los que intervienen multitud de personas, como la radio o televisión.

Estarán, por tanto, afectadas por la garantía del derecho al secreto de las comunicaciones, debiendo respetar este, todas las personas ajenas al proceso comunicativo, independientemente de que sean particulares o los agentes de la Policía Judicial en el curso de una investigación, no afectando la garantía del derecho a los intervinientes en la comunicación, y ello sin perjuicio de que pudiera quedar vulnerado el derecho a la intimidad de alguno de ellos¹⁰⁰.

3.3.4. Los datos de tráfico o asociados

A los elementos anteriores, deben añadirse los datos de tráfico o asociados, los cuales se encuentran protegidos por la obligación de confidencialidad de un tercero prestador de servicios de comunicación, y cuya interceptación o entrega a la Policía Judicial por parte del citado tercero prestador de servicios sin el consentimiento del afectado o, en su defecto, con el soporte de la correspondiente resolución judicial supondría una vulneración del secreto de los referidos datos, lo que a su vez produciría una limitación del derecho al secreto de las comunicaciones.

98 Rodríguez Lainz, J. L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», *cit.*, p. 6.

99 *Vid.* STC 281/2006, de 9 de octubre, FJ 3.

100 El no quedar afectadas las personas intervinientes en la comunicación por la garantía del derecho ya quedó sentado tras la emblemática STC 114/1984, de 29 de noviembre, FJ 7, que declaró que «no hay “secreto” para aquel a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el artículo 18.3 de la Constitución la retención, por cualquier medio, del contenido del mensaje». Declaró, asimismo, que «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, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera “íntima” del interlocutor, pudiesen constituir atentados al derecho garantizado en el artículo 18.1 de la Constitución».

El Convenio de Budapest facilita una definición de los datos de tráfico en su art. 1.d), el cual establece que «por “datos sobre el tráfico” se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente».

Por su parte, la LECrim, tras la reforma operada por la LO 13/2015, se ha ocupado de los que ha denominado «datos electrónicos de tráfico o asociados al proceso de comunicación», concretamente en el art. 588 ter b.2, cuyo último párrafo ofrece igualmente una definición de estos, al disponer que se entenderá por tales datos «todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga». Se trata, por tanto, de datos no coincidentes con el contenido de la comunicación, aunque pueden facilitar todos los elementos que la identifican, tales como los datos necesarios para rastrear e identificar el origen de una comunicación; los necesarios para identificar su destino; los necesarios para determinar la fecha, hora y duración; los que sirven para identificar el tipo de comunicación, ya sea de voz, datos, mensajería o servicios multimedia, y, finalmente, los datos necesarios para identificar el equipo de comunicación de los usuarios.

La protección de los datos de tráfico por el derecho al secreto de las comunicaciones tiene su inicio con la STEDH de 2 de agosto de 1984, caso *Malone c. Reino Unido*, en la cual se determinó que los números de destino de las llamadas, recopilados por un sistema automático de recuento —denominado *comptage*—, aun cuando no suponen la interceptación del contenido de las conversaciones, son parte integrante de las comunicaciones telefónicas, y, por tanto, se encuentran protegidos por el derecho fundamental, por lo que no se puede disponer de estos sin el consentimiento de su titular¹⁰¹.

En nuestro país, puede afirmarse que el *leading case* en relación con la protección de los datos de tráfico lo constituye la STC 123/2002, de 20 de mayo, FJ 6, que siguiendo la referida doctrina del TEDH, estableció que los datos de tráfico «configuran el proceso de comunicación en su vertiente externa y son confidenciales, es decir, reservados del conocimiento público y general, además de pertenecientes a la propia esfera privada

101 Posteriormente, el TEDH, en la Sentencia de 3 de abril de 2007, caso *Copland c. Reino Unido*, declaró en su apdo. 43: «[...] el Tribunal recuerda que la utilización de información relativa a la fecha y duración de las conversaciones telefónicas y en particular los números marcados, puede plantear un problema en relación con el artículo 8, ya que dicha información es “parte de las comunicaciones telefónicas”». Y en el apdo. 44 señaló, del mismo modo, que, «en consecuencia, el 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».

de los comunicantes. El destino, el momento y la duración de una comunicación telefónica, o de una comunicación a la que se accede mediante las señales telefónicas, constituyen datos que configuran externamente un hecho que, además de carácter privado, puede asimismo poseer un carácter íntimo», declarando al mismo tiempo la necesidad de resolución judicial, en defecto del consentimiento del titular, para la cesión de los datos a la Policía Judicial en el marco de una investigación¹⁰².

3.4. Secreto de las comunicaciones e investigación tecnológica

El derecho al secreto de las comunicaciones, como los demás derechos fundamentales, no es absoluto, sino que se encuentra sujeto a unas limitaciones, como así ha sido señalado por la jurisprudencia, que ha declarado en numerosas resoluciones que en toda sociedad democrática existen determinados valores que pueden justificar, con las debidas garantías, su limitación, valores entre los que se incluye la prevención de las infracciones penales, como así lo dispone el apartado 2 del art. 8 del CEDH¹⁰³.

En este sentido, para una adecuada investigación del delito, la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, introdujo en nuestra legislación procesal penal una nueva diligencia de investigación de carácter tecnológico limitativa del derecho al secreto de las comunicaciones, consistente en la intervención de las comunicaciones telefónicas en el ámbito de la instrucción de las causas penales¹⁰⁴, que se articuló mediante una nueva redacción del art. 579 de la LECrim.

102 En relación con la necesidad de resolución judicial, la STC 123/2002, de 20 de mayo, FJ 6, declaró que «la aplicación de la doctrina expuesta conduce a concluir que la entrega de los listados por las compañías telefónicas a la policía sin consentimiento del titular del teléfono requiere resolución judicial, pues la forma de obtención de los datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE. En efecto, los listados telefónicos incorporan datos relativos al teléfono de destino, el momento en que se efectúa la comunicación y a su duración, 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 a efectos, bien de la lícita facturación del servicio prestado, bien de su ilícita difusión».

103 *Vid.* por todas la STS 720/2017, de 6 de noviembre, FJ 6, que declara que «en toda sociedad democrática existen determinados valores que pueden justificar, con las debidas garantías, su limitación (art. 8º del Convenio Europeo). Entre estos valores se encuentra la prevención del delito, que constituye un interés constitucionalmente legítimo y que incluye la investigación y el castigo de los hechos delictivos cometidos, orientándose su punición por fines de prevención general y especial. El propio art 18.3 CE prevé la limitación del derecho al secreto de las comunicaciones mediante resolución judicial (STS n.º 246/1995, de 20 de febrero, entre otras muchas)».

104 Con anterioridad a la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, únicamente se encontraba prevista en nuestra legislación la posibilidad de intervención de las comunicaciones telefónicas en la Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio, que en su art. 18, apartado 1, dispone que «cuando la autorización del Congreso comprenda la suspensión del artículo dieciocho, tres, de la Constitución, la autoridad gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y

Actualmente, las vigentes diligencias de investigación tecnológica pueden suponer una injerencia en el derecho, aunque no de una forma tan directa como con la interceptación de las comunicaciones telefónicas y telemáticas, por cuanto en determinados casos se plantearán dudas sobre el derecho fundamental afectado por la concreta intervención.

La obtención de datos protegidos por el derecho al secreto de las comunicaciones requiere, en todo caso, a diferencia del derecho a la intimidad y por imposición del art. 18.3 CE, una expresa autorización judicial¹⁰⁵, pudiendo incurrir, en caso de realizar la diligencia sin la debida autorización, en la ilicitud prevista en el art. 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

El derecho al secreto de las comunicaciones es susceptible de ser vulnerado principalmente y de forma evidente con la intervención de las comunicaciones telefónicas y telemáticas, pero también con otras diligencias de investigación tecnológica en las que pueden ser captadas conversaciones orales o telemáticas, como así sucede con la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos¹⁰⁶, y, de forma muy singular, mediante los

telefónicas. Dicha intervención solo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público», disponiendo, asimismo, en su apartado 2.º que «la intervención decretada será comunicada inmediatamente por escrito motivado al juez competente».

