EL LEGISLADOR AUSENTE DEL ARTÍCULO 18.3 DE LA CONSTITUCIÓN

(la construcción pretoriana del derecho al secreto de las comunicaciones)

M.ª JOSEFA RIDAURA MARTÍNEZ

SUMARIO

Fecha recepción: 28.06.2017
Fecha aceptación: 10.10.2017

EL LEGISLADOR AUSENTE DEL ARTÍCULO 18.3 DE LA CONSTITUCIÓN

(La construcción pretoriana del derecho al secreto de las comunicaciones)

M.ª JOSEFA RIDAURA MARTINEZ*

Universitat de Valencia

I. INTRODUCCIÓN

Este trabajo aborda los problemas jurídicos que se han venido planteado por la persistente inactividad del legislador a la hora de desarrollar el contenido del derecho fundamental al secreto de las comunicaciones. En efecto, la entrada en vigor de la Constitución coincidió con una ley del siglo XIX claramente obsoleta en este ámbito, y que, además, solo regulaba, y deficientemente, la vertiente procesal de este derecho fundamental.

La relevancia del tema, tanto por su contenido esencial, como por su honda repercusión procesal, ha confirmado que la aprobación de una ley de desarrollo acorde con el texto constitucional era una clara exigencia. Su ausencia, seguramente, se haya visto influenciada por una nueva realidad que ha debido asumir importantes complejidades: la de la revolución digital, la de la lucha antiterrorista interna y trasnacional, la de lucha contra toda clase de crimina-

* Profesora Titular de Derecho Constitucional. Departamento de Derecho Constitucional y Ciencia Política y de la Administración (Facultad de Derecho-Universidad de Valencia). Avda. dels Tarongers, s/n, 46022 Valencia (España). Email: sefa.ridaura@uv.es.

lidad, o la propia dificultad en la determinación del alcance del contenido esencial del derecho.

Esta pasividad del legislador ha abocado a la construcción pretoriana, tanto de la dimensión sustantiva del derecho, como de su desarrollo procesal. En efecto, el hecho de que las comunicaciones se intervinieran de acuerdo con las disposiciones de una ley centenaria, que no respetaba las garantías mínimas para la limitación de un derecho fundamental, ha propiciado que, durante estas últimas décadas, el Tribunal Europeo de Derechos Humanos condenara a España por la falta de calidad de la ley; colmando con su doctrina las carencias legislativas; pero, también el Tribunal Constitucional y el Tribunal Supremo, en ocasiones influenciados por el TEDH, en otras, fijando su propia doctrina, a través de la casuística han ido construyendo este derecho a golpe de sentencias.

Así pues, la realidad es que nos encontramos ante un derecho que se ha construido con la presencia del juez y la ausencia de legislador.

La empeñada y loable determinación casuística de las exigencias de la interceptación de las comunicaciones acordes con el texto constitucional, así como de las múltiples aristas que presenta el contenido de este derecho fundamental, contrasta con la ausencia de una ley que cumpla las garantías de certeza, seguridad, abstracción y generalidad que este instrumento normativo ofrece como una garantía esencial de nuestro Estado de Derecho. Su realización se corresponde, así, con el mandato constitucional dirigido a los poderes públicos en orden a asegurar el respeto del derecho fundamental.

Ciertamente, el derecho al secreto de las comunicaciones plantea múltiples cuestiones que trascienden el objeto de este trabajo. Nosotros nos hemos centrado en poner de relieve los déficits que han abocado a una construcción pretoriana del derecho, remarcando la necesidad de su desarrollo legislativo que, finalmente, se ha abordado con la reciente reforma de la Ley de Enjuiciamiento Criminal, pero solo en su dimensión procesal; falta el desarrollo cabal de su dimensión sustantiva.

II. ENCUADRE CONSTITUCIONAL

1. La entrada en vigor de la Constitución española en el año 1978 coincide en el tiempo con una Ley de Enjuiciamiento Criminal del año 1882 que, en su momento, pudo suponer un gran avance en el marco de la materia que regulaba (el proceso penal), sobreviviendo algunos siglos mediante reformas importantes. Sin embargo, en lo que atañe a nuestro objeto de estudio, centrado en el secreto de las comunicaciones, contenía una regulación parca, desfasada y sin

© UNED. *Revista de Derecho Político*
N.º 100, septiembre-diciembre 2017, págs. 347-404

las debidas garantías procesales. Por tanto, la Constitución converge con una LeCrim centenaria y con alguna otra normativa también vetusta que muy precariamente contenían disposiciones sustantivas y procesales sobre el secreto de las comunicaciones.

En la Constitución el secreto de las comunicaciones aparece regulado como un derecho fundamental, cuya ubicación en el Título I, Capítulo II, Sección Primera le dispensa las máximas garantías contempladas en el artículo 53.1 Ce (reserva de ley, vinculación a todos los poderes públicos y respeto al contenido esencial), así como las jurisdiccionales previstas en el apartado segundo de este mismo precepto, esto es, su protección mediante las garantía preferente y sumaria, y la del recurso de amparo constitucional. Y, aunque el artículo 18.3 era bastante parco, la adecuación del nuevo escenario propiciado por el texto constitucional exigía la acomodación del ordenamiento a sus postulados; en mayor media tratándose de un derecho fundamental. Llama, pues, la atención que la entrada en vigor de la Constitución hubiera propiciado reformas de la LECrim de gran calado, por ejemplo, entre otras, la Ley reguladora del Habeas Corpus (1984); sin embargo no fructificara una actualización de las disposiciones relativas a la intervención de las comunicaciones acorde con las exigencias constitucionales; a lo sumo, como se verá a continuación, una parca reforma en el año 1988, que nos valió diversas —y merecidas— condenas del Tribunal Europeo de Derechos Humanos.

No se abordó, pues, cabalmente el mandato constitucional de desarrollar el derecho fundamental, ni en su dimensión sustantiva ni en la procesal. En este trabajo pretendemos poner de manifiesto que la actuación del legislador era completamente inexcusable en las dos vertientes apuntadas.

Ciertamente, nos plantea serios interrogantes la ausencia tan prolongada del legislador en el desarrollo de un derecho fundamental con implicaciones tan importantes como este, ya que en él convergen diversos intereses protegidos, pues no preserva solo la privacidad, sino también derechos procesales esenciales como la defensa o la presunción de inocencia. Ello le sitúa en una posición de notable relevancia; razón por la que merecía un esfuerzo en orden a su cabal desarrollo. Sin embargo, varios intentos de reforma de la LECrim[1], ante gobiernos de distinto signo, y con diversas mayorías absolutas, hacen difícilmente

[1] *Vid.* Con mayor detalle el estudio de Gimeno Beviá, J.: «La agilización de la justicia penal y el refuerzo de las garantías procesales en las últimas reformas de la LECrim», *Gabilex,* núm. 2/2015, p. 106, en el que explica los intentos durante el primer Gobierno socialista (2004-2008) se creó una comisión de reforma de LECrim que no llegó a presentar oficialmente ninguna propuesta. En la segunda legislatura socialista (2008-2011), sin embargo, sí que se aprobó un texto que llegó a convertirse en Anteproyecto pero que, al ser presentado justo antes de las elecciones

explicable que se haya tenido que esperar cerca de 40 años de vigencia constitucional[2] para abordar la reforma procesal del secreto de las comunicaciones. Mientras, su dimensión sustantiva sigue sin abordarse.

Máxime cuando el incumplimiento del legislador ha abocado al fracaso de numerosas actuaciones de los responsables públicos que, sin cobertura legal suficiente, han tenido que ir sorteando numerosos obstáculos para la obtención de pruebas en la investigación penal. Sólo el empeño y la pericia profesional ha permitido sortearlas. Su consideración como un fracaso, pues, del sistema de justicia penal se ha resaltado en la reciente Sentencia de la Sala Segunda del Tribunal Supremo 106/2017, de 21 de febrero, como tendremos ocasión de destacar en estas páginas.

2. El haz normativo con el que se encuentra la Constitución cuando entra en vigor —a todas luces insuficiente— podía haberse entendido derogado como consecuencia de la eficacia derogatoria de la misma; de forma que la jurisdicción ordinaria podía, perfectamente, haber entendido derogado el artículo 579 de la LECrim, en atención a su competencia para determinar la vigencia de las normas.

En su defecto, se podía haber acudido a la técnica de la inconstitucionalidad sobrevenida, a la que recurrió el Tribunal Constitucional para asegura una pronta depuración de las leyes preconstitucionales contrarias a la Constitución. Sobre todo, porque el TC había declarado en varias resoluciones que el sistema de valores que consagra la Constitución informa todo el ordenamiento jurídico, «lo que se traduce en la necesidad de valorar las normas anteriores a aquélla desde la propia Norma Fundamental, con la consecuencia de que la posible inconstitucionalidad sobrevenida de las normas incompatibles con ella produce efectos de significación retroactiva mucho más intensos que los derivados de la mera derogación, especialmente en materia de derechos fundamentales y libertades públicas» (STC 125/1983, de 26 de diciembre).

Sin embargo, el Alto Órgano no aborda el enjuiciamiento de la Ley hasta que resuelve una cuestión de inconstitucionalidad en STC184/2003, de 23 de octubre. Su insuficiencia había sido ya evidenciada por el Tribunal Supremo y por el Tribunal Europeo de Derechos Humanos; sin embargo el TC concluye, como veremos más adelante, que las deficiencias que esta ley planteaba no podían ser

generales, finalmente no llegó a prosperar. Y, finalmente, el actual Proyecto bajo el mandato del Gobierno popular.

[2] «Sorprende, pues, que siendo tan íntima la relación entre Constitución y procedimiento penal, la democracia española no haya conseguido aprobar una ley de enjuiciamiento criminal elaborada a partir de la cultura jurídica de la libertad. Esto es, desde los fundamentos de la Constitución» Caamaño, F.: «Prólogo del Ministro de Justicia», en *Anteproyecto de ley para un nuevo proceso penal*, Ministerio de Justicia, Madrid, 2011.

objeto de control a través de una cuestión de inconstitucionalidad, ya que su inconstitucionalidad se planteaba por omisiones legislativas, esto es, la llamada inconstitucionalidad por omisión. En consecuencia, el Tribunal Constitucional optó por suplir las deficiencias de la regulación legal[3].

3. El derecho fundamental al secreto de las comunicaciones, en virtud del artículo 53.1, goza de la garantía de la reserva de ley, que, además, ha de ser orgánica (art. 81.1). De dicha exigencia constitucional cabía esperar una ley de este rango que regulara el contenido del derecho al secreto de las comunicaciones; al menos en su contenido esencial (titularidad, objeto, contenido y límites).

Por el contrario, la Ley Orgánica reguladora del contenido de este derecho, como hemos dicho, sigue sin aprobarse. Mientras que la intervención de las comunicaciones se regulaba, en un principio, en la LECrim que tenía carácter ordinario. Y, aunque esta ley ha sufrido constantes modificaciones, la incerteza o indeterminación de los contenidos que debían regularse mediante ley orgánica, a diferencia de los que tenían reserva ordinaria, ha espoleado la acción del legislador en este marco; pues el artículo 579 de la LeCrim, que debe gozar de rango de orgánico, por afectar directamente a uno de los contenidos esenciales del derecho fundamental al secreto de las comunicaciones, ha estado incardinado en el marco de una ley que es ordinaria. Los problemas de articulación material, así como los derivados de la exigencia de la mayoría absoluta requerida para la aprobación, modificación y derogación en una votación final sobre el conjunto del proyecto, desaconsejan la artificiosa técnica de regular conjuntamente contenidos orgánicos con contenidos ordinarios.

Haciéndose eco de dichas dificultades, la reciente reforma de la LECrim ha optado por plantear dos modificaciones independientes: la articulada a través de la Ley 13/2015, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que, al desarrollar derechos fundamentales tiene rango orgánico; y la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales, que al ser de naturaleza estrictamente procesal, lo tiene de ordinaria.

[3] Aragón Reyes, M.: «Intervenciones Telefónicas y Postales (examen de la Jurisprudencia Constitucional)», *Teoría y Realidad Constitucional*, núm. 25/2010, p. 476. A juicio del autor, esta actuación del Tribunal como legislador positivo para remediar la omisión (más exactamente la insuficiencia) de la regulación legal resultaba obligada, puesto que era la única forma de proteger el derecho fundamental, lo que no se hubiera logrado con la simple declaración de la inconstitucionalidad por omisión».

4. El derecho fundamental al secreto de las comunicaciones se ha visto afectado, tanto directa como indirectamente, por una importante dispersión normativa.

En el marco del ordenamiento interno, sin ánimo exhaustivo, cabe destacar, por ejemplo, la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que regula las exigencias en la intervención de las comunicaciones de los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público. Y la intervención de las comunicaciones en concretos ámbitos como Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria; Ley Orgánica 8/2003, de 9 de julio, para la Reforma Concursal[4]; LO 2/1989 reguladora del Código Procesal Militar; o la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. Por su parte, la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, regula las obligaciones de registro documental e información que deben seguir, entre otros, los servicios telefónicos o telemáticos de uso público mediante establecimientos abiertos al público (locutorios).

En el ámbito civil, destaca la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (art.7,1 y.2) que entiende como intromisión ilegítima el emplazamiento de aparatos de escucha o de cualquier otro medio para grabar o conocer cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.

En el marco del Consejo de Europa, el artículo 8 del Convenio Europeo de Derechos Humanos, que garantiza el secreto de las comunicaciones, ha servido, como veremos a continuación, para construir el andamiaje de las garantías que han de presidir su intervención.

Y, en el de la Unión Europea, además de la garantía de las comunicaciones prevista en la Carta Europea de Derechos Fundamentales, diversas disposiciones han incidido directamente sobre este derecho; sobre todo las que han visto la luz a raíz del recrudecimiento del terrorismo yijadista. Se trata de medidas que refuerzan la vigilancia de las comunicaciones en la lucha contra un terrorismo trasnacional que opera, en gran medida, valiéndose de las redes sociales[5]; y que

[4] Por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, contempla en su artículo 1. 1.ª la intervención de las comunicaciones del deudor, con garantía del secreto de los contenidos que sean ajenos al interés del concurso.

[5] Un tratamiento más minucioso de todas estas medidas puede verse en Serra Cristóbal, R.: «Análisis de los riesgos y amenazas para la seguridad, la vigilancia de datos y de comunicaciones digitales en la lucha por la seguridad nacional. Especial referencia a las previsiones legislativas en España», en *Análisis de los riesgos y amenazas para la seguridad*, Flores Giménez, F.

han motivado, en ocasiones, el rechazo del Tribunal de Justicia de la Unión Europea, siendo de capital importancia la Sentencia *Digital Rights Ireland y Seitlinger*, en la que como veremos más tarde, el Tribunal declara la invalidez de la Directiva 2006/24/Ce del Parlamento y del Consejo, de 15 de marzo de 2016, relativa a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.

Asimismo, en atención a dicho carácter trasnacional del terrorismo, la adopción de medidas trasciende el marco de la Unión Europea, de modo que el intercambio de datos con terceros países puede afectar directamente a la intervención de toda clase de comunicaciones; destacando así la renovación del Acuerdo entre la UE y Estados Unidos[6] conocido como «*Safe Harbour*» por el «*EU-US Privacy Shield*» de febrero de 2016, como consecuencia de la Sentencia del Tribunal de Justicia de la Unión Europea en el caso *Schrems*, a la que nos referiremos con posterioridad.