105 La STC 145/2014, de 22 de septiembre, FJ 2, declara que, «en relación con el derecho al secreto de las comunicaciones telefónicas, nuestra doctrina ha venido reiterando que las exigencias de motivación de las resoluciones judiciales que autorizan la intervención o su prórroga forman parte del contenido esencial del art. 18.3 CE. Dicho sintéticamente, éstas deben explicitar, en el momento de la adopción de la medida, todos los elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, en aras del respeto del derecho de defensa del sujeto pasivo de la medida. Por ello, el órgano judicial debe exteriorizar los datos o hechos objetivos que pueden considerarse indicios de la existencia del delito y de la conexión de la persona o personas investigadas con el mismo».

106 López Ortega, J. J., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (II): Captación y grabación de comunicaciones orales mediante dispositivos electrónicos. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización», *Formación a distancia-Consejo General del Poder Judicial*, n.º 3, 2016, p. 21. En relación con las diligencias de captación y grabación de comunicaciones orales, señala este autor que «la tercera modalidad de injerencia regulada en la LECRIM, a todas luces la más invasiva, es la captación y grabación de las conversaciones privadas (comunicaciones orales directas) del investigado en su domicilio o fuera de él (en la vía pública, en otro espacio abierto o en cualquier otro lugar cerrado). Aunque el legislador, acertadamente, ha diferenciado el régimen de las diversas medidas de observación y vigilancia en función de su gravedad, pues no todas afectan del mismo modo y con la misma intensidad al derecho a la intimidad, al regular las vigilancias acústicas las ha equiparado a la interceptación de las comunicaciones telefónicas. La opción del legislador es lógica, no solo porque las conversaciones telefónicas son las que gozan del más alto nivel de protección, sino también porque tras la STC 145/2014 se ha puesto fin a un amplio debate doctrinal sobre el derecho constitucional afectado por la escucha y grabación de las conversaciones entre presentes (comunicaciones orales directas), situando el núcleo de la

registros de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

4. Derecho a la protección de datos de carácter personal o autodeterminación informativa

4.1. Evolución y desarrollo del derecho

Como consecuencia de la irrupción de las TIC, se ha producido una revisión del concepto de intimidad acorde a la nueva realidad, que ha propiciado una ampliación en su contenido, al haber sido superada la anterior concepción por las posibilidades que las TIC ofrecen para captar, conservar, procesar o difundir datos que afectan a cualquier ciudadano en su actividad diaria.

En la actualidad, son numerosos los datos de cualquier persona que circulan por la red ubicándose en registros de organismos o entidades con fines lícitos, tales como el domicilio, documento de identidad, correo electrónico, datos de su tarjeta de crédito, numerosas contraseñas utilizadas para el acceso a portales de proveedores de cualquier servicio o redes sociales, e incluso documentos confidenciales como puede ser sencillamente el resultado de una analítica médica, un extracto bancario o la factura del proveedor de servicios de telefonía e internet, por citar algunos del amplio y heterogéneo elenco de los que podrían ser mencionados.

El uso indebido de tales datos, efectivamente, podría constituir una injerencia en el derecho a la intimidad, pero pronto se planteó, y ya nuestro constituyente de 1978 lo apreció así al redactar el art. 18.4 CE, el establecimiento de un derecho con nombre propio que protegiese a los ciudadanos del tráfico indebido de cualquier dato o conjunto de ellos de los que fuesen titulares, otorgando a cada individuo el poder de disponer sobre el destino que dar a estos.

Como se acaba de decir, y conforme afirma Galán Muñoz, el obligado punto de partida nos viene dado por nuestra Constitución, resultando ciertamente sorprendente que, encontrándonos en el momento de su elaboración y promulgación en una época en la que la informática se encontraba en los inicios de su desarrollo e implantación, el

tutela constitucional en el ámbito del derecho al secreto de las comunicaciones (art. 18.3 CE), a cuyo régimen legal ahora se asimilan». Efectivamente, la STC 145/2014, de 22 de septiembre, al resolver un caso relativo a las grabaciones realizadas al acusado en dependencias policiales, declara en su FJ 7, *in fine* que «de todo lo expuesto se deduce que las grabaciones en dependencias policiales resultaron contrarias al art. 18.3 CE, deviniendo nula la prueba obtenida por ese cauce para todos aquellos que resultaron perjudicados penalmente por ella». No obstante, existe alguna opinión doctrinal que considera que, si el fundamento de la protección del secreto de las comunicaciones se encuentra en la especial vulnerabilidad que se deriva de un tercero intermediario, resultaría difícil entender que este derecho puede resultar afectado por la instalación de un micrófono o mecanismos de grabación de las conversaciones orales directas, quedando afectado en todo caso con esta concreta medida de investigación el derecho a la intimidad. *Vid.* Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Las Rozas (Madrid), Wolters Kluwer, 2016, p. 458.

constituyente español tuviese en cuenta la importancia y peligrosidad que el fenómeno podía representar para los ciudadanos, recogiendo una previsión y un mandato expreso dirigido al legislador para que adoptase las oportunas medidas legales protectoras ante los posibles abusos que se pudiesen llevar a cabo con las tecnologías de la información¹⁰⁷.

Efectivamente, el art. 18 CE, después de garantizar los derechos a la intimidad, personal y familiar, el honor y la propia imagen, la inviolabilidad del domicilio y el secreto de las comunicaciones, dispone en su cuarto y último apartado que «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos», estableciendo así una norma que no es posible encontrar, con la salvedad de una previsión similar en la Constitución portuguesa¹⁰⁸, en otros textos constitucionales anteriores ni tampoco en las normas internacionales relativas a los derechos fundamentales.

Sin embargo, se necesitaba de una legislación de desarrollo, respecto de la cual el legislador no fue especialmente presto, regulándose inicialmente de manera insuficiente con la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que, en su redacción originaria, estableció en la posteriormente derogada disposición transitoria primera que, «en tanto no se promulgue la normativa prevista en el artículo dieciocho, apartado cuatro, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley».

En cualquier caso, y aunque el nuestro y el portugués fuesen los primeros textos constitucionales que se ocuparon de la materia, no puede decirse que en Europa no se tuviese en cuenta este importante asunto del tratamiento de los datos de carácter personal, dado que, con fecha 28 de enero de 1981 se aprobó el Convenio n.º 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, ratificado por España por instrumento de 27 de enero de 1984, que reguló de una forma amplia el tratamiento de los datos de carácter personal, estableciendo claramente su objeto en su art. 1, que bajo la

107 Galán Muñoz, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación», en Galán Muñoz, A. (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, Tirant lo Blanch, 2014, p. 206.

108 La Constitución portuguesa de 2 de abril de 1976 dispone en su art. 35, bajo la rúbrica «Utilización de la informática» lo siguiente: «1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos».

rúbrica «Objeto y fin» dispuso que «el fin del presente Convenio es garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (“protección de datos”)».

Como consecuencia del referido Convenio 108 del Consejo de Europa, en España se promulgó, como primera disposición que desarrolló con autonomía el art. 18.4 CE, la LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, que, aunque cumplía los requisitos para hacer efectivo el derecho¹⁰⁹, tuvo que ser adaptada a la normativa de la UE, que, el 24 de octubre de 1995, aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, origen de la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Por otra parte, la normativa española ha sido indudablemente influida por la jurisprudencia del TEDH y del TC. La STEDH de 26 de marzo de 1987 determinó, en relación con un registro secreto de la policía, que este contenía datos relativos a la vida privada, y que tanto el almacenamiento como su comunicación suponían una violación del derecho al respeto de su vida privada garantizado por el artículo 8.1¹¹⁰. Por su parte, la STEDH de 7 de julio de 1989 declaró la violación del respeto a la vida privada y familiar al no facilitarse al recurrente los datos obrantes en un ayuntamiento en relación con su infancia¹¹¹. Asimismo, la STEDH de 25 de febrero de 1997 determinó que se había producido la violación del derecho a la vida privada por la difusión de la

109 La derogada LO 5/1992, de 29 de octubre, regulaba todos los aspectos de la protección del derecho a la protección de datos, siendo relevante destacar la creación, a través de esta, de la actual Agencia Española de Protección de Datos, que regulaba en su título VI, promulgándose bajo su vigencia el RD 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, que se mantuvo vigente con la LO 15/1999, de conformidad con su disposición transitoria 3.ª Por otra parte, la exposición de motivos de la LO 5/1992 llevó a cabo una minuciosa exposición en relación con la protección del derecho. Entre otros muchos aspectos, señaló: «Los más diversos datos —sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado “dinero plástico”, sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideológicas, por poner solo algunos ejemplos— relativos a las personas podrían ser, así, compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquella a la que solo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos».

110 *Vid.* STEDH, de 26 de marzo de 1987, caso Leander c. Suecia, apdo. 48.

111 *Vid.* STEDH, de 7 de julio de 1989, caso Gaskin c. Reino Unido, apdo. 49.

identidad y enfermedad de una persona, circunstancias que constaban en una sentencia y fueron comunicadas a la prensa¹¹².

En cuanto a la jurisprudencia de nuestro TC, fue especialmente relevante, del mismo modo que la del TEDH, por el apoyo otorgado al legislador para la configuración constitucional del derecho. Como primeros pronunciamientos que otorgaron el amparo por la infracción del art. 18.4 CE, cabe destacar la STC 254/1993, de 20 de julio, en relación con la denegación a un ciudadano de una solicitud de información acerca de sus datos de carácter personal que obraban en ficheros automatizados de la Administración del Estado, o la STC 11/1998, de 13 de enero, en relación con un uso indebido por parte de una empresa del dato relativo a la afiliación sindical de un trabajador de esta¹¹³.

El siguiente paso de la UE, tras la Directiva 95/46/CE, fue el de la incorporación del derecho a la protección de datos en la Carta de Derechos Fundamentales de la UE, cuya vigente redacción es la que se dio a esta como consecuencia de su revisión en 2007 en Estrasburgo con carácter previo a la firma del Tratado de Lisboa.

La Carta tiene fuerza vinculante para todos los países de la Unión conforme al art. 6 del Tratado de la UE, excepto para Polonia y el Reino Unido¹¹⁴⁻¹¹⁵.

Tal y como se menciona en el sitio web de EUR-Lex, el cual da acceso al derecho y jurisprudencia de la UE, la Carta reafirma, dentro del respeto de las competencias y misiones de la Unión, así como del principio de subsidiariedad, los derechos que emanan, en particular, de las tradiciones constitucionales y las obligaciones internacionales comunes a los países de la UE, del CEDH, las Cartas Sociales adoptadas por la UE y por el Consejo de Europa, así como de la jurisprudencia del Tribunal de Justicia de la UE y del TEDH, añadiendo que, al dar mayor visibilidad y

112 *Vid.* STEDH, de 25 de febrero de 1997, caso Z c. Finlandia, apdo. 113.

113 Cabe señalar que, conforme se indica en el antecedente de hecho tercero de la STC 11/1998, de 13 de enero, resulta ilustrativo que la empresa había sido sancionada por los mismos hechos por la Agencia de Protección de Datos en resolución de 18 de diciembre de 1995, con una multa de 50.000.001 de pesetas (actualmente 300.506,06 €), por una infracción tipificada como muy grave en el art. 43.4 c) de la en aquel momento todavía no derogada Ley Orgánica 5/1992, de 29 de octubre.

114 El Tratado de la UE dispone su art. 6.1 que «la Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la UE de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados».

115 Polonia y el Reino Unido, con carácter previo a la aprobación del Tratado de Lisboa, introdujeron el protocolo n.º 30, conforme al cual, y tal y como se dispuso en su art. 2, «cuando una disposición de la Carta se refiera a legislaciones y prácticas nacionales, solo se aplicará en Polonia o en el Reino Unido en la medida en que los derechos y principios que contiene se reconozcan en la legislación o prácticas de Polonia o del Reino Unido».

claridad a los derechos fundamentales, establece una seguridad jurídica dentro de la UE¹¹⁶.

El derecho a la protección de datos de carácter personal se encuentra proclamado en el art. 8 de la Carta, que bajo la rúbrica «protección de datos de carácter personal» dispone: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente».

Posteriormente, la UE ha desarrollado una importante labor legislativa en materia de protección de datos. Así, el 12 de julio de 2002, como complemento a la Directiva 95/46/CE, se aprobó la Directiva 2002/58/CE, de tratamiento de datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas, con la pretensión de armonizar las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección; en particular, en relación con el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales de las comunicaciones electrónicas.

Asimismo, el 15 de marzo de 2006, fue publicada la Directiva 2006/24/CE, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o redes públicas de comunicaciones, por la que se modifica la Directiva 2002/58/CE. Esta directiva fue traspuesta a nuestro ordenamiento con la promulgación de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones¹¹⁷.

Más recientemente, en la UE se ha dictado el vigente Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPDUE), que deroga la Directiva 95/46/CE, encontrándose vigente desde el 25 de mayo de 2018. Asimismo, se ha aprobado el Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.

116 El sitio web de EUR-Lex se encuentra en la dirección <https://eur-lex.europa.eu/homepage.html>. La cita mencionada en relación con la Carta de derechos fundamentales de la Unión Europea, se encuentra en la extensión de la anterior <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISUM%3AI33501>. Consultado el 1 de julio de 2021.

117 La Directiva 2006/24/CE, de 15 de marzo, fue anulada por el Tribunal de Justicia de la UE por Sentencia de 8 de abril de 2014 dictada en los asuntos acumulados C-293/12 y C-594/12, pese a lo cual la Ley 25/2007, de 18 de octubre, que la traspuso, sigue vigente.

Con la aprobación del RGPDUE, y con la finalidad de adaptar a este el ordenamiento jurídico español, se ha promulgado en nuestro país la vigente LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales¹¹⁸, que deroga la LO 15/1999, por lo que, actualmente, la norma prevalente en materia de protección de datos viene constituida por el RGPDUE con las adaptaciones del ordenamiento jurídico español llevadas a cabo por la LOPD 2018.

Finalmente, debe señalarse que, el 27 de abril de 2016, el Parlamento Europeo y el Consejo aprobaron la Directiva 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. Aunque con bastante retraso, ya que el plazo de transposición finalizó el 6 de mayo de 2018, recientemente se ha dado cumplimiento a lo ordenado en la referida directiva, promulgándose la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

4.2. Régimen jurídico básico del derecho a la protección de datos de carácter personal

La idea fundamental en virtud de la cual puede desplegar sus efectos el derecho fundamental a la protección de datos radica en la circunstancia de que para la recogida, tratamiento y cesión de los datos de otra persona se debe disponer del consentimiento de esta.

El artículo 4.11 RGPDUE establece que se entenderá por consentimiento del interesado «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen». En relación con el consentimiento del interesado, el considerando n.º 32 RGPDUE prevé que «el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito,

118 La vigente LOPD 2018, conforme a su preámbulo, pretende lograr la adaptación del ordenamiento jurídico español al RGPDUE y completar sus disposiciones, estableciendo en su art. 1.a) que «el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el art. 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica». Es de destacar, asimismo, que, conforme se establece en el preámbulo de la LOPD 2018, «el Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa», añadiendo que «procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios».

inclusive por medios electrónicos, o una declaración verbal». Por su parte, el art. 9.1 RGPDUE prohíbe el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, excepto en los supuestos relativos al interés general que se detallan en el apartado 2 del citado precepto y en aquellos casos en los que el interesado hubiese dado su consentimiento explícito para el tratamiento de dichos datos personales, siempre y cuando el derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada no puede ser levantada por el interesado.

Por lo que a la investigación del delito se refiere, no será requisito imprescindible el consentimiento del interesado para la recogida y tratamiento de los datos personales, dado que, de acuerdo con lo dispuesto en el art. 236 ter.3 LOPJ, tras la redacción dada a este por la LO 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, «no será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba»¹¹⁹.