5. La realidad ha evidenciado que el derecho al secreto de las comunicaciones trasciende su eficacia horizontal, superándose, así, su configuración como un derecho público subjetivo[7]. La clásica concepción de los orígenes del constitucionalismo, que concebía los derechos como límites a la actuación de los poderes públicos, ha dado paso, hoy en día, a la consideración de los derechos fundamentales como límite a todo poder, tanto público como privado[8].

En este marco, la evolución de los canales de comunicación ha venido acompañada, también, de los sujetos que pueden intervenir dichas comunicaciones,

---

y Ramón Chornet. C. (coords.), Tirant lo Blanch, Valencia, 2017, pp. 110 y ss., en el que resalta, fundamentalmente, la Directiva 2016/680, de 27 de abril, sobre el tratamiento de datos por las autoridades en el ámbito de la prevención y persecución del crimen, que abre un nuevo escenario más reforzado en el ámbito del intercambio de datos entre Estados.

[6] En cuyo marco cabe destacar la Ley FISA (*Foreigh Intelligence Surveillance Act*), que permite a las autoridades participar en la vigilancia interna sobre los ciudadanos; autorizando expresamente a las agencias de inteligencia para controlar las llamadas telefónicas, el correo electrónico y todo tipo de comunicaciones sin orden judicial, al menos hasta una semana. Ley aprobada bajo la presidencia de Carter en 1978, que se ha mantenido incluso durante la presidencia de Obama, y que se ha renovado recientemente hasta 2017. *Vid.* también Serra Cristóbal, R.: «The impact of counter-terrorism security measures on fundamental eights», *Democrazia e Sicurezza - Democracy* & *Security Review,* núm. 2/2015, pp. 17-61.

[7] Tesis que compartimos con Rebollo Delgado quien se muestra crítico con la configuración de este derecho, únicamente, como un derecho público subjetivo, ya que «los modernos ingenios tecnológicos y significativamente los referidos alas comunicaciones» pueden provocar la vulneración de este derecho por los particulares. Rebollo Delgado. L.: «El secreto de las comunicaciones: problemas actuales», *Revista de Derecho Político*, núms. 48-49/2000, pp. 366 y ss.

[8] *Vid.* sobre dicha concepción Bilbao Ubillos, J. M.: *La eficacia de los derechos frente a particulares*, Centro de Estudios Políticos y Constitucionales, Madrid, 1997.

de modo que ya es no solo es un poder público, con la correspondiente autorización judicial, quien puede interferir en el proceso de la comunicación; pues son muchos los operadores privados que pueden hacerlo, ante los que el ciudadano está inerme[9]. Dicha dimensión se ha reconocido, también, por la doctrina constitucional, cuando afirma que sea cual sea el ámbito objetivo del concepto de comunicación, «la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros» ajenos a la comunicación misma, ya sean públicos o privados, pues el derecho posee eficacia *erga omnes*[10].

6. Las nuevas tecnologías han actuado profusamente sobre las comunicaciones creando nuevos espacios de comunicación, nuevos canales de comunicación, y, en consecuencia, nuevos retos en orden a su protección. Han propiciado también la irrupción de nuevos métodos de delinquir, y, por consiguiente, la exigencia de acomodar las herramientas de intervención pública al nuevo escenario, evidenciando la insuficiencia de una legislación que, ni por asomo, podía presumir lo que era un IP[11], un WhatsApp, un IMEI, Skype, o Face Time.

Ciertamente, la complejidad de los métodos de investigación puede desembocar en excesos que escapan del control judicial y que implican una clara afectación, cuanto menos, de la vida privada. Por tanto, la irrupción de las nuevas tecnologías ha de venir acompañada, ineludiblemente, de operadores públicos que manejen el nuevo lenguaje, los nuevos modos de operar en la investigación, y que permitan mantener el equilibrio entre nueva investigación tecnológica, derechos fundamentales y garantías procesales.

III. LA CONSTRUCCIÓN JURISPRUDENCIAL DE LA DIMENSIÓN SUBSTANTIVA DEL DERECHO AL SECRETO DE LAS COMUNICACIONES

El artículo 18.3 CE protege el secreto de las comunicaciones en general, y la inviolabilidad de la correspondencia en particular; salvo autorización del interesado. El precepto es conciso; pero se atisba de su lectura el contenido sustantivo del derecho y su intervención. En este apartado nos centraremos en señalar los aspectos sustantivos más relevantes del derecho que han ido perfilándose a golpe

[9] Sirva de ejemplo la *Operación Captor* en A Estrada (Pontevedra) que ha permitido la detención de los integrantes de un grupo organizado para hackear las cuentas de correo electrónico corporativo de sus profesores y conseguir los exámenes para luego distribuirlos.

[10] Sentencia 56/2003, de 24 de marzo.

[11] Martínez Martínez, R.: «En torno a la consideración jurídica del número IP», *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, núm. 1/2005, pp. 283-304.

de sentencia, ya que no encontramos ninguna ley —orgánica— que los desarrolle. Contenido sustantivo que es ineludible para la configuración de este derecho fundamental, que comprende su configuración, alcance, titulares y las clases de comunicaciones protegidas.

1. Configuración del derecho al secreto de las comunicaciones

Está pacíficamente admitido[12] que el secreto de las comunicaciones está configurado como una garantía formal que cubre no solo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores. Así se ha venido reconociendo por el Tribunal Europeo de Derechos Humanos que, desde bien temprano, la concibió como una garantía formal y no material (caso Malone/1984); asumiendo dicha tesis el Tribunal Constitucional desde la Sentencia 114/1984. Esta posición se ha consolidado en la doctrina constitucional, reafirmándose dicho carácter formal y abstracto, y en consecuencia, predicándose el secreto de lo comunicado, sea cual sea su contenido y pertenezca o no la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado[13].

En consecuencia, esta naturaleza jurídica formal implica que la comunicación se protege frente a terceros, ajenos a la misma, pertenezca o no el objeto de la misma al ámbito de lo personal, lo íntimo o lo reservado, sea banal o no, sea relevante o no. De ahí que no pueda identificarse el secreto con el contenido privado de la comunicación. No son, pues, las comunicaciones privadas las que determinan el núcleo de la garantía, sino la privacidad de la comunicación, independientemente del contenido que tenga. De ello deriva la presunción *iuris et* de *iure* de que lo comunicado es «secreto», en un sentido sustancial.

El bien constitucionalmente protegido por el artículo 18.3 es, así, la libertad de las comunicaciones, dirigiéndose a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia *erga omnes)* ajenos a la comunicación misma» (STC 114/1984, de 29 de noviembre).

---

[12] «El bien constitucionalmente protegido es el derecho de los titulares a mantener el carácter reservado de una información privada o, lo que es lo mismo, a que ningún tercero pueda intervenir en el proceso de comunicación y conocer de la idea, pensamiento o noticia transmitida por el medio» Gimeno Sendra, V: «La intervención de las comunicaciones telefónicas y electrónicas», *El Notario*, núm. 39/2001, p. 6.

[13] Por todas STC 34/1996, de 11 de marzo.

1.1 El secreto de la comunicación como derecho autónomo de la intimidad

El secreto de las comunicaciones está enclavado en el 18 CE junto con otros derechos, encabezados en su apartado primero por los derechos al honor, a la intimidad y a la propia imagen, la inviolabilidad del domicilio (18.2) y, finalmente, la protección frente al uso de la informática (18.4), lo que permite plantearnos qué consecuencias pueden extraerse de esta ordenación conjunta de estos derechos, con el objeto de determinar el bien jurídico protegido por el secreto de las comunicaciones y las implicaciones que de ello derivan.

La primera cuestión que se plantea en este orden es determinar si nos encontramos ante un derecho instrumental del derecho a la intimidad, o, por el contrario, si estamos ante un derecho autónomo; y si lo es ¿por qué no cuenta con una ley de desarrollo?.

La consideración de este derecho como un derecho instrumental del derecho a la intimidad ha sido defendida por un sector doctrinal, que ha concebido el secreto de las comunicaciones como garantía del derecho a la vida privada y, en especial, de la intimidad personal, por constituir éste su núcleo esencial[14]. En esta dirección el T. S declaraba que el secreto de las comunicaciones «no es sino una manifestación, y muy cualificada, del derecho a la intimidad personal y familiar»[15].

Más generalizada es la posición que mantiene su carácter autónomo, aún reconociendo la existencia de un tronco común entre ellos. En este sentido, afirma Blanca Rodríguez Ruiz que es un aspecto de la intimidad que tiene fronteras conceptuales propias y puede ser reconocido como un derecho autónomo, aunque siempre tendrá como telón de fondo la intimidad [16]. En esta misma línea Lucas Murillo[17] mantiene la distinta naturaleza, pues mientras el secreto de las comu-

[14] Montañes Pardo, M. A.: *La Intervención de las Comunicaciones (doctrina jurisprudencial),* Aranzadi, 1999, p. 22.

[15] STS de 20.12.1996. Incluso la Exposición de Motivos del Ley Orgánica 7/1984, de 15 de octubre, afirmaba en relación con el artículo 192 bis que «al objeto de dar la máxima protección a los derechos constitucionales al honor y a la intimidad personal (art. 18.1 C. E.), para cuya efectividad el secreto de las comunicaciones es un instrumento constitucionalmente previsto (art. 18.3 CE).

[16] Rodríguez Ruiz, B.: *El secreto de las comunicaciones: tecnología e intimidad*, Ed. McGraw Hill, Madrid, 1998, p. 23.

[17] Lucas Murrillo de la Cueva, P.: «Notas sobre el derecho fundamental al secreto de las comunicaciones», en *Constitución, Estado de las Autonomías y Justicia Constitucional*: (libro homenaje al profesor Gumersindo Trujillo) / coord. por Luis Aguiar De Luque, 2005, p. 669. Mantiene que aunque no sean intimidad y secreto «magnitudes necesariamente conexas», no significa que se sitúen en ámbitos distintos; solo quiere decir que los instrumentos jurídicos correspondientes

nicaciones es predominantemente formal, la intimidad es un concepto material, pero remarca la conexión del secreto de las comunicaciones con la vida privada.

La dimensión formal del derecho conduce a la necesaria conexión entre ambos, por tener un tronco común, pero destacando su carácter autónomo[18], al protegerse las comunicaciones, con independencia de su carácter íntimo o privado[19]. Y, aunque tomando en consideración la ubicación del precepto, puede desprenderse que el constituyente ha querido establecer un ámbito «en el que el individuo sea el único capacitado para dar o no a conocer aquello que le afecta de forma personal y directa», dicha fundamentación común no implica que estemos ante los mismos objetos de protección jurídica[20].

Ciertamente, la protección de la comunicación, como hemos visto anteriormente, no se garantiza por su contenido privado o no; lo que conduce a Jiménez Campo a mantener la distinción entre intimidad como un concepto de carácter material, mientras que el secreto garantiza la libertad de comunicaciones[21]. Adviértase que la equivalencia entre intimidad y secreto se rompe en ocasiones, ya que este último puede proteger también otros derechos[22]. De este modo, como advertía Martín Morales, el secreto de las comunicaciones «funciona como una garantía de la intimidad, pero adquiriendo, además, la función de garantía de una gran variedad de derechos y libertades: contribuye

operan de manera diferente», lo cual es comprensible porque su naturaleza no es la misma: «Los términos propios de las palabras que la Constitución usa, la ubicación sistemática de este derecho, la finalidad que persigue, son todos ellos argumentos que conducen a la misma conclusión: la conexión del secreto de las comunicaciones con la vida privada, con la intimidad».

[18] Diaz Revorio, J.: «El derecho fundamental al secreto de las comunicaciones», *Derecho PUCP, Revista de la Facultad de Derecho*, núm. 59/2006, pp. 159-175. Enrique Belda Pérez-Pedrero señala la íntima relación entre el artículo 18.1 y el 18.3 al compartir una finalidad común de garantía de las relaciones personales, pero señala que tienen objetos distintos, en: «El derecho al secreto de las comunicaciones», *Anuario. Parlamento y Constitución*, núm. 2/1998.

[19] Sempere Rodríguez, C.: «Comentario al artículo 18 CE», en Alzaga Villaamil, O.: *Comentarios ala Constitución española de 1978*, Edersa, Madrid, 1996, p. 426. Considera el autor que tanto la inviolabilidad del domicilio como el secreto de las comunicaciones protegen «el derecho de la persona a la vida en libertad, garantizada por el respeto a la vida privada y el libre desarrollo de la personalidad (arts. 1 y 10 CE).

[20] Rebollo Delgado, L.: «El secreto de las comunicaciones: problemas actuales», en *Revista de Derecho Político*, núms. 48-49, 2000, pp. 366 y ss.

[21] Jiménez Campo, J.: «La garantía constitucional del secreto de las comunicaciones», *REDC*, núm. 20/1987, p. 41.

[22] Balaguer Callejón, F., en el Prólogo al libro de Martín Morales, R.: *El régimen constitucional del secreto de las comunicacione*s, Civitas, Madrid, 1995, p. 13.

a asegurar la libertad ideológica y política, garantiza la libertad de empresa, el secreto profesional, etc.» [23].

La naturaleza formal que permite proteger el proceso de la comunicación, independientemente de su contenido, contribuye a reafirmar el carácter autónomo del derecho, y la principal consecuencia que se anuda a dicha naturaleza autónoma es, realmente, el alcance de su protección.

Precisamente, en este tema se ha producido una notable evolución en la doctrina constitucional, ya que, en sus inicios, el Tribunal consideraba que la finalidad principal del secreto de las comunicaciones era el respeto del ámbito privado de la vida personal y familiar, que debía quedar excluido del conocimiento ajeno y de las intromisiones de los demás; salvo autorización del interesado [24]. Posteriormente, aun reconociendo la estrecha relación entre intimidad y el secreto de las comunicaciones [25], mantendrá que tiene éste último sustantividad propia respecto del derecho a la intimidad; por lo que, no solo protege las comunicaciones que tengan un contenido privado o íntimo, sino que el objeto directo de protección «es el proceso de comunicación en libertad y no por sí solo el mensaje transmitido, cuyo contenido puede ser banal o de notorio interés público» [26]. Protegiéndose así la libertad de la comunicación [27] (114/1984) el contenido del mensaje, sea de la naturaleza que sea, así como la identidad de los interlocutores o de los corresponsales, garantizando su impenetrabilidad por parte de terceros. Mientras que la intimidad, que es un concepto de carácter objetivo o material, protege un ámbito reservado de la vida de las personas excluido del conocimiento de terceros.

Un argumento que consideramos que permite la distinción entre ambos derechos con mayor claridad es el siguiente: mientras que el secreto de las comunicaciones protege dicha impenetrabilidad por parte de terceros; el derecho a la intimidad opera perfectamente inter partes; deslindándose la protección de quien recibe, por ejemplo, una carta, el 18.3 le garantiza que ningún agente externo la pueda interceptar (en sentido amplio), mientras que la del interlocutor que difunde su contenido, estaría protegida por el artículo 18.1. Por tanto, lo que la Constitución garantiza es su impenetrabilidad por parte de terceros, rechazando la interceptación o el conocimiento antijurídicos de las comunicaciones ajenas, y, excluyendo que este derecho pueda oponerse frente a quien tomó parte en

[23] Martin Morales, R.: *El régimen constitucional*, *ob. cit.,* p. 44.

[24] STC 110/1984, de 26 de noviembre.

[25] STC 85/1994, de 14 de marzo.