4.3. Autonomía de la protección de datos frente al derecho a la intimidad

Tal y como afirma Díez-Picazo Giménez, el mandamiento constitucional de limitación del tratamiento de datos, en principio, es una garantía para la efectividad de los derechos al honor y a la intimidad, conforme se expresa por el propio art. 18.4 CE,

119 Señala Pérez Gil, para diferenciar el tratamiento de datos de la recogida y cesión de estos, que el tratamiento se refiere a una operación o conjunto de operaciones sobre datos que deben encontrarse estructurados, ser accesibles y estar almacenados en ficheros, cronológicamente intermedio entre la recogida y su eventual conclusión, por lo que «lo relevante es observar que cuando la obtención de datos constituya la recopilación inicial de los mismos, estaremos ante un supuesto de recogida, mientras que será cesión cuando sea posterior en el tiempo al tratamiento». Indica el autor que se trata de una distinción de notable trascendencia, habida cuenta del diferente grado de injerencia en el derecho a la protección de datos de carácter personal, de la recogida y tratamiento en relación con la cesión, la cual constituye una actuación más gravosa para el titular de los datos que la mera recogida, siendo mayor su potencialidad lesiva del derecho a la protección de los datos de carácter personal. Esa diversa intensidad justifica que el art. 11 LOPD establezca precauciones suplementarias en relación con la cesión al marcar una serie de supuestos tasados en los que cabe prescindir del consentimiento del titular de los datos. Pérez Gil, J., González López, J. J., «Cesión de datos personales para la investigación penal. Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal», *Diario La Ley - Sección Doctrina*, n.º 7401, 2010, p. 10.

pesando en este sentido sobre el legislador un mandato para que la regulación del tratamiento de datos se realice de forma respetuosa con los derechos fundamentales¹²⁰.

Sin embargo, aunque inicialmente se pudo entender este derecho como una variedad del derecho a la intimidad, pronto el TC determinó la autonomía de la protección de datos de carácter personal respecto del derecho a la intimidad, no obstante la estrecha relación mantenida entre ambos.

Aun así, debe destacarse que, a nivel jurisprudencial, tuvo una gran relevancia para la consolidación de la autonomía del derecho la Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983¹²¹, que formuló el concepto de «autodeterminación informativa», el cual, posteriormente, ha sido usado por nuestro TC al ocuparse de la aludida delimitación entre ambos derechos.

Afirma Hoffmann-Riem que «este nuevo derecho fundamental se convirtió en la base de la moderna legislación alemana de protección de datos, en particular de las leyes generales de protección de datos, así como de numerosas reglas especiales sobre la protección de datos personales y de la consiguiente jurisprudencia»¹²².

La derogada LO 5/1992, de 29 de octubre, estableció el criterio básico diferenciador, reproducido en la LOPD 1999, disponiendo ambas normas orgánicas, en su art. 3.a, que se entenderá por datos de carácter personal «cualquier información concerniente a personas físicas identificadas o identificables».

Por su parte, el RGPDUE establece, en su art. 4.1, que se entenderá por «datos personales» toda información sobre una persona física identificada o identificable («el interesado»), considerando como tal «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

Por tanto, el acceso no autorizado a documentos o archivos en los que no consten datos que se refieran a personas identificadas o identificables ha de entenderse como

120 Díez-Picazo Giménez, L. M., «Sistema de Derechos Fundamentales», *cit.*, p. 308.

121 La Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983 se dictó como consecuencia de la controversia que se produjo en torno a la recolección de datos estadísticos conforme a la Ley del Censo, datos anónimos como el nombre y apellidos, domicilio, situación económica, profesión, etc., respecto de los cuales se declaró la facultad del individuo de decidir por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a su propia vida.

122 Hoffmann-Riem, W., «Innovaciones en la jurisprudencia del Tribunal Constitucional alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la sociedad de la información», *Revista de Derecho Constitucional Europeo*, vol. 11, n.º 22, 2014, p. 131.

una injerencia en el derecho a la intimidad del art. 18.1 CE, pero no como una vulneración del derecho a la protección de datos de carácter personal del art. 18.4 CE.

En todo caso, ha tenido especial importancia la delimitación de ambos derechos que llevó a cabo la jurisprudencia, siendo de destacar la STC 254/1993, de 20 de julio, FJ 6, que declaró que aunque nos encontramos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, estamos igualmente ante «un derecho o libertad fundamental, el derecho a la libertad frente a potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática». Especialmente relevante es, asimismo, la STC 292/2000, de 30 de noviembre¹²³.

De este modo, a partir principalmente de estas resoluciones del TC, se va conformando el derecho a la autodeterminación informativa o *habeas data*, entendido como el derecho de cualquier persona para solicitar y obtener la información que sobre su persona obre en cualquier base de datos, pública o privada, informática o no, con la potestad para que se proceda a su eliminación o actualización¹²⁴, teniendo en cuenta que, como afirma Bayo Delgado, «la protección de datos parte de la idea de que los datos pertenecen al sujeto a quien se refieren, sobre los que debe mantener su control (*habeas data*), salvo excepciones legalmente previstas»¹²⁵.

123 Declara esta sentencia en su FJ 6, que, a diferencia del derecho fundamental a la intimidad del art. 18.1 CE, cuya finalidad es la de proteger frente a cualquier invasión que pueda realizarse en el ámbito de la vida privada, «el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado», lo que «impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías», sin que el objeto de este derecho fundamental quede reducido solo a los datos íntimos de la persona «sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal», es decir, «todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

124 Resulta muy ilustrativa la definición que la STC 96/2012, de 7 de mayo, FJ 6, realiza del derecho a la protección de datos del art. 18.4 al declarar que «la llamada libertad informática es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención» y añadió en el FJ 7, que se refiere a cualquier dato que sea relevante o tenga incidencia en el ejercicio de cualesquiera derechos de la persona, «sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado».

125 Bayo Delgado, J., «La protección de datos en la investigación policial y en el proceso penal», *Jueces para la Democracia. Información y Debate*, n.º 63, 2008, p. 11.

El control del individuo en todo momento sobre sus datos personales hace que el derecho presente un contenido con una vertiente positiva y otro con sentido negativo. De forma positiva, el derecho confiere un poder de acceso a los datos relativos a uno mismo, independientemente de la ubicación donde se encuentren, así como a su cancelación o actualización. Por su parte, su contenido negativo comporta una facultad de oponerse a cualquier utilización de estos para fines distintos para los que fueron almacenados.

Este doble contenido del derecho a la protección datos constituye otro de los aspectos que muestran su autonomía respecto del derecho a la intimidad, como igualmente lo ha señalado la STC 292/2000, de 30 de noviembre, al declarar que «el derecho a consentir el conocimiento y el tratamiento informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos»¹²⁶.

4.4. Datos de tráfico o asociados y protección de datos de carácter personal

Al ser examinado anteriormente el derecho al secreto de las comunicaciones, en el apartado 3.3.4 se hizo referencia a los datos de tráfico o asociados como un elemento de la comunicación protegido por el secreto de las comunicaciones, que puede tener un gran valor para la investigación penal. Sin embargo, son muchas las voces que se inclinan por considerar una buena parte de los datos de tráfico o asociados como integrantes del contenido del derecho a la protección de datos de carácter personal.

Así, por ejemplo, Marchena Gómez afirma que «es seguro que algunos de esos datos merecen la consideración de datos propios del contenido material del derecho a la inviolabilidad de las comunicaciones. Pero todos, desde luego, no son susceptibles de esa etiqueta». Y es que, efectivamente, el alcance constitucional de los derechos a la intimidad, a la inviolabilidad de las comunicaciones y a la protección de datos no es equivalente, tratándose de derechos «de distinto significado axiológico y, por tanto, sometidos en su restricción a un régimen jurídico no siempre idéntico»¹²⁷.

En el mismo sentido, la jurisprudencia ya destacó en alguna sentencia que algunos de los datos de tráfico deberían ser encuadrados no dentro del derecho al secreto de las comunicaciones (art. 18.3 CE), sino en el marco del derecho a la intimidad personal (art. 18.1 CE) con la salvaguarda que puede dispensar la Ley de Protección de Datos de Carácter Personal¹²⁸.