[26] STC 170/2013, de 7 de octubre.

[27] En este sentido se pronuncia también Díez-Picazo, L. M.ª: *Sistema de Derechos Fundamentales*, Civitas, Madrid, 2003.

dicha comunicación[28]. En el secreto de las comunicaciones estamos, pues, ante una protección *ad extra*, mientras que la intimidad opera, tanto *ad extra* como *ad intra*.

Pero, la relevancia de la separación del ámbito de protección de los derechos fundamentales a la intimidad personal (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE) se proyecta sobre el régimen de protección constitucional de ambos derechos. Así, mientras que la intervención de las comunicaciones requiere siempre resolución judicial, «no existe en la Constitución reserva absoluta de previa resolución judicial» respecto del derecho a la intimidad personal.[29] Ahora bien, ello no significa que la entrada en la intimidad no deba estar rodeada de una serie de garantías de modo que toda injerencia ha de contar con una justificación objetiva, razonable, prevista en la ley, idónea, necesaria. No olvidemos que también el artículo 18.1 regula un derecho fundamental y, en consecuencia, su limitación ha de cumplir con estas exigencias[30]; reconociéndose por el Tribunal que aún habiéndose admitido que «de forma excepcional que en determinados casos y con la suficiente y precisa habilitación legal» sean posibles determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, la legitimidad constitucional de dichas prácticas, requiere también el respeto de las exigencias dimanantes a) del principio de proporcionalidad, de modo que mediante la medida adoptada sea posible alcanzar el objetivo pretendido; b) —idoneidad—; que no exista una medida menos gravosa o lesiva para la consecución del objeto propuesto; c) —necesidad—; d) y que el sacrificio del derecho reporte más beneficios al interés general que desventajas o perjuicios a otros bienes o derechos atendidos la gravedad de la injerencia y las circunstancias personales de quien la sufre —proporcionalidad estricta[31].

[28] SSTC 114/1984, FJ 7; 175/2000, de 26 de junio, FJ 4; y 56/2003, de 24 de marzo, FFJJ 2 y 3.

[29] STC 123/2002, de 20 de mayo.

[30] SSTC 37/1989, de 15 de febrero, FJ 7; 207/1996, de 16 de diciembre, FJ 3; y 70/2002, de 3 de abril, FJ 10), entre otras.

[31] El Tribunal Constitucional considera que siendo el juez es el garante de los derechos fundamentales, se exige por regla general la autorización judicial previa en las injerencias al derecho a la vida privada, aunque tal autorización no esté expresamente exigida por el artículo 18.1 de la Constitución (STC 37/1989 de 15 de febrero, 57/1994 de 28 de febrero y 207/1996 de 16 de diciembre). Sin embargo, en la medida en que esta autorización no está prevista por la Constitución, el Tribunal Constitucional ha admitido en su STC 70/2002 de 3 de abril una excepción a dicha regla «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, a condición que la misma se realice también desde el respeto al principio de

1.2 El secreto como derecho autónomo, pero en conexión con otros derechos

Este reconocimiento autónomo del derecho al secreto de las comunicaciones no impide que pueda contribuir a la salvaguarda de otros derechos, libertades o bienes constitucionalmente protegidos, «como el secreto del sufragio activo, la libertad de opinión, ideológica y de pensamiento, de la libertad de empresa, la confidencialidad de la asistencia letrada o, naturalmente también, el derecho a la intimidad personal y familiar» [32].

Asimismo, R. Martínez ha destacado el poder de atracción del derecho fundamental a la protección de datos sobre algunos de los derechos del artículo 18 de la Constitución. Para el autor existe el peligro de una «cierta desnaturalización o desprotección del derecho al secreto de las comunicaciones cuando se aplican criterios de protección de datos a los supuestos de uso policial de datos técnicos vinculados a las comunicaciones» [33].

Señaladamente, en el marco del proceso penal, el triángulo formado entre secreto de las comunicaciones, tutela judicial efectiva y derecho a la presunción de inocencia es el que mayor relevancia adquiere. En efecto, el secreto de las comunicaciones puede estar en estrecha relación con el derecho a la tutela judicial efectiva, ya que la intervención de una comunicación puede venir anudada a las garantías del proceso y, en definitiva, a la presunción de inocencia. La conexión prueba ilícita y presunción de inocencia cobra todo su significado en el marco de este proceso, siendo de capital importancia resolver en qué casos puede o no conferirse valor a las escuchas, ya que en ningún momento el TEDH ha establecido que sea contraria al Convenio una condena basada exclusivamente en pruebas obtenidas ilícitamente [34].

---

proporcionalidad, siempre que «la valoración de la urgencia y necesidad de la intervención policial ha de realizarse ex ante, y es susceptible de control judicial *ex post,* al igual que el respeto del principio de proporcionalidad».

[32] STC 281/2006, de 9 de octubre.

[33] Martínez Martínez, R.: «El derecho fundamental a la protección de datos: perspectivas», *IDP*, núm. 5/2007, p. 58.

[34] López Guerra, L.: «El Diálogo entre el Tribunal Europeo de Derechos Humanos y los Tribunales». *Teoría y Realidad Constitucional*, núm. 32, 2013. Apunta que el Tribunal Europeo de Derechos Humanos, en *Bykov*, siguiendo jurisprudencia anterior, admite la presencia de una violación del derecho a la intimidad personal del artículo 8 del Convenio, como consecuencia de la grabación ilegítima; sin embargo, no considera que se haya producido una vulneración del derecho a un debido proceso por el hecho de que se haya empleado en éste una prueba ilegítimamente obtenida, destacando que «…Debe tenerse en cuenta que en el supuesto concreto de *Bykov,* el Tribunal además aduce que hubo otras pruebas a considerar por el juez nacional. Pero en ningún momento el Tribunal ha establecido que sea contraria al Convenio una condena basada exclusivamente en pruebas obtenidas ilícitamente», pp. 148-149.

2. ALCANCE DEL DERECHO AL SECRETO DE LAS COMUNICACIONES

2.1 Alcance frente a terceros

La naturaleza formal del secreto implica que el alcance de su protección se ciña solo a los interlocutores frente a terceros; planteándose en ese caso si la revelación de la información por uno de los interlocutores goza o no de protección. Ello plantea toda una serie de situaciones de difícil articulación: por ejemplo, qué pasa cuando uno de los interlocutores grava una conversación y la difunde; o cuando entrega a otro la carta recibida; o cuando emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes.

En este marco puede plantearse una rica casuística: por ejemplo, el uso del ordenador personal por ambos cónyuges, entrando uno de ellos entra en el servidor del correo del otro. Ciertamente, el uso de un ordenador personal por ambos no autoriza que uno de ellos entre en el servidor de correo de otro protegido con claves; en ese caso estaríamos ante una vulneración del secreto de la comunicación; mientras que si el servidor está en abierto difícilmente puede sostenerse tal secreto; ya que no habría expectativa de secreto. Y ese mismo supuesto podría plantearse si ambos utilizaran los canales de comunicación como *face time, Skype,* etc en abierto. En estos casos, solo el blindaje a través de clave permitiría recabar la tutela del artículo 18.3, en los demás casos estaríamos ante una hipotética vulneración de la intimidad[35].

La respuesta más pacífica es que esa información revelada por uno de los interlocutores está cubierta por las garantías del artículo 18.1 pero no por las del artículo 18.3. Pero, aún en ese caso, ello no hace más que derivar su protección hace el apartado 1 de este precepto; sin embargo, no resuelve si dicha protección

[35] Rodríguez Lainz, J. L: «Sobre la dimensión privada y familiar del derecho al secreto de las comunicaciones», *Diario La Ley*, n.º 7598, 28 de marzo de 2011, trabajo en el que se plantea innumerables situación en este orden, por ejemplo: ¿Alcanza este poder de exclusión al uso que pueda hacer el otro interlocutor de aquello que es el contenido o componentes externos de la comunicación en la que participa?; ¿podemos hablar de un deber de secreto que impediría, incluso cuando la conversación acredita la comisión de una infracción criminal, su desvelo sin incurrir en ilicitud?; ¿podemos hablar realmente de la existencia de una *dimensión familiar* del secreto de las comunicaciones, acorde con el concepto constitucional de derecho a la intimidad familiar a que se refiere el artículo 18.1 CE?; ¿alcanzaría esta pretendida dimensión familiar del secreto de las comunicaciones a la posibilidad de tener lícito acceso uno de los integrantes del grupo familiar sobre contenidos y datos de tráfico de las comunicaciones de otro sin su conocimiento o consentimiento?; ¿bajo qué circunstancias?

alcanza a toda clase de contenido o solo al que tenga carácter íntimo. Esto es, el secreto de las comunicaciones garantiza el proceso de comunicación con independencia del contenido **íntimo** o no; pero, la revelación de la comunicación por uno de los interlocutores, derivada al artículo 18.1, tendría cobertura solo en los casos en que su contenido recaiga en el esfera de la intimidad[36].

El Tribunal Constitucional en la Sentencia 114/1984 entiende que derecho al secreto de las comunicaciones no puede oponerse frente a quien tomó parte en la comunicación misma. «No hay «secreto» para aquél a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el artículo 18.3 de la C. E». Lo expresa claramente el Tribunal Supremo cuando, al reconocer la licitud de las conversaciones privadas grabadas por uno de los interlocutores, afirma que la vulneración del derecho recogido en el artículo 18.3 CE solo ocurre cuando se graba una conversación «de otro», pero no cuando se graba una conversación «con otro» (STS de 5-04-17). Por lo que, el levantamiento del secreto por uno de los intervinientes no se consideraría violación del artículo 18.3 CE, sino, en su caso, vulneración del derecho a la intimidad, en atención al deber de reserva en función del contenido de lo comunicado[37]. Incluso el propio Tribunal ha entendido[38] que no existe vulneración del derecho al secreto de las comunicaciones cuando uno de los interlocutores en la comunicación telefónica (el denun-

[36] Semper plantea que «Cabría mantener, pues, que el artículo 18.3 CE impone también a los comunicantes el deber de guardar secreto con independencia de la naturaleza privada, íntima o confidencial de su contenido, sin perjuicio de que tal derecho no pueda considerarse absoluto y quepan limitaciones fundadas en intereses legítimos y constitucionalmente relevantes, siempre que resulten proporcionadas», ob. cit., p. 442.

La protección de la revelación por parte de uno de ellos derivada del apartado primero del artículo 18 CE., la refuerza Rodríguez Lainz, con el artículo 7.2 de la LO 1/1082, de 5 de mayo, de Protección civil del Derecho al Honor, a la Intimidad y a la Propia Imagen, al considerar como intromisión ilegítima en el secreto de las comunicaciones la «utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción». Rodríguez Lainz, J. L: «Sobre la dimensión privada y familiar del derecho al secreto de las comunicaciones», *Diario La Ley*, n.º 7598, 28 de Marzo de 2011.

[37] En esta línea sostiene Jimenez Campo que la grabación subrepticia de la comunicación verbal por uno de los participantes no implica contravención del secreto de la comunicación, «sea cual sea el juicio moral que esta conducta pueda merecer, con ella no se viola ningún secreto ni se hace otra cosa que documentar, de modo específico, lo que más tarde se va a revelar», ob. cit., p.

[38] STC 56/2003. Así lo mantiene también Guisasola Lerma, C.: «Tutela penal del secreto de las comunicaciones, Estudio particular del supuesto de interceptación ilegal de telecomunicaciones por autoridad o funcionario público», en *Constitución, Derechos Fundamentales y Sistema Penal*, Cuerda Arnau, M. L. (Coord.), Tirant lo Blanch, Tomo I, p. 949.

ciante del chantaje al que se encontraba sometido) quien autorizó expresamente a la Guardia Civil a que registrara sus conversaciones para poder determinar así el número desde el que le llamaban.

Esta construcción puede tener repercusiones bien distintas en los ámbitos civil y penal. En este último González Cussac advierte y critica, posición que compartimos, la tesis de los que haciendo una lectura defectuosa de la STC 114/1984 han considerado que entre interlocutores no rige la protección constitucional del artículo 18 CE cuando uno de ellos decide revelarlo[39]. En efecto, como advierte el autor, desde la perspectiva del derecho penal «desde el contenido del artículo 18.1 CE el deber de reserva constitucionalmente protegido no impide la transmisión oral o por escrito de lo comunicado por una de las partes, ya que puede entenderse que éstas renuncian implícitamente a controlar el destino de la información desde que la transmiten o comparten». Ahora bien, persisten las dudas acerca de la «valoración penal a la respuesta en circulación de la propia comunicación —o de su grabación subrepticia—, habida cuenta que el acto de comunicación no conlleva una renuncia a controlar la eventual plasmación material o la grabación de lo comunicado».

Sin embargo, la Sala 2.ª del Tribunal Supremo[40], partiendo del carácter no horizontal de los derechos fundamentales reconocidos en la Constitución, mantiene que no existe una vulneración del derecho a la intimidad cuando el propio afectado es el que ha exteriorizado sus pensamientos sin coacción de ninguna especie, considerando que el artículo 18 de la CE no garantiza el mantenimiento del secreto de los pensamientos que un ciudadano comunica a otro. Su posición se concreta en que «No existe vulneración al derecho a la intimidad cuando es el propio recurrente quien ha exteriorizado el contenido de sus pensamientos sin coacción de ninguna especie»[41];«(...) cuando alguien emite voluntariamente sus secretos, sabe que se desaloja de su intimidad respecto a otros «quienes no podrán incurrir en ningún tipo de reproche jurídico»». Solamente cabría admitir una tal vulneración «(...) si la conversación fuese fruto de una coacción o añagaza policial para provocar la autoinculpación del recurrente»[42].

A nuestros efectos la revelación entre interlocutores queda fuera del ámbito del artículo 18.3, pero no nos alberga duda que puede recibir la protección del

[39] Gonzalez Cussac, J. L.: «La tutela penal del derecho a la intimidad desde el canon de la expectativa razonable de privacidad», en *Derecho Penal para un Estado Social y Democrático de Derecho. Estudios en Homenaje al Profesor Emilio Octavio de Toledo y Ubieto*, Madrid, Servicio de Publicaciones de la Universidad Complutense, pp. 641-652.

[40] *Vid.* Con mayor detenimiento Rodriguez Lainz, J. L.: *Sobre la dimensión…,* ob. cit.

[41] STS 1017/2001, de 9 de junio, la 386/2002, de 27 de febrero.

[42] STS, Sala 2.ª, 1017/2001, de 9 de junio.

artículo 18.1. Cuándo deba entenderse que ese contenido reviste notas de intimidad es una cuestión que escapa del objeto de este trabajo.

Lo que sí ha quedado sentado recientemente en orden a las comunicaciones verbales es que ni el artículo 579.2 LECrim ni la normativa penitenciaria habilitan la intervención de las comunicaciones verbales directas entre los detenidos en dependencias policiales[43]. Nuevamente, se incide en la doctrina del Tribunal Constitucional y del Tribunal Supremo reafirmando que la insuficiencia de la regulación legal y la posibilidad de suplir los defectos de la Ley, no puede «ser trasladada a un escenario de injerencia en el secreto de las comunicaciones en el que no exista previsión legal alguna».

2.2 Alcance del proceso de comunicación

¿Qué intervalo protege el artículo 18.3 y qué sucede cuando se ha superado la fase del tránsito de la comunicación? Esto es, ¿desde cuándo y hasta cuándo el proceso de la comunicación goza de la cobertura de este apartado?; ¿cubre solo la comunicación en tránsito?, ¿o también el posterior almacenaje de lo comunicado?; por ejemplo ¿alcanza a la correspondencia guardada por su destinatario, o al almacenaje de mensajes de correo electrónico?; y, en consecuencia, si concluida la comunicación ya ha finalizado la cobertura del secreto de la comunicación, ¿ésta pasa a estar cubierta por el artículo 18.1 o por el artículo 18.4?

De acuerdo con la doctrina constitucional, el secreto puede resultar vulnerado tanto por la interceptación en sentido estricto (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 (114/1984). Pero, la duda que se plantea es si ese conocimiento antijurídico debe ser adquirido durante el proceso comunicativo, o si cabe la posibilidad de abarcar más allá, cuando este ha finalizado, alcanzando, también, al contenido o elementos externos conservados en un soporte u objeto físico[44].

En la STC 70/2002 de 3 de abril el Tribunal sostiene 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

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

[44] Rodríguez Lainz, J. L: «Sobre la naturaleza formal del derecho al secreto de las comunicaciones: dimensión constitucional e histórica», *Diario La Ley*, n.º 7647, Sección Doctrina, 8 de Junio de 2011, p. 5 y ss. en las que realiza el estudio más detallado de la doctrina constitucional, que seguimos.

constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos», de modo que la protección de este derecho viene referido, sólo, a las interferencias habidas o producidas en un proceso de comunicación[45]. La trascendencia del tema se centra en la posibilidad o imposibilidad de valoración de la 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.

Se ha ido consolidando la tesis de que el control posterior de las escuchas, al no tener lugar durante la ejecución del acto limitativo del derecho al secreto de la comunicación, no forma parte de las garantías del artículo 18.3, sin perjuicio de su relevancia a efectos probatorios. Pues el derecho al Secreto de las comunicaciones rige mientras se desarrolla el proceso de la comunicación; ratificándose en la Sentencia de la Sala de lo Penal del Tribunal Supremo 864/2015, de 10 de diciembre que derecho al secreto de las comunicaciones rige mientras se desarrolla el proceso de comunicación. Una vez cesado éste, llegado el mensaje al receptor, sale del ámbito del artículo 18.3 CE, sin perjuicio, en su caso, del derecho a la intimidad[46]. Ciertamente, esta posición nos plantea serias dudas, a las que nos referiremos más tarde.

2.3 Alcance en relación con los titulares

El contenido esencial del derecho al secreto de las comunicaciones plantea, asimismo, importantes cuestiones relativas a su titularidad; aunque en este trabajo señalaremos solo algunas de ellas.

[45] Manteniéndose esta línea en la STC 137/2002, que el proceso de la comunicación debía haberse iniciado para poder contar con la cobertura del artículo 18.3, manteniendo que la entrega de los listados de llamadas por las compañías telefónicas a la policía sin consentimiento del titular del teléfono requiere resolución judicial. Ya que «La difusión sin consentimiento de los titulares del teléfono o sin autorización judicial de los datos captados en la interferencia directa en el proceso de comunicación, supone la vulneración del derecho al secreto de las comunicaciones». Lo que le lleva a concluir que a intervención de una carta en poder de un detenido por la policía, sin autorización judicial, no afecta al derecho al secreto de las comunicaciones sino, en su caso, al derecho a la intimidad; aunque tampoco vulnera el derecho a la intimidad porque existe un fin constitucionalmente legítimo; la medida limitativa del derecho está prevista en la ley y hay una estricta observancia del principio de proporcionalidad.

[46] SSTS 342/2013, de 17 de abril; 786/2015, de 4 de diciembre, 859/2014, de 26 de noviembre.

Por un lado, se suscita qué alcance tiene este derecho en relación con los menores de edad; reconociéndoles la Ley Orgánica[47], la titularidad del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones. El problema que plantea este reconocimiento es el de determinar su contenido preciso y los límites, ya que se vincula a los padres o tutores, así como a los poderes públicos para que lo respeten y los protegerán frente a posibles ataques de terceros. Pues bien, esta protección del menor en ocasiones puede colisionar con el deber de los padres o tutores, ya que podemos plantearnos ¿hasta qué punto puede un padre o tutor que advierte que un menor del que es responsable puede estar teniendo problemas de acoso o de pederastia no conocer sus comunicaciones?[48].

La solución de los conflictos que se pueden plantear en este sentido, no la contiene la Ley del Menor, destacando la interpretación de Pablo Luca Murillo, cuando entiende que la protección del derecho del menor lo es frente a terceros, pero que en relación con los padres puede llegar a valorarse su injerencia en la comunicación, debiéndose valor las circunstancias y la edad del menor[49].

Cabe destacar en este sentido la referida Sentencia de la Sala de lo Penal del Tribunal Supremo 864/2015, de 10 de diciembre, en la que se plantea el acceso a

[47] Ley Orgánica 8/2015, de 22 de julio, de modificación del sistema de protección a la infancia y a la adolescencia. 2. *Las comunicaciones del menor con familiares y otras personas allegadas serán libres y secretas.* Sólo podrán ser restringidas o suspendidas por el Director del centro en interés del menor, de manera motivada, cuando su tratamiento educativo lo aconseje y conforme a los términos recogidos en la autorización judicial de ingreso. La restricción o suspensión del derecho a mantener comunicaciones o del secreto de las mismas deberá ser adoptada de acuerdo con la legislación aplicable y notificada a las personas interesadas, al menor y al Ministerio Fiscal, quienes podrán recurrirla ante el órgano jurisdiccional que autorizó el ingreso, el cual resolverá tras recabar informe del centro y previa audiencia de las personas interesadas, del menor y del Ministerio Fiscal.

Asimismo, el artículo 3 de la Ley 1/1982, de 5 de mayo de Protección Civil del Derecho al Honor, a la Intimidad y a la Propia Imagen establece que el consentimiento deberá prestarse por ellos mismos (menores) si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil, para en los restantes casos otorgarse mediante escrito de su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado.

[48] Rodriguez Laínz: *La dimensión…*, ob. cit, analiza las STS 803/2010, de 30 de septiembre, que prevé la posible apreciación de circunstancias en las que se justifique la conducta de los padres de adentrarse en la intimidad o secreto de las comunicaciones de sus hijos para protegerlos de graves afrentas contra su interés……. Entran en juego, no solo el cumplimiento de un derecho-deber, sino incluso situaciones de auténtica legítima defensa o estado de necesidad, a la vez que circunstancias en las que el error de hecho o de prohibición desplegará toda su eficacia excluyente de responsabilidad criminal.

[49] Lucas Murillo de la Cueva, P.: *Notas sobre el derecho fundamental..,* ob. cit*,* p. 673.

la cuenta abierta por una menor de una red social por parte de su madre sin contar con su anuencia, ante la sospecha de que pudiera estar siendo víctima de un delito. Y, aunque la Sala reconduce el tema planteado a la lesión del derecho a la intimidad, mantiene una argumentación igualmente válida en este orden de consideraciones, ya que parte de la titularidad de la patria potestad —no como poder— sino como función tuitiva respecto de la menor; sostiene que es la madre quien accede a esa cuenta ante signos claros de que se estaba desarrollando una actividad presuntamente criminal en la que no cabía excluir la victimización de su hija. Desde esta perspectiva, afirma que *«No puede el ordenamiento hacer descansar en los padres unas obligaciones de velar por sus hijos menores y al mismo tiempo desposeerles de toda capacidad de controlar en casos como el presente en que las evidencias apuntaban inequívocamente en esa dirección»*. De forma que, la inhibición de la madre ante hechos de esa naturaleza, contrariaría los deberes que le asigna por la legislación civil[50]. En definitiva, permite el acceso de los padres a las cuentas de las redes sociales de sus hijos menores, ante las sospechas de que éstos estén siendo víctimas de un delito.

Asimismo, el alcance del derecho al secreto de las comunicaciones ha venido planteando importantes problemas en el ámbito penitenciario. Por un lado, la relación de especial sujeción que supone la vida en prisión puede incidir sobre las comunicaciones de los internos en centros penitenciarios, afectándose en este caso al artículo 18.3 CE[51]. Por otro, en este mismo ámbito puede producirse también una afectación de las comunicaciones entre el abogado y su cliente interno en el centro; afectando, en este caso al derecho de defensa. Ámbito en el que la insuficiencia, ambigüedad y complejidad[52] de la normativa española sobre

[50] La Sentencia aborda el tema del ciberacoso sexual introducido en la LO 5/2010 (art. 183 bis, delito online child grooming), en la que se dirime la petición de nulidad de las pruebas obtenidas en los mensajes de Facebook y Whatsapp intercambiados entre el autor y las víctimas. Máxime cuando «Se trataba además de actividad delictiva no agotada, sino viva: es objetivo prioritario hacerla cesar. Tienen componentes muy distintos las valoraciones y ponderación a efectuar cuando se trata de investigar una actividad delictiva ya sucedida, que cuando se trata además de impedir que se perpetúe, más en una materia tan sensible como esta en que las víctimas son menores».

[51] Revriego Picón, F.: «El secreto de las comunicaciones en los centros penitenciarios: comunicaciones escritas «entre» reclusos», *Boletín de la Facultad de Derecho de la UNED*, núm. 26/2005, pp. 573-588., así como *Los derechos de los reclusos en la jurisprudencia constitucional*, Universitas, 2008.

[52] Martínez Alarcón, M. L.: «El derecho al secreto de las comunicaciones de los internos en establecimiento penitenciario con sus representantes legales», *Revista Española de Derecho Constitucional*, núm. 92, 2011, pp. 141-167; Chaves Pedrón, C.: «El secreto de las comunicaciones en el medio penitenciario. Especial referencia a las comunicaciones abogado cliente», *Revista jurídica de la Comunidad Valenciana: jurisprudencia seleccionada de la Comunidad Valenciana*, núm. 49/2014, pp. 167-184.

la intervención de las comunicaciones, se intensifica como se ha venido demostrando en la realidad.

Por último, el Centro Nacional de Inteligencia puede proceder al control de las comunicaciones, de acuerdo con lo establecido en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, completada por la LO 2/2002 y modifica la Ley Orgánica del Poder Judicial, a los efectos de establecer un control judicial de las actividades del citado Centro que afecten a los derechos fundamentales reconocidos en el artículo 18.2 y 3 de la Constitución española. Determina tanto la forma de nombramiento de un Magistrado del Tribunal Supremo específicamente encargado del control judicial de las actividades del Centro Nacional de Inteligencia, como el procedimiento conforme al cual se acordará o no la autorización judicial necesaria para dichas actividades. El plazo para acordarlas será ordinariamente de setenta y dos horas, pudiendo reducirse, de forma extraordinaria y por motivos de urgencia debidamente justificados, a veinticuatro horas. Sin embargo, no especifica los hechos que pueden dar lugar a su intervención.

2.4 Alcance en relación con las clases de comunicación

El carácter obsoleto de la LECrim, conducía a que el artículo 579 únicamente planteara la interceptación de las comunicaciones postales, telegráficas y telefónicas. Ello ha abocado a la Jurisdicción ordinaria y a la constitucional a abordar los nuevos conceptos de comunicación, extendiendo la protección del artículo 18.3 a toda clase de comunicación, y en particular a las nuevas tecnologías. 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[53]. Aunque, como ha advertido Ascensión Elvira, el Tribunal Constitucional ha sentado una doctrina más clara en relación con las comunicaciones tradicionales, mientras que en relación con las nuevas tecnologías se muestra más dubitativo[54].

[53] Así lo ha reconocido el Tribunal Supremo en Sentencia 51/2010, de 5 de febrero, SSTS núm. 367/2001, de 22 de marzo y núm. 1377/1999, de 8 de febrero.

[54] Elvira Perales, A.: «Qué hay de nuevo en torno al derecho al secreto de las Comunicaciones» en *La constitución política de España: estudios en homenaje a Manuel Aragón Reyes* / coord. por Francisco Rubio Llorente, Javier Jiménez Campo, Juan José Solozábal Echavarría, M. Paloma Biglino Campos, Angel José Gómez Montoro, 2016, CEPC, Madrid, 2016, pp.

Pero, son diversos los problemas detectados acerca del alcance de las comunicaciones que gozan de la cobertura del artículo 18.3 CE.

(i) Por un lado, se ha venido suscitando a la largo de todos estos años el alcance de la protección constitucional acerca de los **envíos postales**; de hecho, ha generado una importante doctrina constitucional en la que el Tribunal Constitucional admitió implícitamente que el paquete postal quedaba amparado bajo la cobertura del derecho al secreto de las comunicaciones del artículo 18.3 CE; sin embargo, con posterioridad ha clarificado que la noción constitucional de comunicación postal es una noción restringida que no incluye todo intercambio realizado mediante los servicios postales (281/2006). Se identifica la comunicación postal con la correspondencia; por lo que no gozan de la protección constitucional aquellos objetos —continentes— que por sus propias características no son usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías[55]; ni tampoco gozan de la protección constitucional del artículo 18.3 CE aquellos objetos que, pudiendo contener correspondencia, sin embargo, la regulación legal prohíbe su inclusión en ellos. Y es que, como ha señalado en reiteradas Sentencias la Sala Segunda del Tribunal Supremo, el artículo 18.3 no protege directamente el objeto físico, el continente o soporte del mensaje en si, sino que éstos solo se protegen de forma indirecta, tan solo en la medida en que son instrumento a través del cual se efectúa la comunicación entre las persones —destinatario y remitente—[56].

(ii) Respecto de las **comunicaciones telefónicas** no se regulaba su intervención hasta la reforma operada en la LECRim en el año 1988, de modo que habiendo evolucionado tanto este canal de comunicación[57], se ha ido planteando y resolviendo casuísticamente la equiparación entre la **telefonía móvil y la fij**a. Y en este campo, podemos encontrar un elevado número de pronunciamientos

613-614, por lo que apunta la conveniencia de que profundice en la clarificación y alcance de los límites del secreto de las comunicaciones en este campo, trascendiendo para ello de los medios de comunicación clásicos.

[55] ATC 395/2003, de 11 de diciembre.

[56] Por todas, *vid.* la Sentencia 340/2016, de 6 de abril.

[57] Recientemente, el TEDH ha dictado sentencia el 8 de noviembre de 2016 en el asunto Figueiredo Teixeira c. Andorra, en el que el demandante reclamaba la vulneración de su derecho a la vida privada y familiar, por el almacenamiento y utilización como prueba en el proceso penal en el que figuraba como acusado, del registro de llamadas realizadas desde su número privado de teléfono móvil. El TEDH concluye que el almacenamiento de los datos de las llamadas por parte de la compañía telefónica y su posterior transmisión a requerimiento del juzgado no constituye una vulneración del derecho a la vida privada del acusado, ya que si bien la utilización de dichos datos constituye una injerencia en su vida privada, dicha injerencia se encuentra prevista por ley, es proporcional y se encuentra suficientemente justificada por la finalidad perseguida.

que han debido enfrentarse a supuestos novedosos generados por el avance de las nuevas tecnologías.

Uno de los problemas que se plantea en el marco de la telefonía móvil es determinar si el secreto de las comunicaciones ampara tanto el contenido de la comunicación como los elementos externos, planteándose el alcance del secreto respecto de los denominados datos de tráfico[58], que se han han diferenciado del contenido de la comunicación. Habiendo sentado al respecto el TS que los datos de tráfico generados están protegidos por el artículo 18.3 CE, entendiendo como tales siguiendo la pauta interpretativa ofrecida por el TEDH, los datos indicativos 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[59]. Mientras que información albergada en la serie IMSI no participa de ninguna de esas características, y, en consecuencia no le alcanza la cobertura del artículo 18.3.