126 STC 292/2000, de 30 de noviembre, FJ 7.

127 Marchena Gómez, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el art. 18 de la CE. Proceso penal y nuevas tecnologías», en Marchena Gómez, M., González-Cuéllar Serrano, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015, p. 287.

128 *Vid.* STS 247/2010, de 18 de marzo, FJ 2, que declaró: «[...] a nuestro juicio, sin pretensiones ni mucho menos de sentar doctrina (*obiter dicta*), los datos identificativos de un titular o de un

Se trata de una distinción de gran relevancia, dado el distinto alcance constitucional de los derechos del art. 18 CE¹²⁹, debiéndose tener en consideración, primordialmente, que, para la injerencia en el derecho a la protección de datos, al igual que sucede con el derecho a la intimidad, en el art. 18.4 CE no se exige autorización judicial, existiendo un régimen más flexible para la intromisión en la intimidad y protección de datos que cuando se trata del derecho al secreto de las comunicaciones¹³⁰.

En este punto debe señalarse que el legislador —por lo que respecta ya no a todos los datos o ficheros de carácter personal sino a los datos que han de ser conservados por las operadoras— promulgó la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. De acuerdo con su art. 1.1, «esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales»¹³¹.

terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (art. 18.3 CE) sino en el marco del derecho a la intimidad personal (art. 18.1 CE) con la salvaguarda que puede dispensar la Ley de Protección de Datos de Carácter Personal, LO 15/1999 de 13 de diciembre: art. 11.2 d. o su Reglamento, RD 1720/2007 de 21 de diciembre, que entró en vigor el 31 de marzo de 2008, sin desprejar la Ley 32 de 3 de noviembre de 2003, General de Telecomunicaciones y su Reglamento, R.D. 424 de 15 de abril de 2005, en los que parece desprenderse que sin el consentimiento del titular de unos datos reservados, contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo los casos especiales que autorizan sus propias normas, entre las que se halla la autorización judicial, que lógicamente estaría justificada en un proceso de investigación penal».

129 Señala a este respecto la Circular 1/2013 de la FGE que, «desde luego, no todos los datos digitalizados merecen la consideración de datos propios del contenido material del derecho a la inviolabilidad de las comunicaciones. Debe analizarse la funcionalidad de cada dato para ubicarlo bajo el manto protector del derecho a la intimidad (art. 18.1 CE), del derecho a la inviolabilidad de las comunicaciones (art. 18.3 CE) o del derecho a la protección de datos (art. 18.4 CE), cada uno con su propio sustrato axiológico y, correlativamente, cada uno con una protección de intensidad variable». *Vid.* Fiscalía General del Estado, Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, *cit.*, p. 19.

130 Tal y como se señaló al ocuparnos de la delimitación entre el derecho al secreto de las comunicaciones y el derecho a la intimidad, y conforme declaró la STC 70/2002, de 3 de abril, FJ 10, es necesaria la autorización judicial conforme a criterios de proporcionalidad, si bien esa regla se exceptiona en aquellos casos en los que existan razones de intervención policial inmediata, lo cual se hace extensivo a la protección de datos de carácter personal pero no así respecto de las injerencias en el derecho al secreto de las comunicaciones.

131 El art. 5.1 de la Ley 25/2007 fija una obligación de conservación por un plazo de doce meses computados desde la fecha en que se haya producido la comunicación. No obstante, de forma reglamentaria, se podrá ampliar o reducir dicho plazo para conservación de determinados datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste

Llegados a este punto, ante esta doble naturaleza de los datos de tráfico o asociados se plantea el problema de la distinción entre los que se encontrarán protegidos por el derecho al secreto de las comunicaciones o, en su caso, por el derecho a la protección de datos de carácter personal.

El legislador ha tenido en cuenta tal circunstancia con la reforma operada por la LO 13/2015, estableciendo una salvedad que en el proyecto inicial no figuraba¹³². Así, en relación con la incorporación al proceso de los datos de tráfico o asociados, dispone el apartado 1 del art. 588 ter j LECrim que «los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial». Con este precepto se establece una distinción en relación con los datos que requieren autorización judicial para su cesión, dado que será necesaria la autorización judicial para la cesión de datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación, siempre que «se encuentren vinculados a un proceso de comunicación».

Puede afirmarse, por tanto, que quedan establecidas dos modalidades de datos de tráfico: los que se encuentran vinculados a un proceso de comunicación y aquellos que no tienen tal atributo. Los que se encuentren vinculados a un proceso de comunicación estarán protegidos por el derecho al secreto de las comunicaciones y su cesión precisará en todo caso de autorización judicial. Por su parte, respecto de los que no se encuentren vinculados a un proceso de comunicación, no siempre será necesaria la autorización judicial.

Probablemente no serán pocos los problemas que surjan para la distinción entre los datos que se encuentran vinculados o no a un proceso de comunicación, habida cuenta de la amplitud de la relación de datos que se establecen en el art. 3.1 de la Ley 25/2007. Afirma Marchena Gómez que «exigir del juez de instrucción que discierna en el caudal de datos que las operadoras están obligadas a reservar entre aquellos que tienen vinculación a un proceso de comunicación —respecto de los que sería obligada la autorización judicial— y aquellos otros que, por su falta de vinculación con ese proceso estarían exentos de esa exigencia, no es, desde luego un buen criterio»¹³³.

del almacenamiento y conservación de los datos, así como el interés de estos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

132 El proyecto inicial de 20 de marzo de 2015 de reforma de la LECrim, que dio lugar a la LO 13/2015, no establecía la condición mencionada de que se tratase de datos electrónicos «vinculados a un proceso de comunicación», lo cual fue introducido a través de la enmienda n.º 108 (*Boletín de las Cortes Generales-Congreso de los Diputados* de 29 de mayo de 2015) con la justificación de «mejora técnica con la finalidad de mejorar la redacción».

133 Marchena Gómez, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el art. 18 de la CE. Proceso penal y nuevas tecnologías», *cit.*, p. 300.

Existe, no obstante, algún pronunciamiento del TS acerca de los datos que merecen la protección reforzada del derecho al secreto de las comunicaciones. Concretamente ha declarado que, «en principio, ese carácter habría de predicarse, actualizando la pauta interpretativa ofrecida por el TEDH, de los datos identificativos del origen y del destino de la comunicación, del momento y duración de la misma y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada»¹³⁴.

Doctrinalmente se ha afirmado que el criterio de distinción podría venir de la mano de la diferente naturaleza del dato en cuestión: dinámica o estática, de tal forma que podrían entenderse como datos vinculados aquellos de carácter dinámico que son interceptados durante el proceso de comunicación que los está generando y desvinculados de ese proceso los de naturaleza estática almacenados por las operadoras una vez concluido el proceso de comunicación, con obligación de conservación¹³⁵.

Aunque tales criterios pueden resultar orientativos para el juez, no parecen suficientes. Por ello, *de lege ferenda* y en aras de una mayor seguridad jurídica, sería necesaria la sistematización de una forma clara de los datos que de la extensa relación del art. 3 de la Ley 25/2007 quedan vinculados a un proceso de comunicación. El acceso a estos exigiría en todo caso el requisito de la reserva jurisdiccional, y, por tanto, su régimen jurídico quedaría diferenciado del relativo al de los datos que, por no encontrarse vinculados a un proceso de comunicación, tendrían un régimen más flexible, pudiendo en casos de urgencia ser reclamados directamente por el Ministerio Fiscal o la Policía Judicial a las operadoras.

134 *Vid.* STS 249/2008, de 20 de mayo, FJ 4.

135 Lanzarote Martínez, P., «La nueva regulación de las intervenciones telefónicas y telemáticas: Algunas cuestiones claves y otras discutibles», *Revista del Ministerio Fiscal*, n.º 3, 2017, p. 84.