Estos números IMSI (número internacional de la tarjeta telefónica o IMEI (número correspondiente al chasis del terminal) son datos que permiten identificar tanto el número como la localización del teléfono, por lo que al permitir identificar la tarjeta SIM se consideran datos de tráfico. Sin embargo, tras una cuestionada posición de la Sala Segunda del Tribunal Supremo, iniciada con la Sentencia 130/2007, de 19 de febrero, se reafirma que la captura de estos I. M. S. I. o I. M. E. I. no precisa de previa autorización judicial. Reafirmándose en la más reciente STS 481/2016, de 2 de junio en la que reitera y aclara su posición concluyendo que I. M. S. I., por sí solo ni es un dato integrable en el concepto de comunicación, ni puede ser encuadrado entre los datos especialmente protegidos, ya que solo expresa una serie alfanumérica incapaz de identificar, por su simple lectura, el número comercial del abonado y otros datos de interés para la identificación de la llamada. Por tanto, la recogida o captación técnica del I. M. S. I. no necesita autorización judicial, sin embargo, la obtención de su

[58] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, aplicable a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado. En su artículo 3 establece los datos que los operadores han de conservar, y en la Disposición final primera, de Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Regulando los datos que los sujetos obligados deberán facilitar al agente facultado para la interceptación.

[59] SSTS n.º 249/2008, de 20 de mayo, 776/2008, de 18 de noviembre, 688/2009, de 18 de junio.

plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia[60].

Asimismo, el TS ha entendido que la obtención del número PIN (dato de acceso a loa terminal) del teléfono utilizado, por un investigado no necesita autorización judicial, por no tratarse de dato alguno relativo a las comunicaciones (STS 551/2016, de 22 de junio).

Por otro lado, el acceso al registro de llamadas de un móvil sin autorización judicial si que se ha considerado como una vulneración del secreto de **las comunicaciones**[61]**.** Pero no el acceso a la agenda, pues los datos extraídos no forman parte de una comunicación actual o consumada, sino una intromisión al derecho a la intimidad[62]**.**

La telefonía móvil plantea una serie de problemas en orden a su seguridad de compleja articulación; nos referimos a la encriptación de terminales y archivos que impiden el acceso a los mismos incluso a las compañías. Si bien es cierto que este tema se ha planteado en Estados Unidos en el denominado «Caso San Bernardino», puede plantearse en un futuro nada lejano en nuestro ordenamiento[63]. Las «puertas traseras» pueden afectar al secreto de las comunica-

[60] «Ni es un dato integrable en el concepto de comunicación, ni puede ser encuadrado entre los datos especialmente protegidos…..ese número de identificación solo expresa una serie alfanumérica incapaz de identificar, por su simple lectura, el número comercial del abonado y otros datos de interés para la identificación de la llamada. Para que la numeración I. M. S. I. brinde a los investigadores toda la información que alberga, es preciso que esa serie numérica se ponga en relación con otros datos que obran en poder del operador. Y es entonces cuando las garantías propias del derecho a la autodeterminación informativa o, lo que es lo mismo, del derecho a controlar la información que sobre cada uno de nosotros obra en poder de terceros, adquieren pleno significado. Los mismos agentes de Policía que hayan logrado la captación del I. M. S. I. en el marco de la investigación criminal, habrán de solicitar autorización judicial para que la operadora correspondiente ceda en su favor otros datos que, debidamente tratados, permitirán obtener información singularmente valiosa para la investigación».

[61] La entrega de los listados de llamadas telefónicas por las compañías telefónicas a la policía, sin consentimiento del titular del teléfono, requiere resolución judicial (SSTC 123/2002, 115/2013; SSTEDH casos *Malone contra Reino Unido* de 2 de agosto de 1984, *Copland contra Reino Unido* de 3 de abril de 2007).

[62] STC 115/2013, de 9 de mayo. De modo que, al no ser el derecho a la intimidad un derecho absoluto, puede ceder ante intereses constitucionales relevantes siempre que el fin sea constitucionalmente legítimo y proporcionado (STC 142/2012).

[63] Muy sucintamente, en este caso se plantea un conflicto entre el Buró Federal de Investigaciones de EE. UU (FBI) y la compañía Apple. Como reacción a las revelaciones de Edward Snowden sobre los programas de vigilancia electrónica Apple decide proteger sus dispositivos con archivos encriptados, de modo que ni siquiera ella puede tener acceso a los mismos. Tras los atentados en 2015 de San Bernardino (California), el FBI solicita a Apple el acceso al terminal del autor de los mismos, pues al estar protegido exigía levantar el System Information File (SIF) para

ciones, y no solo en relación con los poderes públicos, sino también en relación con particulares especializados en hackear cuentas y terminales. Pensemos, por ejemplo, que no solo algunos terminales están protegidos, sino que también los mensajes de whatsapp están encriptados, de modo que cuando la Policía solicita la intervención de un terminal, la compañía no puede acceder a dichos contenidos encriptados.

(iii) Las comunicaciones electrónicas, amparadas en el artículo 18.3, plantean nuevos problemas acerca del alcance temporal y el soporte físico de su secreto; esto es, se trata de determinar si los correos electrónicos residenciados en el ordenador cuentan con la cobertura o no del artículo 18.3[64]. Siendo de especial interés al respecto las directrices de la Fiscalía General del en su Circular 1/2013, en las que se reconoce que debe considerarse necesaria la autorización judicial para acceder a cualquier mensaje enviado por correo electrónico, ya se trate de correo electrónico enviado y recibido pero no leído, correo en fase de transferencia o correo ya enviado, recibido y leído y que se encuentra almacenado.

Sin embargo, más recientes Sentencias del Tribunal Supremo (342/2013, de 17 de abril y 786/2015, de 4 de diciembre) abordan este tema y han entendido que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en algunas de las bandejas del

---

acceder a la información del dispositivo. La Compañía niega dicho acceso alegando que ello supondría abrir una puerta alternativa de acceso distinta a la contraseña: la denominada «puerta trasera». Y, aunque el FBI solicitaba que solo ellos y Apple podían disponer de la información que después podría ser destruida, ésta basa su negativa en que abrir puertas alternativas supone un riesgo elevado, pues muchos hackers o empresas podrían acceder, también, a la información. La negativa de Apple preservando la seguridad de su sistema termina con la obtención de la información ofrecida por una empresa israelí, que, además, cobró una cantidad muy elevada por la realización del servicio (90.0000 dolares).

Los medios The Associated Press, Usa Today y Vice News solicitan ante un Tribunal Federal que obligue al FBI a revelar las herramientas que contribuyeron a desbloquear el teléfono. Este pasado 30 de septiembre de 2017 el Tribunal ha denegado la petición, amparándose en que revelar la información pondría en riesgo la identidad del servicio de desbloqueo; del mismo modo, la Corte niega que deba ofrecerse información sobre el coste económico de esta operación.

[64] Coincidimos con Ascensión Elvira cuando plantea que «mantenerla como protección del derecho al secreto de las comunicaciones ofrece una mayor garantía además porque….la intromisión de la intimidad no precisa previa autorización judicial. Además resulta una interpretación más adecuada con la consideración de que constituye una vulneración del artículo 18.3 «el conocimiento antijurídico de lo comunicado», *ob. cit,* p. 606. *Vid.* también sobre las comunicaciones electrónicas Zoco Zabala, C: «Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de SITEL con el artículo 18.3 CE», *InDret*, 4/ 2010.

programa de gestión dejan de integrarse en el ámbito propio de la inviolabilidad de las comunicaciones[65], ya que la comunicación ha concluido su ciclo.

Ciertamente, nos parece cuestionable esta posición, pues vacía de contenido el derecho al secreto de las comunicaciones electrónicas. Aunque el Tribunal Constitucional ha entendido que el contenido de un ordenador personal se encuentra protegido por el derecho a la intimidad, entendemos que no todo el contenido de un ordenador puede esta sujeto al artículo 18.1 de la Constitución. De hecho, la bandeja del servidor de correo está protegida por clave de acceso, por ello no compartimos el criterio de la temporalidad del proceso de la comunicación para derivar su protección al artículo 18.3. La bandeja del correo puede tener un elevado número de correos guardados durante varios años, de modo que mientras esté protegido por clave de acceso creemos que constituye secreto de la comunicación. Distinto sería el supuesto de que un correo se guardara en un archivo del ordenador depositado en una carpeta abierta, sin acceso limitado.

Y el mismo tratamiento puede darse a un mensaje de un teléfono móvil, cuyo acceso esté cerrado.

En el marco de las comunicaciones electrónicas debemos referirnos a la STJUE[66] (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland Ltd*[67] en la que se declara la invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. La Directiva tenía como objetivo la lucha contra la delincuencia organizada, y, por tanto regulaba la utilización de los datos relativos al uso de comunicaciones electrónicas como instrumentos valiosos en la prevención de delitos y la lucha contra dicha la delincuencia organizada. En particular, en relación con el objeto de nuestro

[65] Esta es la posición mantenida por el TEDH en el caso Copland c. Reino Unido (2007).

[66] Asunto C-293/12. Y es que como ha puesto de relieve Artemi Rallo Lombarte el «TJUE se ha convertido en un auténtico juez garante de la privacidad ante la evolución tecnológica global», en «El Tribunal de Justicia de la Unión Europea como garante de la privacidad en Internet», *Teoría y Realidad Constitucional*, núm. 39/2017, p. 584.

[67] El Tribunal entiende que se han sobrepasado los límites que exige el respeto del principio de proporcionalidad, y señala que los datos que han de conservarse permiten saber con que persona y de que modo se ha comunicado un abonado o un usuario registrado, determinar el momento de la comunicación y el lugar desde el que esta se ha producido y conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un periodo concreto. Estos datos, considerados en su conjunto, pueden proporcionar indicaciones muy precisas sobre la vida privada de las personas cuyos datos se conservan, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, las relaciones sociales y los medios sociales frecuentados.

trabajo, regulaba[68] la conservación de todos los datos de tráfico relativos a la telefonía fija, la telefonía móvil, el acceso a Internet, el correo electrónico por Internet y la telefonía por Internet. Por lo tanto, era aplicable a todos los medios de comunicación electrónica, comprendiendo a todos los abonados y usuarios registrados.

El Tribunal sienta las exigencias de que dicho uso por parte de las autoridades nacionales debe responder a un objetivo de interés general, comprobando la proporcionalidad de la injerencia para lograr los objetivos, sujetándose al control jurisdiccional.

Muy sintéticamente, la Directiva afectaba, con carácter global, a todas las personas que utilizaran servicios de comunicaciones electrónicas, de modo que podían conservarse datos de personas que no estuvieran, ni siquiera indirectamente, en una situación que pudiera dar lugar a acciones penales.

- No exigía ninguna relación entre los datos conservados y una amenaza para la seguridad pública; ni se limitaba a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que pudieran estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves.
- Tampoco fijaba criterios objetivos que permitieran delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que, debido a la magnitud y la gravedad de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, puedan considerarse suficientemente graves para justificar tal injerencia. Por el contrario, la Directiva 2006/24 se limitaba a remitir de manera general a los delitos graves tal como se definen en la legislación nacional de cada Estado miembro.

La Sentencia es, desde luego, relevante. Aunque puede destacarse que, en principio, solo afectaría a nuestro ordenamiento interno en dos temas concretos: en relación con la exigencia de proporcionalidad y en relación con la consideración de delitos graves definidos en nuestro ordenamiento. Los demás temas apuntados estaban ya regulados en la Ley 25/2007 de 18 de octubre, de conser-

[68] Artículo 3 en relación con su artículo 5, apartado 1. «Considera el Tribunal que la normativa de la Unión de que se trate debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos».

vación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Además, en relación con la las reglas relativas a la seguridad y a la protección de los datos conservados por los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, la Directiva 2006/24 no garantizaba que los proveedores aplicaran un nivel especialmente elevado de protección y seguridad a través de medidas técnicas y organizativas, y no garantizaba la destrucción definitiva de los datos al término de su período de conservación; ni obligaba a que los datos en cuestión se conservaran en el territorio de la Unión.

Cabe destacar que estas objeciones no son relevantes desde el punto de vista del ordenamiento español, ya que el Título VIII del Real Decreto 1720/2007[69] impone a los operadores de telecomunicaciones la aplicación de las medidas de nivel de medios de seguridad, así como contar con un registro de accesos sujeto a una serie de exigencias.

Pero, la protección de datos concernientes a las comunicaciones electrónicas se enfrenta, también, a los retos de los movimientos internacionales de datos; en este marco es de especial interés la Sentencia del Tribunal de Justicia de la Unión Europea 6 de octubre de 2015, en el «*caso Schrems*»[70], que declara la invalidez de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, por permitir a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas.

La citada Decisión era relativa al acuerdo para mantener el flujo de datos derivados de comunicaciones electrónicas entre la Unión Europea y EEUU garantizando los derechos fundamentales, a través del un puerto seguro. Este acuerdo Safe Harbor (Puerto Seguro) es una plataforma a la que voluntariamente se adhieren las empresas americanas aceptando unas normas de protección de datos y respeto a la privacidad acordes con la legislación comunitaria. Sin embargo, estos principios de puerto seguro no son aplicables a las autoridades norteamericanas, que, en el marco de FISA, pueden hacer prevalecer las exigencias de seguridad nacional, interés público y cumplimiento de la ley de EEUU sobre el régimen de puerto seguro. Ello permite la intervención de las comunicaciones sin autorización judicial.

[69] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. El artículo 103, en concreto, regula el Registro de accesos.

[70] Sentencia en el asunto C-362/14, Maximillian Schrems/Data Protection Commissioner.

La Sentencia *Safe Harbor* entiende que el sistema jurídico norteamericano no garantiza, entre otros, el secreto de las comunicaciones en el contexto de los poderes que le otorga FISA[71]; por lo que declara la invalidez de la Decisión considerando que la Directiva sobre el tratamiento de los datos personales dispone que en principio solo se pueden transferir dichos datos a un país tercero si éste garantiza un nivel de protección adecuado de dichos datos. Considerando que las autoridades nacionales de control deben poder apreciar con toda independencia si la transferencia de los datos de una persona a un país tercero cumple las exigencias establecidas por la Directiva. El Tribunal de Justicia considera que la Comisión carecía de competencia para restringir de ese modo las facultades de las autoridades nacionales de control.

Tras esta Sentencia que declara la invalidez del *Safe Harbor*, la necesidad de encontrar un marco seguro ha dado paso a la aprobación por la Comisión Europea[72] del Acuerdo *Privacy Shield* (Escudo de Privacidad) en julio de 2016[73]. Este Acuerdo sigue planteando una serie de interrogantes que escapan del objeto y la dimensión de este trabajo[74].