IV. EL ENTORNO VIRTUAL

1. La existencia del llamado entorno virtual

Como consecuencia del desarrollo de la informática y de las TIC en general, y muy especialmente por la creciente amplitud de espacio virtual a disposición de los ciudadanos (bien en pequeños dispositivos y, sin embargo, con una enorme capacidad de almacenamiento, o bien mediante el suministro de espacio virtual por parte de las compañías tecnológicas a los particulares —la llamada nube—), se ha venido planteando en los últimos años la problemática en relación con la información que de cada persona podría extraerse como consecuencia del examen en conjunto de toda la información acumulada en los referidos dispositivos.

Aunque el acceso de forma individual a cada uno de los datos almacenados podría suponer —sin perjuicio de valorar cada caso concreto— una injerencia en un concreto derecho fundamental a la vida privada del art. 18 CE, lo cierto es que toda la información examinada de forma global permitiría en muchos casos extraer conclusiones sobre los hábitos de una persona, sus desplazamientos, relaciones sociales, preferencias sexuales, ideología, religión, etc., facilitando la obtención de un perfil sobre su manera de sentir, pensar o comportarse. Ello dio lugar a que por parte de determinados sectores doctrinales se invocara la existencia del llamado «entorno virtual», como una realidad que se estimaba digna de protección y que ha sido definido como «conjunto de informaciones en formato digital que una persona genera con su actividad mediante dispositivos electrónicos, de manera consciente o inconsciente, con voluntariedad o sin ella»¹³⁶.

Uno de los primeros antecedentes en cuanto al planteamiento de esta realidad puede encontrarse como consecuencia del estudio que se lleva a cabo del derecho a la intimidad frente a las amenazas de la tecnología dentro del desarrollo del art. 18.4 CE. Como consecuencia de este surge, además de una concepción objetiva y subjetiva, una nueva perspectiva del concepto del derecho a la intimidad a la que se denominó «teoría del mosaico», en virtud de la que existen datos que, *a priori*, son irrelevantes desde el punto de vista del derecho a la intimidad, pero que, unidos unos con otros, pueden servir para configurar una idea prácticamente completa de cualquier individuo¹³⁷.

Posteriormente, ya en época más actual y como consecuencia de la posibilidad de obtener pruebas acreditativas de la comisión de cualquier delito mediante las TIC, se

136 Delgado Martín, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015», *Diario La Ley - Sección Doctrina*, n.º 8693, 2016, p. 2.

137 Rebollo Delgado, L., «Derecho al honor, derecho a la intimidad y a la propia imagen. Inviolabilidad del domicilio, secreto de las comunicaciones y límites al uso de las nuevas tecnologías», *cit.*, pp. 181-182. El autor afirma que la teoría del mosaico ha sido formulada por Madrid Conesa, quien señala que la idea completa que se puede configurar de cualquier individuo lo es «al igual que ocurre con las pequeñas piedras que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado». Madrid Conesa, F., *Derecho a la intimidad, informática y Estado de Derecho*, Valencia, 1984, p. 45.

plantea la necesidad de conferir al entorno virtual una adecuada protección a causa de la vulneración que, por el acceso a tal conjunto de información digital, supondría para los derechos fundamentales a la libertad y la intimidad¹³⁸, proponiéndose que la ley se enfrente a los complejos retos que plantea la persecución penal en el entorno virtual adoptándose soluciones a los problemas que se suscitan entre investigación tecnológica y los derechos fundamentales a la privacidad en general¹³⁹.

Esta realidad innegable de la existencia de un entorno virtual, entendida como tal, y no como derecho independiente, como se verá más adelante, también fue reconocida por el TC, al declarar que la observación por los demás del cúmulo de información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional, permitiría descubrir aspectos de la esfera más íntima del ser humano¹⁴⁰.

2. La declaración jurisprudencial del entorno virtual como un derecho independiente

La problemática en relación con las injerencias sobre el entorno virtual se manifiesta de forma notable una vez que, para la investigación del delito, se hace necesario el acceso policial a los dispositivos informáticos de almacenamiento a fin de obtener pruebas en formato digital.

Se plantea entonces la cuestión de cuál, o cuáles, de los derechos del art. 18 CE (intimidad, inviolabilidad de las comunicaciones o protección de datos de carácter personal) podría resultar vulnerado, habida cuenta de que no todos gozan del mismo grado de protección. Esta cuestión se puso de manifiesto una vez que quedó sentado que la orden de entrada y registro no daba cobertura al registro de dispositivos

138 Afirma González-Cuéllar Serrano que «por la misma razón que los datos digitales constituyen un provechoso filón para la indagación y el esclarecimiento de los delitos son un preciado tesoro para la persona: en espacios minúsculos o en segmentos temporales de gran fugacidad se concentra una extraordinaria cantidad de información sobre las más variadas actividades de la vida, muchas de ellas íntimas o de una naturaleza diversa a la privada, pero también secreta o reservada. A la enorme utilidad del entorno digital como ámbito de desarrollo de la persecución penal se une la tremenda lesividad potencial de la aprehensión de datos para la libertad individual, grave problema que colocará en profunda crisis nuestro ya deficiente sistema de garantías constitucionales, dadas las dificultades que se presentan para la aplicación en el ciberespacio de los mecanismos de protección de los derechos fundamentales ejercidos en el mundo físico». *Vid.* González-Cuéllar Serrano, N., «Garantías constitucionales de la persecución penal en el entorno digital», *cit.*, p. 890.

139 González-Cuéllar Serrano, N., «Garantías constitucionales de la persecución penal en el entorno digital», *cit.*, p. 916.

140 *Vid.* STC 173/2011, de 7 de noviembre, FJ 3 *in fine*, la cual declaró que, «quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona».

informáticos, lo que dio lugar a ciertas vacilaciones jurisprudenciales, imponiéndose finalmente el criterio de la necesidad de autorización judicial independiente a la de entrada y registro domiciliario, el cual ha quedado finalmente reflejado en el derecho positivo con la LO 13/2015.

El primer exponente jurisprudencial que se refiere a la existencia de un derecho propio lo constituye la STS 342/2013, de 17 de abril, que, partiendo de la necesidad e importancia de que «la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal», declara que, «más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual»¹⁴¹, doctrina que ha sido reiterada en algunas sentencias posteriores¹⁴².

141 *Vid.* STS 342/2013, de 17 de abril, FJ 8, que declaró lo siguiente: «El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipientario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar —de hecho, normalmente albergará— información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones [...].»

En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal.

La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital».

142 *Vid.* SSTs 97/2015, de 24 de febrero, FJ 4; 786/2015, de 4 de diciembre, FJ 1, y 426/2016 de 19 de mayo, FJ 7.º

3. Problemas en cuanto a la efectiva existencia de un derecho. Reconducción a los derechos a la vida privada del art. 18 CE

Partiendo de la realidad indiscutible de la existencia del entorno virtual al que se ha hecho referencia, que podrá y deberá tener incidencia en todas las ramas del Derecho, no puede afirmarse que este constituya un derecho con *nomen iuris* propio, básicamente, al no constar un reconocimiento expreso por parte del legislador, sin que por otra parte pueda afirmarse la preexistencia de tal derecho, por cuanto la problemática relativa a sus efectos es una cuestión novedosa, al nacer como consecuencia de la irrupción de las TIC.

Recientemente, al referirse el TS a los dispositivos de almacenamiento masivo de información, tras señalar que la necesidad de autorización judicial para el acceso a estos obedece a la circunstancia de la serie compleja y densa de datos que en ellos pueden ser almacenados (que afectan de modo muy variado a la intimidad del investigado —tales como comunicaciones tuteladas por el art. 18.3 CE; contactos, fotografías, archivos personales, tutelados por el art. 18.1 CE; o datos personales y de geolocalización, que pueden cobijarse en el derecho a la protección de datos del art. 18.4 CE— y cuya contemplación disgregada de cada una de esas realidades con regímenes de protección diferenciados resultaría ineficaz), ha declarado que «el legislador con buen criterio ha optado por otorgar un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando ese derecho constitucional de nueva generación, el derecho a la protección del propio entorno virtual», lo cual ha sido reiterado en alguna sentencia posterior¹⁴³.

Del mismo modo, se ha afirmado doctrinalmente que el derecho al entorno virtual se encuentra comprendido dentro del derecho a la privacidad del art. 8 CEDH y que al aceptar la existencia de un derecho fundamental al entorno virtual pierden relevancia los debates dogmáticos acerca de si el registro remoto de un ordenador afecta a cualquiera de los derechos del art. 18 CE, pues englobaría a todos ellos¹⁴⁴. Asimismo, se ha señalado que el tratamiento unitario de los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, responde al reconocimiento de un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual¹⁴⁵.

143 Vid. SSTS 204/2016, de 10 de marzo, FJ 11, y 489/2018, de 23 de octubre, FJ 5.

144 Bachmaier Winter, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», *Boletín del Ministerio de Justicia*, n.º 2195, 2017, pp. 21-22.

145 Conde-Pumpido Tourón, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, p. 21, consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/PonenciaCondePumpidoTouron.pdf?idFile=4d9fe168-e9ee-4cd9-a783-68eab6158e47, el 12 de junio de 2020.

No se comparten las menciones relativas a que el legislador ha configurado un derecho de nueva generación, así como la existencia de un derecho propio y menos aún que pueda otorgarse la naturaleza de derecho constitucional al entorno virtual, dicho sea con el máximo respeto a las resoluciones del TS, dado el importante reconocimiento de la figura que examinamos desde la STS 342/2013 anteriormente mencionada, cuya relevancia es incontrovertible. En tal sentido, tampoco pueden compartirse opiniones doctrinales que afirman que el art. 588 sexies apartados a y b LECrim ha refrendado absolutamente dicho reconocimiento¹⁴⁶.

Con la LO 13/2015 no se ha configurado este pretendido derecho. El legislador se ha limitado a establecer la necesidad de que, por parte del juez competente, se lleve a cabo una ponderación de las razones que justifican el registro de un ordenador, otorgando un tratamiento unitario a esta amplia variedad de datos, ofreciendo, de este modo, una mayor protección a los diferentes derechos fundamentales que pueden ser afectados, que no son otros que los derechos a la vida privada del art. 18 CE.

La necesidad de autorización judicial fijada con la reforma de la LECrim para la ejecución de un registro de dispositivos de almacenamiento masivo, con independencia de la entrada y registro domiciliario, no puede interpretarse en el sentido de que se reconozca la existencia de un nuevo derecho. Tal exigencia se impone por dos cuestiones independientes, como son las siguientes:

1. Porque la posibilidad de intervenir tan variados y desconocidos datos que afectan a la vida privada nunca podrá ser considerada una injerencia leve en el derecho a la intimidad, y, por ello, tratándose siempre de una injerencia grave, será necesaria la autorización judicial, con excepción de los casos de urgencia en los que puedan intervenir directamente las FCSE.
2. El derecho al secreto de las comunicaciones podría verse vulnerado.

Por estas razones, de producirse una intromisión indebida en el entorno virtual en la que se desvelaran preferencias, ideología o, en definitiva, la manera de sentir, pensar o comportarse de un ciudadano, quedaría transgredido en todo caso su derecho a la intimidad, sin perjuicio de que, adicionalmente y dependiendo de cada caso concreto, quedasen vulnerados los derechos al secreto de las comunicaciones o el derecho a la protección de datos de carácter personal.

Cuestión distinta es el criterio interpretativo, a nuestro juicio totalmente aceptable, que se desprende tanto del espíritu de la norma (art. 588 sexies LECrim) como de la línea jurisprudencial iniciada con la STS 342/2013, conforme al que, tal y como mencionó esta sentencia, la ponderación que el juez competente ha de llevar a cabo de las razones que justifican el registro de un ordenador ha de realizarla sin perder de

¹⁴⁶ Vid. Rodríguez Lainz, J. L., «Sobre el concepto de alcance de la medida de injerencia tecnológica en la Ley Orgánica 13/2015», en Díaz Martínez, M., López-Barajas Perea, I. (dirs.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Valencia, Tirant lo Blanch, 2019, p. 38.

vista la multifuncionalidad de los datos, por lo que su tratamiento jurídico sería más adecuado, si todos los datos reveladores del perfil personal se contemplan de forma unitaria.

Es lo que de otra forma ha expresado Delgado Martín, al señalar que una de las consecuencias de la existencia del entorno virtual se concreta en que el legislador de la reforma de 2015 ha otorgado un tratamiento unitario a la injerencia en el espacio virtual del afectado mediante el acceso a los datos contenidos en los dispositivos electrónicos, «lo que contribuye a garantizar una protección eficaz de los diferentes derechos fundamentales que pueden resultar afectados»¹⁴⁷. Es decir, se trata de proteger eficazmente los derechos del art. 18 CE otorgándoles un tratamiento unitario al momento de la decisión judicial.

Por ello, con anterioridad a emitir su resolución, el juez competente deberá, atendiendo a las circunstancias del caso concreto y a criterios de necesidad y proporcionalidad, valorar la incidencia del acceso a todo el cúmulo de datos de la persona investigada, lo cual no hará sino reconducir el pretendido derecho al entorno virtual a los auténticos derechos proclamados en la CE.

Así, de una forma similar a la que autores como Frígols i Brines afirman que los derechos fundamentales del art. 18 CE «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 todos los derechos del art. 18 CE manifestaciones concretas de ese derecho fundamental de libertad, desgajadas del mismo a los meros efectos de una mejor protección de esas parcelas de realidad»¹⁴⁸, podría decir ahora que, para la información almacenada globalmente en un ordenador o cualquier dispositivo de almacenamiento, los derechos a la intimidad, secreto de las comunicaciones y protección de datos de carácter personal se agrupan a fin de dar una adecuada protección al entorno virtual que constituye toda la información almacenada.

El entorno virtual debe protegerse porque en él coexisten los derechos fundamentales a la vida privada. Pero ello no significa que pueda elevarse a la categoría de derecho tal realidad, aun siendo cierto que todos los datos que se puedan localizar dentro de los dispositivos informáticos conjuntamente considerados podrían describir el perfil ideológico de cualquier persona. Finalmente, derivaría en una vulneración de la intimidad personal.

En definitiva, con el juicio de proporcionalidad del juez en relación con el entorno virtual, se está protegiendo finalmente el derecho a la intimidad personal, que es el que resultaría infringido de conocerse de forma indebida las preferencias, ideología o,

147 Delgado Martín, J., «Investigación tecnológica y prueba digital en todas las jurisdicciones», *cit.*, p. 365.

148 Frígols i 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», *cit.*, p. 43.

en definitiva, las formas de sentir, pensar o comportarse de cualquier persona, sin perjuicio de la vulneración del secreto a las comunicaciones y protección de datos, por lo que, tal y como se decía, se produce una reconducción a los derechos del art. 18 CE.

4. Proposición de una adecuada regulación

El hecho de que en el apartado anterior se haya puesto de manifiesto nuestra disconformidad con el reconocimiento del entorno virtual como un derecho constitucional no obsta para considerar necesaria una adecuada regulación con la que quede cubierta la tutela del entorno digital frente a injerencias estatales.

Esta regulación no puede entenderse realizada con la reforma operada por la LO 13/2015, dado que, además de no haber sido planteado de dicho modo por el legislador, no se ha procedido a una definición y concreción de los aspectos esenciales del entorno virtual, no habiéndose efectuado mención alguna en cuanto a las facetas de la vida privada que pueden quedar vulneradas, sin que tampoco se hayan concretado los supuestos de urgencia en los que la Policía Judicial podría intervenir sin autorización judicial y sin que, asimismo, conste una específica regulación en cuanto a las medidas de seguridad que adoptar en relación con los dispositivos intervenidos.

Llegados a este punto, nos parece sumamente acertada la propuesta de González-Cuéllar Serrano cuando sitúa el problema en toda su complejidad en el ámbito del art. 18.4 CE, reclamando el desarrollo legal del derecho constitucional que dicho precepto contiene, «no solo frente a la recopilación, tratamiento automatizado y utilización de datos personales, sino también ante el aprovechamiento por los órganos de persecución penal de los sistemas de almacenamiento y comunicación de datos digitales para la investigación y prueba de los delitos»¹⁴⁹.