2.5 Comunicaciones abiertas e intervención privada

Ciertamente, podemos encontrar supuestos en los que, aún tratándose de comunicaciones, éstas pueden ser objeto de intervención, incluso fuera del marco de un procedimiento judicial, y sin necesidad, a priori, de autorización judicial. Estamos ante comunicaciones que no se realizan a través de medios o canales cerrados, habiéndose aceptado la intervención de las mismas en determinados casos. En el marco laboral se ha abierto paso la doctrina del canal cerrado y de la expectativa de privacidad, que se sustenta en los siguientes términos:

Por un lado, la Sentencia 241/2012 del Tribunal Constitucional ha reconocido que, en virtud de las facultades de auto organización, dirección y control

[71] Martinez Martinez, R.: «Safe Harbor: retos para el modelo europeo de la privacidad» (http://tecnologia.elderecho.com/tecnologia/privacidad/Safe-Harbor-modelo-europeo-privacidad_11_874180003. html). 19/10/2015.

[72] Es interesante la COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO: Los flujos transatlánticos de datos: recuperar la confianza instaurando estrictas salvaguardias, Bruselas, 29.2.2016 (http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016DC0117).

[73] López Lapuente, L: «Las transferencias de datos a EE. UU.: la transición del Safe Harbor al Privacy Shield» y un paso más allá», *Actualidad Jurídica Uría Menéndez*, 45/2017, pp. 36-38.

[74] Que constituirá uno de los eslabones de nuestra actual línea de investigación centrada en la Privacidad y la Seguridad.

correspondientes a cada empresario, es admisible «la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales». De modo que es posible el acceso por la empresa a unos ficheros informáticos en los que quedan registradas las conversaciones electrónicas mantenidas por dos trabajadoras a través de un programa de mensajería, que habían instalado en un ordenador de uso común a todos los trabajadores, y que no tenía clave de acceso. Fundamentalmente, porque la instalación del programa se había producido vulnerando la prohibición de la entidad de instalar programas en el ordenador. Ante esta prohibición y ante la utilización de canales, no privados, sino corporativos no cerrados, no cabe en palabras del Tribunal «una expectativa razonable de confidencialidad derivada de la utilización del programa instalado». El TC determina, así, que el contenido de los mensajes no estaba sometido al «secreto de las comunicaciones», dado que se almacenaban automáticamente en el disco duro del ordenador, que era de uso común y al que todos los trabajadores accedían sin clave. En definitiva, no era un canal cerrado de comunicación y no había expectativa de privacidad.

Por otro, la Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre[75], ratifica que el artículo 18.3 CE protege únicamente ciertas comunicaciones: las que se realizan a través de determinados medios o canales cerrados; por lo que, no gozarán de la protección constitucional de éste las comunicaciones abiertas realizadas por un canal del que no puede predicarse la confidencialidad. La remisión de correos electrónicos a través de un canal de comunicación abierto queda fuera de la protección constitucional al secreto de las comunicaciones, permitiendo la inspección por parte del empresario.

En todo caso, la actuación de verificación empresarial no puede entenderse de forma excesivamente amplia, sino que ha de estar sujeta a un juicio de proporcionalidad; entendiendo que éste ha de consistir en una justificación de la medida de la intervención, fundándose en la existencia de sospechas de un comportamiento irregular del trabajador. Además, esta intervención ha de ser idónea para la finalidad pretendida por la empresa, consistente en verificar si el trabajador cometía efectivamente la irregularidad sospechada; la medida ha de considerarse necesaria, dado que, como instrumento de transmisión de dicha infor-

[75] En este caso el Convenio colectivo aplicable al trabajador, tipificaba como falta leve la «utilización de los medios informáticos propiedad de la empresa para fines distintos de los relaciones con el contenido de la prestación laboral». La expresa prohibición convencional del uso extralaboral del correo electrónico, y su limitación a fines profesionales, llevaba implícita la facultad de la empresa de controlar su utilización.

mación confidencial, el contenido o texto de los correos electrónicos serviría de prueba de la citada irregularidad ante la eventual impugnación judicial de la sanción empresarial. Finalmente, la medida ha de ser ponderada y equilibrada.

Es necesario resaltar que estas exigencias en el marco laboral pueden verse condicionadas por la interpretación del TEDH en la reciente Sentencia (Gran Sala) dictada en el Caso *Barbulescu contra Rumania*, el día 5 septiembre 2017[76]. En ella sienta novedosamente que:

- La información al trabajador de que sus comunicaciones puedan ser controladas ha de ser con carácter previo. El Tribunal entiende que para ser considerada como previa, la advertencia del empleador debe darse antes de que comience la actividad de supervisión.
- Ha de informarse de la naturaleza y alcance de la vigilancia, así como del grado de intrusión en su vida privada y en su correspondencia.

[76] La empresa tenía un código de conducta interno en el que constaba que quedaba terminantemente prohibido usar las ordenadores, fotocopiadoras, teléfonos, télex y fax para fines personales. El Sr. Barbalescu fue despedido por trasgredir dicho Código pues se le imputaba haber mantenido conversaciones con su familia y pareja sentimental a través de la aplicación *Yahoo Messenger* durante la jornada de trabajo. el Tribunal considera que las autoridades nacionales no protegieron adecuadamente el derecho del demandante respeto de su vida privada y su correspondencia y que, por lo tanto, no valoraron el justo equilibrio entre los intereses en juego. En consecuencia, se había producido una violación del artículo 8 del CEDH. Pues el demandante no había recibido una advertencia previa por parte de su empresa. No parecía que el demandante hubiera sido informado con antelación del alcance y de la naturaleza del control efectuado por la empresa o de la posibilidad de que la empresa tuviera acceso al contenido de sus comunicaciones.

En síntesis las exigencias del TEDH se concretan en: a) la advertencia de que los correos pueden ser supervisados debe ser, en principio, clara en cuanto a la naturaleza de la supervisión y antes del establecimiento de la misma. b) en relación con el alcance de la supervisión debe hacerse una distinción entre el control del flujo de comunicaciones y el de su contenido. También se debería tener en cuenta si la supervisión de las comunicaciones se ha realizado sobre la totalidad o solo una parte de ellas y si ha sido o no limitado en el tiempo y el número de personas que han tenido acceso a sus resultados (véase, en este sentido, la sentencia Köpke, precitada). Lo mismo se aplica a los límites espaciales de la vigilancia. c) Dado que la vigilancia del contenido de las comunicaciones es por su naturaleza un método mucho más invasivo, requiere justificaciones más fundamentadas. d) es necesario evaluar, en función de las circunstancias particulares de cada caso, si el objetivo perseguido por el empresario puede alcanzarse sin que éste tenga pleno y directo acceso al contenido de las comunicaciones del empleado. e) proporcionalidad en los resultados. f) las garantías ofrecidas al trabajador debían impedir que el empleador tuviera acceso al contenido de las comunicaciones en cuestión sin que el empleado hubiera sido previamente notificado de tal eventualidad. g) las autoridades internas deben velar para que los empleados, cuyas comunicaciones hayan sido objeto de seguimiento, puedan presentar un recurso ante un órgano judicial que tenga competencia para pronunciarse, al menos en esencia, sobre el cumplimiento de los criterios antes expuestos y la legalidad de las medidas impugnadas.

• Debe determinar los motivos concretos que justifica la introducción de las medidas de control.

• Ha de determinar si el empresario puede optar por utilizar medidas menos intrusivas para la vida privada y la correspondencia del trabajador.

Y, pese a que la doctrina del Tribunal Constitucional, como hemos visto, sujeta las facultades de control del empresario a unas exigencias, sin embargo, no figura entre ellas la determinación de los motivos concretos que justifican la intervención, así como el alcance de dicha vigilancia. En consecuencia, y en virtud del carácter vinculante de la doctrina del TEDH, estas exigencias deberán incorporarse a nuestro ordenamiento interno[77].

Finalmente, en el marco de la actividad privada no pueden desdeñarse las facultades que la Ley de Seguridad Privada[78], permite a los detectives privados, sobre todo en este orden laboral.

IV. LA CONSTRUCCIÓN JURISPRUDENCIAL DE LAS EXIGENCIAS PARA LA INTERVENCIÓN DE LAS COMUNICACIONES

El artículo 18.3 CE contempla expresamente la exigencia de resolución judicial para la intervención de las comunicaciones, sin más matización. No rodea, pues, a dicha resolución de ninguna exigencia, y tampoco especifica la exigencia de habilitación legal previa; máxime cuando ésta es inexcusable en orden a la limitación de un derecho fundamental.

1. Insuficiencia de la norma y fijación jurisprudencial de los requisitos de intervención

Cuando entró en vigor este precepto constitucional, la LECrim, que era la ley (ordinaria) que regulaba la intervención de las comunicaciones[79], no se aco-

[77] Así como advierte Preciado Domènech, C. H. «Nos hallamos ante una de esas resoluciones que marcará época y que supondrá, entre otras cosas, la necesidad de revisar la reciente doctrina del Tribunal Constitucional(TC), en concreto la STC 241/2012, de 17 de diciembre y la STC 170/2013, de 7 de octubre», «Comentario de urgencia a la STEDH de 5 de septiembre de 2017Caso Barbulescu contra Rumanía (Gran Sala) Recuperando la dignidad en el trabajo», *Thomson Reuters*.

[78] Ridaura Martínez, M.ª J.: *Seguridad Privada y derechos fundamentales*, Tirant lo Blanch, Valencia, 2015.

[79] Artículos 579, 581, 583, 586, y 588 de Ley de Enjuiciamiento Criminal relativas a la entrada y registro en lugar cerrado, al examen de libros y papeles y a la detención y apertura de la correspondencia escrita y telegráfica.

modó para cumplir con las exigencias de respeto al derecho fundamental al secreto de las comunicaciones; ello provocó que esta normativa fuese objeto de diversos pronunciamientos judiciales, especialmente del Tribunal Europeo de Derechos Humanos. En efecto, ya la Sentencia *Valenzuela contra el Reino de España*, de 30 de julio de 1998 el TEDH declaró que el derecho español vigente en 1985 no indicaba con suficiente claridad la extensión y modalidades de la injerencia de la autoridad pública en el derecho al respeto de la vida privada y a la correspondencia, vulnerando con ello el artículo 8 del Convenio Europeo de Derechos Humanos. La declaración de dicha vulneración la sustenta el TEDH en la doctrina que sobre este derecho había venido fijando en diversas Sentencias:

i. La interceptación de las conversaciones telefónicas constituye una injerencia de una autoridad pública en el derecho al respeto a la vida privada y a la correspondencia, que vulnera el artículo 8.2 salvo que esté «prevista por la ley», persiga uno o varios fines legítimos, y sea «necesaria, en una sociedad democrática» para alcanzarlos[80].

ii. Las palabras «prevista por la ley» buscan: a) que la medida incriminada tenga una base en el derecho interno; b) también concierne a la calidad de la «ley», exigiendo que sea compatible con la preeminencia del derecho, implicando así que el derecho interno debe ofrecer una cierta protección contra atentados arbitrarios de los poderes públicos (sentencia Malone).

De esta exigencia deriva la necesidad de la accesibilidad de la ley para la persona implicada, que debe poder prever además las consecuencias para ella[81].

iii. El peligro de arbitrariedad aparece con singular nitidez allí donde un poder de apreciación se ejerce en secreto. Por tanto, el derecho interno debe emplear términos suficientemente claros para indicar a todos de manera suficiente en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a tomar tales medidas[82].

iv. Como garantías mínimas, necesarias para evitar los abusos, que deben figurar en la ley, las Sentencias *Kruslin y Huvig*, indican:

— «la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial;
— la naturaleza de las infracciones a que puedan dar lugar;
— la fijación de un límite a la duración de la ejecución de la medida;

[80] Todas ellas citadas en la Sentencia Valenzuela Contreras, cuya cita, no reproducimos textualmente seguimos (Sentencia Kopp contra Suiza, de 25 marzo 1998).

[81] Malone p. 32, ap. 67; y Sentencias Kruslin, p. 20, ap. 27, y Kopp.

[82] Sentencias Malone, pp. 31-32, ap. 66, 67, Kruslin, pp.. 22-23, ap. 30, Halford, p. 1017, ap. 49 y Kopp.

— las condiciones de establecimiento de los atestados que consignen las conversaciones interceptadas;

— las precauciones que se deben tomar para comunicar, intactas y completas, las grabaciones realizadas, con el fin de ser controladas eventualmente por el Juez y la defensa;

— las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de dichas cintas, sobre todo tras un sobreseimiento o una absolución[83]».

Conviene precisar que el TEDH está situando la calidad de la ley como piedra angular para la salvaguarda del secreto de las comunicaciones, ya que construye las anteriores exigencias tomando como referencia el artículo 8.2 del CEDH, que exige que toda injerencia de la autoridad pública en el ejercicio de este derecho ha de estar 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*».

Puede advertirse de su lectura que todas las exigencias sentadas en las Sentencias referidas son materiales, y están dirigidas a determinar cómo las ha de prever la ley para que tenga la calidad suficiente que permita su intervención. Y es que el CEDH está configurando una fórmula que se articula básicamente «en torno a los principios de legalidad y necesidad, dejando en cambio indeterminada la «autoridad pública» que puede adoptar la medida de intervención de las comunicaciones»[84]. Por tanto, la previsión legal, que además ha de ser de calidad, aparece en la jurisprudencia de Estrasburgo como inexcusable para la limitación del derecho fundamental, en este caso, al secreto de las comunicaciones.

Sin embargo, es cierto que el artículo 18.3 de la CE al exigir la resolución judicial para la intervención de las comunicaciones había permitido que las escuchas telefónicas no se practicaran con absoluta carencia de exigencias, ya dicha intervención generó que, pese a la insuficiencia de la LECrim, tanto desde la jurisdicción ordinaria como de la constitucional, se aprovechara la aplicación concreta para introducir las garantías exigidas por el Convenio Europeo de Derechos Humanos; lo reconoció el TEDH en la Sentencia *Valenzuela Contrera*s, resaltando, en particular, el Auto del Tribunal Supremo de 18

[83] Cit., p. 24, ap. 35, y pp. 56, ap. 34 respectivamente.

[84] *Vid.* el Voto Particular formulado por Pedro Cruz Villalón en la STC 49/1999.

de junio de 1992 —caso Naseiro[85]. Pero, como se indicaba desde Estrasburgo, el problema se planteaba más por la formulación legal que por la aplicación judicial de la misma. Lo que abocó al TEDH a reconocer que la norma española que habilitaba la intervención de las comunicaciones *no tenía calidad suficiente*[86]; ya que debía indicar de manera suficiente clara en qué circunstancias o en qué condiciones se habilita el poder público para intervenir las comunicaciones.

El artículo 579 LECrim[87] fue reformado por la LO 4/1988, 25 mayo, de reforma de la Ley de Enjuiciamiento Criminal, precisando las modalidades de control de la intervención de las conversaciones telefónicas. Según este artículo, únicamente podía realizarse la vigilancia de las comunicaciones telefónicas por resolución motivada del Juez, cuando existieran indicios que hicieran pensar que se podía obtener por este medio el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. Estas mismas garantías debían rodear las resoluciones de prórroga de esta medida de vigilancia; ordenando que las transcripciones de las conversaciones grabadas tuvieran lugar bajo el control del Secretario Judicial.

Esta reforma legal se consideró insuficiente y acarreó nuevas condenas a España; así en la Sentencia *Prado Bugallo contra España*, de 18 de febrero de 2003, el TEDH volvió a declarar la vulneración del artículo 8 del CEDH, ya que artículo 579 LECrim no cumplía con las exigencias requeridas por dicho precepto relativas a la previsión legal de la injerencia condiciones exigidas por la juris-

---

[85] Un estudio mucho más detallado del tema puede verse Martín-Retortillo Baquer, L: «La calidad de la ley Jurisprudencia del Tribunal Europeo de Derechos Humanos (especial referencia a los casos «Valenzuela Contreras» y «Prado Bugallo», ambos contra España)», *Derecho Privado y Constitución*, núm.17/2003, especialmente las pp. 392 y ss.

[86] Cruz Villalón, P: «Control de la calidad de la ley y calidad del control de la ley», *Derecho Privado y Constitución*, núm.17/2003, p. 149: «Calidad de la ley» es una expresión que recibe hoy su sentido más específico entre nosotros a través de una jurisprudencia del TEDH que viene exigiendo condiciones estrictas de previsibilidad al legislador de los derechos fundamentales, en particular, al legislador de algunas medidas particularmente rigurosas puestas a disposición de los poderes públicos, cuales son la prisión provisional y la intervención de la correspondencia, en términos que han venido siendo todo menos irrelevantes para nosotros.

[87] López-Barja de Quiroga, J.: *Las escuchas telefónicas y la prueba ilegalmente obtenida*, Ed. Akal, 1989, p. 182, al advertir respecto de la actual regulación del artículo 579 LECrim que: «Llama poderosamente la atención la escasez normativa. Por primera vez se regula en nuestro país el tema de las intervenciones telefónicas, del que no resulta ocioso repetir que se trata de la limitación de un derecho fundamental, y nos encontramos únicamente con dos apartados, lacónicos y a todas luces insuficientes».

prudencia del Tribunal[88] para evitar abusos. Asimismo se consideraba insuficiente la regulación de naturaleza de las infracciones que podían dar lugar a las escuchas, con la fijación de un límite a la duración de la ejecución de la medida, y con las condiciones de establecimiento de las actas de síntesis que consignan las conversaciones intervenidas, ya que las consideraba como de competencia exclusiva del Secretario Judicial. Las insuficiencias se referían, igualmente, a las precauciones para comunicar intactas y completas las grabaciones realizadas, para su control eventual por el Juez y por la defensa, ya que la Ley no contenía ninguna disposición al respecto.

2. LA PERSISTENCIA EN NO LEGISLAR

La persistencia del legislador español[89] en no reformar la legislación siguió abocando a la jurisdicción ordinaria y a la constitucional a colmar las lagunas legislativas, enjuiciando los casos siguiendo las exigencias del Tribunal Europeo de Derechos Humanos[90]. Son máximo exponente para la fijación los requisitos de adecuación de las intervenciones telefónicas al derecho al secreto de las comunicaciones el mencionado Auto de 18 de junio de 1992, así como la unificación y consolidación de la jurisprudencia constitucional a partir de 1998 plasmada, sobre todo, en la STC 49/1999, de 5 de abril, de 5 de abril, que aclaraban como exigencias relativas al contenido de la ley. Adviértase hasta qué punto se ajusta a la doctrina del Tribunal Europeo:

> «la definición de las categorías de personas susceptibles de ser sometidas a escucha judicial; la naturaleza de las infracciones susceptibles de poder dar lugar a ella; la fijación de un límite a la duración de la ejecución de la medida; el proce-

[88] «El artículo 579 de la Ley Orgánica de Enjuiciamiento Criminal, redactado según la Ley Orgánica 4/1988, de 25 de mayo de 1988, no ofrece una reglamentación exhaustiva, sino que se limita a determinar: a) la forma que debe adoptar la resolución de intervenir las líneas (motivada, artículo 248.2 de la Ley Orgánica del Poder Judicial b) el plazo y los motivos de la prórroga (hasta tres meses prorrogables por períodos iguales); el objetivo de la medida (conseguir por esos medios descubrir o verificar un hecho o una circunstancia importante para el asunto); y d) los casos en los que la medida es admitida, a saber la existencia de una persona sometida a investigación o con respecto a la que existen indicios de responsabilidad criminal».

[89] El título que Catala i Bas, Alexandre, H., da a uno de sus trabajos en este tema es revelador «Escuchas telefónicas: un encuentro con el Tribunal Constitucional y un desencuentro con el legislador español», en *Revista Europea de Derechos Fundamentales*, núm. 15/2010, pp. 279-294.

[90] *Vid.* con posterioridad SSTC 202/2001, 49/1999; SSTS 610/2007, 513/2010. STC 123/2002, de 20 de mayo; SSTC 184/2003, de 23 de octubre; ATC 11/2007, de 15 de enero; STC 26/2006.

> dimiento de transcripción de las conversaciones interceptadas; las precauciones a observar, para comunicar, intactas y completas, las grabaciones realizadas a los fines de control eventual por el Juez y por la defensa; las circunstancias en las cuales puede o debe procederse a borrar o destruir las cintas, especialmente en caso de sobreseimiento o puesta en libertad.»

El TC resalta las carencias de la ley española, pero destaca también que la incorporación por los jueces ordinarios de los criterios derivados del artículo 8 del Convenio, tal y como había sido interpretado por el Tribunal Europeo de Derechos Humanos, resultaría respetuosa con derecho al secreto de las comunicaciones; aunque persistiesen las carencias de la ley.

Aunque, como advierte Javier Matía Portilla, algunos de los avances dados en esta nueva jurisprudencia no pueden calificarse de sorprendentes, porque ya se habían adelantado en otras resoluciones[91]; y considera que, aunque el Tribunal Constitucional asume la doctrina Valenzuela Contreras, no extrae de la misma todas sus consecuencias, ya que, cerrándose la argumentación del TEDH en el punto de la falta de calidad de la ley, pese a las garantías que el órgano judicial trató de establecer que derivaban de la doctrina del TEDH, no era necesario examinar más cuestiones. Sin embargo, el TC aún reconociendo la inadecuación del artículo 579 LeCrim, separa la vulneración provocada por la ley de la actuación de los órganos jurisdiccionales que autorizaron la intervención[92].

---

[91] Matia Portilla, F. J.: «Legislador, derechos fundamentales y proceso», *Revista Española de Derecho Constitucional*, núm. 58/2000. Por ejemplo, que el control que la Constitución exige para limitar el secreto de las comunicaciones no se colma con la mera existencia de un auto judicial, aunque en él la decisión judicial se encuentre convenientemente fundamentada la decisión del órgano judicial; o la exigencia de que la ejecución de la diligencia se vea rodeada de cautelas y garantías para asegurar que la intromisión en el derecho fundamental afectado sea proporcionada, pp. 249, y 264-265.

[92] De hecho, Cruz Villalón sostiene en el Voto Particular que formula a la Sentencia que entiende que la vulneración «la produce ya la sola deficiencia de ley, sin que sea necesario, para confirmar dicha vulneración, el examen y valoración que se hace en la Sentencia de la actuación judicial». «Desde luego, no es ese el modo de operar del TEDH en los casos Huvinúg, Kruslin y Valenzuela, donde la sola constatación de estas carencias lleva a apreciar una transgresión del artículo 8 CEDH. Por lo que hace a nuestro ordenamiento constitucional, no creo que podamos decir que se ha vulnerado el derecho fundamental por la deficiencia de la ley y, sin embargo, afirmar que la lesión puede ser contrarrestada por el juez, pues las carencias de previsibilidad no son susceptibles de una subsanación ex post facto. La doctrina de los casos Huvig y Kruslin es que, mientras no se cubran las deficiencias de la ley, el TEDH seguirá apreciando vulneraciones del derecho fundamental (cosa distinta, pero no irrelevante, es que la reparación de esta vulneración, como en el caso Valenzuela, se considerase satisfecha con la sola declaración de la misma).

3. LA INSUFICIENCIA DEL PRECEPTO, NO POR LO QUE DICE, SINO POR LO QUE DEJA DE DECIR

Colmar lagunas e insuficiencias legales a golpe de Sentencias ha permitido seguir residenciando en sede constitucional la lesión del derecho al secreto de las comunicaciones ocasionada por la falta de habilitación legal suficiente desde la perspectiva de la «calidad de la ley» necesaria para salvaguardar la previsibilidad de la medida restrictiva del derecho fundamental, dado que el artículo 579 de la no cumple los requisitos exigidos de forma reiterada por el Tribunal Europeo de Derechos Humanos.

De la copiosa jurisprudencia destacamos la STC 184/2003[93], ya que, pese a resolver una demanda de amparo, en ella se solicita que se plantee la cuestión de la inconstitucionalidad, reconociendo la Sala de lo Penal del Tribunal Supremo que el artículo 579 LECrim resulta insuficiente «por el considerable número de espacios en blanco que contiene en materias tales como los supuestos que justifican la intervención, el objeto y procedimiento de ejecución de la medida, así como de la transcripción en acta del contenido de los soportes magnéticos, la custodia y destrucción de las cintas, etc.».

Esta situación, calificada por la Sala, de práctica «anomia» legislativa se entiende suficientemente colmada por la doctrina jurisprudencial, que han interpretado el artículo 18.3 CE, de conformidad con el artículo 8 del Convenio y de su órgano de aplicación que es el Tribunal Europeo de Derechos Humanos. Considerando que «Este cuerpo de doctrina elaborado de esta manera en numerosísimos precedentes jurisprudenciales, debe considerarse... como complemento del Ordenamiento jurídico».

El Tribunal Constitucional, aún volviendo a reconocer que el artículo 579 LECrim adolece de vaguedad e indeterminación en aspectos esenciales, por lo que no satisface los requisitos necesarios exigidos por el artículo 18.3 CE para la protección del derecho al secreto de las comunicaciones, sin embargo, desestima la petición del planteamiento de la autocuestión de inconstitucionalidad entendiendo que «este mecanismo está previsto para actuar sobre disposiciones legales que en su contenido contradicen la Constitución, pero no respecto de las que se avienen con aquélla y cuya inconstitucionalidad deriva no de su enunciado, sino de lo que en éste se silencia».

En consecuencia, entiende «inútil» su planteamiento, «en la medida en que la reparación de la eventual inconstitucionalidad solo podría alcanzarse suplien-

[93] García Couso, S.: «Comentario a la Sentencia del Tribunal 184/2003, de 23 de octubre», en *Revista Española de Derechos Fundamentales*, núm. 2/2003, pp. 131-144.

do las insuficiencias de las que trae causa y no mediante la declaración de inconstitucionalidad y, en su caso, nulidad de un precepto que no es contrario a la Constitución por lo que dice, sino por lo que deja de decir».

El resultado de dicha «anomia legislativa» es la sucesión de condenas, ya que en 2006 el TEDH vuelve a condenar a España en el caso *Abdulkadir Coban* c. *España,* de 26 de septiembre de 2006, y aunque sigue reconociendo la labor jurisprudencial para incorporar la doctrina del TEDH*,* resaltando que su incorporación a través del cuerpo jurisprudencial viene a colmar las exigencias del CEDH[94], ya que en ella se establece reglas claras y detalladas que «precisan a priori con suficiente claridad la extensión y las modalidades de ejercicio del poder de apreciación de las autoridades en el ámbito objeto de consideración». Pese a ello, vuelve a reconocer la necesidad de reformar el artículo 579 LeCrim.

4. LA EXIGENCIA DE MOTIVACIÓN DE LA INTERVENCIÓN COMO INTEGRANTE DEL CONTENIDO ESENCIAL DEL DERECHO

La exigencia de motivación de las resoluciones judiciales que autorizan la intervención (o su prórrogas) forman parte del contenido esencial del artículo 18.3 CE; por tanto, estamos ante una exclusividad jurisdiccional de tal autorización, pero sujeta a una serie de exigencias.

Es cierto que, como ha recordado el TS, las exigencias establecidas en nuestro ordenamiento para las intervenciones telefónicas son de las más estrictas que existen en el ámbito del derecho comparado, pues en algunos ordenamientos no se exige autorización judicial, siendo suficiente la intervención de una autoridad gubernativa; en otros, aún exigiendo autorización judicial, generalmente ordenamientos de corte anglosajón, no se imponen al Juez las exigencias de motivación establecidas por nuestra jurisprudencia (STS núm. 635/2012, 17 de julio). Sin embargo, puesto que en nuestro ordenamiento la resolución judicial motivada de autorización de intervención forma parte del contenido esencial del secreto de las comunicaciones, la obsolescencia de la norma española en este tema ha abocado a que haya sido la doctrina del Tribunal Supremo y del Constitucional la que, como hemos visto, también a la luz de la doctrina del TEDH, haya ido colmando sus exigencias.

[94] Un estudio más detallado puede verse en Cano Palomares, G.: «El diálogo entre tribunales y el derecho al secreto de las comunicaciones telefónicas (a propósito de la decisión *Coban* C. España del Tribunal Europeo de Derechos Humanos de 25 de septiembre de 2006) «, *Revista Española de Derecho Europeo* núm. 24/2007.

(i) La resolución judicial que autorice la intervención debe contener, bien en su propio texto o en la solicitud policial a la que se remita[95]:

> «1. Con carácter genérico los elementos indispensables para realizar el juicio de proporcionalidad. 2. Los datos objetivos que puedan considerarse indicios de la posible comisión de un hecho delictivo grave, que deben ser accesibles a terceros. 3. Los datos objetivos que puedan considerarse indicios de la posible conexión de las personas afectadas por la intervención con los hechos investigados, que no pueden consistir exclusivamente en valoraciones acerca de la persona. 4. Los datos concretos de la actuación delictiva que permitan descartar que se trata de una investigación meramente prospectiva. 5. La fuente de conocimiento del presunto delito, siendo insuficiente la mera afirmación de que la propia policía solicitante ha realizado una investigación previa, sin especificar mínimamente cual ha sido su contenido, ni cuál ha sido su resultado. 6. El número o números de teléfono que deben ser intervenidos, el tiempo de duración de la intervención, quién ha de llevarla a cabo y los períodos en los que deba darse cuenta al Juez de sus resultados a los efectos de que éste controle su ejecución» (STS núm. 635/2012, de 17 de julio).

En definitiva, es esencial para excluir la vulneración constitucional que la intervención sea acordada judicialmente en una resolución que explicite los elementos indispensables para realizar el juicio de proporcionalidad, con el objeto de permitir su control posterior[96].

(ii) Las carencias de la ley permitieron que la intervención, en ocasiones, se autorizara mediante las denominadas «Diligencias indeterminadas», y no por diligencias previas. La principal consecuencia es que las primeras no constituyen un proceso legalmente existente, y no se notifican necesariamente al Ministerio Fiscal, de ahí que muchas resoluciones se hayan considerado contrarias a las exigencias de la resolución judicial de autorización[97], ya que en ellas el secreto no afecta solo al afectado por la intervención, sino también que tampoco las conoce el Ministerio Fiscal.

De hecho, la Sala Segunda del Tribunal Supremo ha venido remarcando, «que lo ortodoxo es dictar el auto habilitante de la intervención en diligencias previas, al no estar previstas específicamente en nuestra Legislación las llamadas

[95] STS núm. 635/2012, de 17 de julio, 912/2016, de 1 de diciembre.

[96] La Sala Segunda del Tribunal Supremo ha seguido ratificando la nulidad de la prueba cuando dicho auto se halla motivado por remisión a un oficio policial que solo contiene sospechas que no sirven para deducir de modo indiciariamente racional una actividad delictiva (STS, Sala Segunda 106/2017, de 21 de febrero).

[97] Se discierne claramente este tema en la Sentencia del Tribunal Supremo 1789/2013, de 18 de abril.

indeterminadas, y que, por ello, estas diligencias no constituyen un proceso legal hábil para adoptar una medida de esta naturaleza»[98].