Efectivamente, el art. 18.4 CE ordena al legislador que mediante ley «limite el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se trata, al igual que en su día se hizo con la protección de datos de carácter personal, de cumplir tal mandato conforme a la realidad de la era digital, entendiendo que la expresión «limitará el uso de la informática» ha de entenderse como una expresión de una gran amplitud, dirigida al uso de la informática que hagamos todos, incluido, por supuesto, el Estado en el ámbito de la investigación del delito.

149 González-Cuéllar Serrano, N., «Garantías constitucionales de la persecución penal en el entorno digital», *cit.*, pp. 890-891. Señala este autor al final de esta obra (p. 916) que «la ley, consecuentemente, por mandato constitucional específico, debe enfrentarse a los complejos retos que plantea la persecución penal en el entorno digital [...] y adoptar soluciones para los problemas que la revolución tecnológica suscita respetuosas con los derechos fundamentales a la privacidad, la inviolabilidad del domicilio y el derecho de las comunicaciones, que eviten la improvisación y la arbitrariedad a las que en demasiadas ocasiones conducen las lagunas y contradicciones de nuestro anquilosado y decrépito Derecho Procesal Penal».

BIBLIOGRAFÍA

- ALEXY, R., «Los derechos fundamentales y el principio de proporcionalidad», *Revista Española de Derecho Constitucional*, n.º 91, 2011, pp. 11-29.
- ÁLVAREZ CONDE, E., «El sistema constitucional español de derechos fundamentales», *Corts: Anuario de derecho parlamentario*, n.º 15, 2004, pp. 115-146.
- BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», *Boletín del Ministerio de Justicia*, n.º 2195, 2017.
- BARNES, J., «El principio de proporcionalidad. Estudio preliminar», *Cuadernos de Derecho Público*, vol. 5, 1998, pp. 15-49.
- BAYO DELGADO, J., «La protección de datos en la investigación policial y en el proceso penal», *Jueces para la Democracia. Información y Debate*, n.º 63, 2008, pp. 11-25.
- CASTILLO RIGABERT, F., «Derechos fundamentales e investigación en las diligencias previas (Estudio de la reciente jurisprudencia de la Sala II del TS)», *Anales de Derecho (Universidad de Murcia)*, n.º 13, 1995, pp. 13-37.
- CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», *Ponencias de formación continuada - Ministerio Fiscal*, 2016. Consultado en <https://www.fiscal.es/documentación>.
- DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015», *Diario La Ley - Sección Doctrina*, n.º 8693, 2016.
- Investigación tecnológica y prueba digital en todas las jurisdicciones*, Las Rozas (Madrid), Wolters Kluwer, 2016.
- DÍEZ-PICAZO GIMÉNEZ, L. M., *Sistema de Derechos Fundamentales*, Cizur Menor (Navarra), Editorial Aranzadi, 2013.
- Fiscalía General del Estado, Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, 2013.
- Circular 4/2013, de 30 de diciembre, sobre las Diligencias de Investigación, 2013.
- Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal, 2019.
- Circular 5/2019, sobre registro de dispositivos y equipos informáticos, 2019.
- FRÍGOLS i 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, Javier (dir.), Jareño Leal, A. (coord.), *La protección jurídica de la intimidad*, Madrid, Iustel, 2010, pp. 37-91.
- GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la

información y la comunicación», en Galán Muñoz, A. (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, Tirant lo Blanch, 2014, pp. 203-279.

GARCÍA-ATANCE y GARCÍA de MORA, M. V., «La Constitución Dogmática (I). Estado de Derecho y naturaleza de los derechos.», en García-Atance y García de Mora, M. V., Gutiérrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado, C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, pp. 25-54.

GIMENO SENDRA, J. V., *Manual de Derecho Procesal Penal*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015.

—«Medidas limitadoras de derechos fundamentales en el proceso penal», en Pérez-Cruz Martín, A. J., Ferreiro Baamonde, X. (dirs.) Neira Pena, A. (coord.), *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional)*, A Coruña, 2 y 3 de junio de 2011, A Coruña, Universidade da Coruña, 2012, pp. 73-90.

GONZÁLEZ-CUÉLLAR SERRANO, N., «El principio de proporcionalidad en el Derecho procesal español», *Cuadernos de Derecho Público*, n.º 5, 1998, pp. 191-215.

«Garantías constitucionales de la persecución penal en el entorno digital», en Díaz Maroto y Villarejo, J. y otros), *Derecho y Justicia Penal en el Siglo XXI*, Madrid, Colex, 2006, pp. 887-916.

HOFFMANN-RIEM, W., «Innovaciones en la jurisprudencia del Tribunal Constitucional alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la sociedad de la información», *Revista de Derecho Constitucional Europeo*, vol. 11, n.º 22, 2014, pp. 123-146.

KLUTH, W., «Prohibición de exceso y principio de proporcionalidad en Derecho alemán», *Cuadernos de Derecho Público*, n.º 5, 1998, pp. 219-237.

LANZAROTE MARTÍNEZ, P., «La nueva regulación de las intervenciones telefónicas y telemáticas: Algunas cuestiones claves y otras discutibles», *Revista del Ministerio Fiscal*, n.º 3, 2017, pp. 58-85.

LUCENA CID, I. V., «El concepto de la intimidad en los nuevos contextos tecnológicos», en Galán Muñoz, A. (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, Tirant lo Blanch, 2014, pp. 15-53.

MADRID CONESA, F., *Derecho a la intimidad, informática y Estado de Derecho*, Valencia, 1984.

MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el art. 18 de la CE. Proceso penal y nuevas tecnologías», en Marchena Gómez, M., González-Cuellar Serrano, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015, pp. 171-403.

MEGIÁS QUIRÓS, J. J., «Privacidad e internet: intimidad, comunicaciones y datos personales», *Anuario de Derechos Humanos - Nueva Época*, n.º 3, 2002, pp. 515-560.

- MORENO CATENA, V. CORTÉS DOMÍNGUEZ, V., *Derecho Procesal Penal*, Valencia, Tirant lo Blanch, 2019.
- PERELLÓ DOMENECH, I., «El principio de proporcionalidad y la jurisprudencia constitucional», *Jueces para la Democracia. Información y Debate*, n.º 28, 1997, pp. 69-75.
- PÉREZ GIL, J.; GONZÁLEZ LÓPEZ, J. J., «Cesión de datos personales para la investigación penal. Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal», *Diario La Ley - Sección Doctrina*, n.º 7401, 2010.
- REBOLLO DELGADO, L., «Derecho al honor, derecho a la intimidad y a la propia imagen. Inviolabilidad del domicilio, secreto de las comunicaciones y límites al uso de las nuevas tecnologías», en García-Atance y García de Mora, M. V., Gutiérrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado, C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, pp. 177-203.
- El derecho fundamental a la intimidad*, Madrid, Dykinson, 2000.
- RODRÍGUEZ LAINZ, J. L., «El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre», *Diario La Ley - Sección Doctrina*, n.º 8122, 2013.
- «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», *Diario La Ley*, n.º 8143, 2013, pp. 1-14.
- «Sobre el concepto de alcance de la medida de injerencia tecnológica en la Ley Orgánica 13/2015», en Díaz Martínez, M., López-Barajas Perea, I. (dirs.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Valencia, Tirant lo Blanch, 2019, pp. 17-48.
- RUIZ RUIZ, R., De la TORRE MARTÍNEZ, L., «Algunas aplicaciones e implicaciones del principio de proporcionalidad», *Revista Telemática de Filosofía del Derecho*, n.º 14, 2011, pp. 27-44.
- SUBIJANA ZUNZUNEGUI, I. J., «Policía judicial y derecho a la intimidad en el seno de la investigación criminal», *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, n.º 10, 1997, pp. 121-160.
- VELASCO NÚÑEZ, E., «Correo electrónico, SMS y virus troyanos: aspectos procesales penales», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 22, 2009.