También el Tribunal Constitucional desde la Sentencia 49/1999, de 5 de abril, ha señalado que la garantía jurisdiccional del secreto de las comunicaciones no se colma con la concurrencia formal de una autorización procedente de un órgano jurisdiccional, «sino que ésta ha de ser dictada en un proceso, único cauce que permite hacer controlable, y con ello jurídicamente eficaz, la propia actuación judicial[99]. No es, pues, suficiente la existencia de una investigación previa, sino que el proceso es el «único cauce que permite hacer controlable, y con ello jurídicamente eficaz, la propia actuación judicial».

(iii) Una consecuencia ineludible de que las exigencias de motivación de las resoluciones judiciales que autorizan la intervención o su prórroga formen parte del contenido esencial del artículo 18.3 CE, es que su conculcación supone la vulneración del derecho y la invalidación, en su caso, de las pruebas obtenidas[100]. En efecto, la ilicitud de las pruebas de intervenciones telefónicas por vulneración del artículo 18.3 conlleva la nulidad de todo lo actuado en aplicación de lo dispuesto en el artículo 11 LOPJ (teoría de los frutos del árbol envenenado). La ilicitud de la prueba constituye un **fracaso del sistema de justicia penal**[101]; ya que si bien puede entenderse que es señal de que funcionan los mecanismos de blindaje de los derechos fundamentales; no deja de ser un fracaso por cuanto significa el reconocimiento de que se ha vulnerado un derecho fundamental y de que probablemente

En atención a las fuentes externas de conocimiento, esto es, las informaciones proporcionadas por servicios extranjeros, en el marco de la cooperación penal internacional, el Tribunal Supremo ha entendido que no pueden imponerse las reglas propias, debiendo respetarse el ordenamiento de cada país,

[98] STS núm. 273/1997, de 24 de febrero, entre otras.

[99] Aunque el Tribunal Constitucional lo que ha considerado contrario a las exigencias del artículo 18.3 CE no es la mera inexistencia de un acto de notificación formal al Ministerio Fiscal de la intervención telefónica, sino el hecho de que la misma, al no ser puesta en conocimiento del Fiscal, pueda acordarse y mantenerse en un secreto constitucionalmente inaceptable, en la medida en que no se adopta en el seno de un auténtico proceso que permite el control de su desarrollo y cese (STC 197/2009, de 28 de septiembre. Y el Tribunal Supremo viene sosteniendo que la falta de notificación al Ministerio Fiscal, solo constituiría, en su caso, una irregularidad procesal, sin trascendencia alguna respecto al derecho al secreto de las comunicaciones telefónicas del artículo 18.3).

[100] STC, entre muchas otras, 54/1996, de 26 de marzo, 26/2010, de 27 de abril.

[101] Por ese mal funcionamiento no ha podido culminar el proceso con una resolución ajustada a la realidad material. STS, Sala Segunda 106/2017, de 21 de febrero.

siempre y cuando éstos respeten las reglas mínimas del Tratado de Roma o el de Nueva York[102].

V. LA EXIGIDA REFORMA DE LA LEY DE ENJUICIAMIENTO CRIMINAL

Las constantes exigencias de modificación de la legislación se han concretado en la aprobación de la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (en adelante LOMLE-Crim). Así se había manifestado el Tribunal Supremo advirtiendo que en este tema se requería «imperativamente y sin más demoras una regulación completamente renovada, en una nueva Ley procesal penal que supere la obsolescencia de nuestra legislación decimonónica[103].

Es pues una ley orgánica la que regula en qué circunstancias o en qué condiciones se habilita el poder público para intervenir las comunicaciones. La nueva ordenación pretende colmar un vacío legislativo tan prolongado en el tiempo, que había generado gran inseguridad jurídica, así como una quiebra de las garantías procesales. Una reforma que como se ha señalado debía atender al mismo tiempo, «por un lado, la protección de los derechos afectados, con la necesarias garantías judiciales de salvaguardia de los mismos, y, por otro lado, la necesidad de facilitar a los investigadores las herramientas eficaces para el mejor desarrollo posible de su trabajo, tan importante en la lucha contra muchas de la formas actuales de criminalidad»[104].

A continuación destacaremos algunos de los aspectos más relevantes de esta nueva ordenación:

1. Detención y apertura de la correspondencia escrita y telegráfica[105], que alcanza la postal y telegráfica, incluidos faxes, burofaxes y giros. Así, el nuevo artículo 579, en orden a la naturaleza de las infracciones susceptibles de poder dar lugar a ella, acota el ámbito material de aplicación, de modo que la intervención solo podrá acordarse en el marco de una serie de delitos: 1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de pri-

[102] STS 146/2016, de 25 de enero.

[103] STS 912/2016, de 1 de diciembre.

[104] Jaén Vallejo, M. y Perrino Pérez, A. L.: *La reforma procesal penal de 2015*, Dykinson, Madrid, 2015, p. 146.

[105] Capítulo III, artículos 578 a 588, modificándose el artículo 579 y añadiéndose un nuevo 579 bis.

sión; 2.º Delitos cometidos en el seno de un grupo u organización criminal; 3.º Delitos de terrorismo. Constituyendo éste uno de los temas más exigidos.

Respecto de la fijación de un límite a la duración de naturaleza de las infracciones susceptibles de poder dar lugar a ella, regula los plazos máximos de duración de hasta tres meses, prorrogable por iguales o inferiores períodos hasta un máximo de dieciocho meses

Aunque prevé una serie de casos particulares: en caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas, la intervención 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.

Asimismo, contempla las excepciones a la necesidad de autorización judicial, en los mismos términos que se había previsto jurisprudencialmente: a) Envíos postales[106] 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.

Además, se crea un nuevo artículo 579 bis, que permite que el resultado de la detención y apertura de la correspondencia escrita y telegráfica pueda ser utilizado como medio de investigación o prueba en otro proceso penal; estableciendo las condiciones para ello, en particular en cuanto al tratamiento de los denominados «hallazgos casuales» (art. 588 bis i) y a la continuación de la medida, en aquel otro proceso, para lo que se requerirá un nuevo auto judicial que convalide esta situación.

[106] Se incorpora, así, la reiterada doctrina, entre otras SSTS 103/2002, de 18 de enero; 404/2004, de 30 de marzo; 185/2007, de 20 de febrero; 115/2015, de 5 de marzo.

2. La LOMLECrim establece una serie de disposiciones comunes[107] para las denominadas medidas de investigación tecnológica que inciden, no solo sobre el derecho al secreto de las comunicaciones, sino también a otros derechos contemplados en el artículo 18 de la Constitución. Las Disposiciones que afectan al artículo 18.3 son las relativas a la interceptación de las comunicaciones telefónicas y telemáticas[108], pero también, las que atañen al registro de dispositivos de almacenamiento masivo de información y a los registros remotos sobre equipos informáticos. Mientras que la captación y la grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes afectan, en unos casos al derecho a la intimidad (18.1), y en otros también al protección de datos (18.4).

En primer lugar, establece para todas ellas unos principios comunes, que suponen la consagración en la Ley de los principios que había venido sentado el TEDH y que se habían por la doctrina tanto del Tribunal Constitucional como del Tribunal Supremo: exigencia de autorización judicial dictada con plena sujeción a los principios de especialidad[109]; y sujeta a los principios de idoneidad, excepcionalidad, necesidad, y proporcionalidad de la medida: fijando, asimismo, los criterios para determinar dicha proporcionalidad: que sean tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros.

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

[107] Capítulo IV, de disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemática, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y el registro remoto de equipos informáticos (arts. 588 bis a) hasta 588 bis k).

[108] Cavero Forradellas, G.: «La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal», destaca también la determinación de que sea el Secretario de Estado de Seguridad el sucede al Director de Seguridad del Estado, como facultado para disponer una intervención telefónica gubernativa excepcional e imprescindible. La categoría de las empresas operadoras y demás sujetos colaboradores obligados para la práctica de las intervenciones telefónicas.

[109] Pues como ya el TC había manifestado «no se trata de satisfacer los intereses de una investigación meramente prospectiva, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan de los encargados de la investigación, por más legítima que sea esta aspiración, pues de otro modo se desvanecería la garantía constitucional (SSTC 49/1999, de 5 de abril, 167/2002, de 18 de septiembre; 184/2003, de 23 de octubre.

de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho (art. 588 bis a) apartado 5) [110].

En segundo lugar, la LOMLECrim contempla una serie de exigencias comunes a todas ella. Así, con el objeto de evitar el problema que ha venido planteándose en relación con las solicitudes policiales de intervención, así como de las resoluciones no argumentadas debidamente y, por tanto, indebidamente motivadas, se detallan una serie de exigencias, pues su adopción podrá acordarla el juez de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial. Por un lado, establece las exigencias de la solicitud de la policía judicial o el Ministerio Fiscal de autorización judicial /[588 bis.b)]. Y, por otro, las exigencias que ha de satisfacer la resolución judicial que autorice la medida: el hecho punible objeto de investigación y su calificación jurídica, los indicios racionales en que se fundamenta la medida; la identidad de los investigados y de cualquier otro afectado por la medida; la extensión de la mediada de injerencia, especificando su alcance y motivando el cumplimiento de los principios rectores; la unidad investigadora de la Policía Judicial encargada de la intervención; la duración de la medida; la forma y periodicidad en la que el solicitante ha de informar al juez; la finalidad perseguida; el sujeto obligado que llevará a cabo la medida (588 bis.c).

Aparecen, pues, reguladas las medidas en que se enmarcaba el sistema de intervención SITEL; así, como advierte Rodríguez Laínz, este principio de proporcionalidad, anticipado por la jurisprudencia del Tribunal Supremo, encuentra también su reflejo en otros preceptos como el artículo 588 bis.2.4 relativo a la exigencia de la mención en la solicitud de la extensión de la medida con especificación de su contenido; así como en el artículo 588 bis c.3.c) relativa a la

[110] Rodríguez Lainz, J. L: «Sobre la Ley orgánica de modificación de la LeCrim para el fortalecimiento de las garantías procesales: la regulación de las medidas de investigación tecnológica». Entiende el autor que el principal mérito de este apartado 5 radica en que «la sola superación de determinados límites cuantitativos penológicos o pertenencia a concretas categorías de infracciones criminales ha dejado de ser por sí misma un aval de superación del principio de proporcionalidad», ya que, por ejemplo, la STC 82/2002, de 22 de abril, llegó a considerar que la sola calificación de un delito como grave en los casos en los que la pena con la que se castiga el delito sea calificada de tal por el Código Penal exime de atender a criterio suplementario diverso al de la propia pena, p. 10. https://www.fiscal.es/fiscal/publico/ciudadano/documentos/ponencias_formacion_continuada/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOI9HT0cDT2DDbz-8Qx3dDBxNvC1NDPwMjQwMDPULsh0VAei-qqo!/?numElementosPorPagina=10&paginaDestino=9.

Velasco Nuñez, E., «Investigación tecnológica de delitos: disposiciones comunes e interceptaciones telefónicas y telemáticas», Jornadas de especialistas en criminalidad informática, Centro de Estudios Jurídicos, CEJ, 2016, p. 3. http://www.cejmjusticia.es/cej_dode/flash/ebook/assets/img/cejponencia1462865634628/cejponencia1462865634628

extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis.a)[111].

En tercer lugar, prevé el secreto de la solicitud y las actuaciones; la duración, el control de la actuación policial por el Juez de Instrucción, el cese de la medida, así como las cautelas para asegurar la autenticidad e integridad de los soportes puestos a disposición del juez, y la destrucción de los registros.

3. La interceptación de las comunicaciones telefónicas y telemáticas[112]. La reforma quiere romper con el carácter obsoleto de la anterior LECrim, pues ésta solo contemplaba la interceptación de las comunicaciones postales, telegráficas y telefónicas; incluyendo, las nuevas tecnologías, de modo que implica la posible intervención de las comunicaciones telefónicas y telemáticas como los SMS y el correo electrónico, así como la interceptación, por ejemplo, de los mensajes de Whatsapp.

Es importante destacar que la autorización para la interceptación solo cabrá en el caso de delitos dolosos con pena que tenga límite máximo de, al menos, tres años de prisión, delitos cometidos por grupo u organización criminal y delitos de terrorismo, añadiéndose los cometidos por medio de instrumentos informáticos o de cualquier otra tecnología de la información o telecomunicación[113]. Se trata de uno de los temas que reclamaba su ordenación, pues el antiguo artículo 579 eludía.

Los terminales o medios que pueden ser intervenidos se refieren a los del investigado, tanto habitualmente, pero también ocasionalmente; incluyendo los listados de las llamadas de las compañías [588 ter.b)]. E incorpora también novedosamente la intervención a terceros, en el caso de que exista constancia se sirva del terminal o medio para transmitir o recibir información, o bien que el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad (588 ter c).

En relación con la solicitud de autorización judicial[114], además de los requisitos que hemos visto anteriormente en el artículo 588 bis.b), prevé la identificación del número del abonado, del terminal o de la etiqueta técnica; la identi-

---

[111] Rodríguez Lainz, J. L.: *El secreto de las telecomunicaciones y su interceptación legal. (adaptado a la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal), Sepin, Madrid, 2016*

[112] En particular la interceptación de las comunicaciones telefónicas y telemáticas está regulada en el Capítulo V, arts, 588 ter.a) a 588 ter.m).

[113] Jaen Vallejo, M. y Perrino Perez, A. L.: *La reforma procesal penal de 2015*, ob. cit., p. 152.

[114] Sin embargo, advierte Zoco Zabala que sigue siendo poco innovadora, ya que no menciona cual es el significado de los indicios racionales que han de ser esgrimidos por el juez; y

ficación de la conexión objeto de la intervención; los datos necesarios para identificar el medio de telecomunicación[115]. Define los datos de tráfico asociados al proceso de comunicación; regulándose el deber de colaboración de los prestadores de servicios de telecomunicaciones, así como de toda persona que de alguna forma pudiera contribuir a facilitar las comunicaciones del sujeto investigado. Estableciéndose así el deber de secreto de todos ellos y las consecuencias derivadas de su incumplimiento (delito de desobediencia) (588 ter.e).

En virtud del artículo 588 ter.j) el acceso a los datos de tráfico electrónicos de trafico (esto es, listados de llamadas entrantes y salientes, requieren autorización judicial, y los prestadores de servicios tienen el deber de colaboración. Estableciendo el control de la medida (588 ter.f) de modo que Policía Judicial pondrá a disposición del juez, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas, asegurando la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas. Estas garantías tratan de evitar, en sintonía con las sentencias del Tribunal Supremo, que se pueda manipular o distorsionar la grabación[116], imponiendo la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el sistema central.

Regula, además, la duración, la solicitud de prórroga y el acceso de las partes a las grabaciones.

La LOMLECrim da un tratamiento jurídico individualizado al acceso por agentes de policía al IMSI, IMEI (588 ter.l), dirección IP (588 ter.k) y otros elementos de identificación de una determinada tarjeta o terminal, en consonan-

---

tampoco menciona los fines a los que sirve la intervención, *Nuevas tecnologías y control de las comunicaciones*, Aranzadi, Madrid, 2015, p. 147

[115] Estableciendo también que para determinar la extensión de la medida, la solicitud de autorización puede tener por objeto: a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta. b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza. c) La localización geográfica del origen o destino de la comunicación. d) El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos. En relación con estos, como advierte Zoco Zabala, ya el artículo 90 RGLT establece la obligación del órgano judicial de mencionar alguno de ellos. La diferencia —indica— es que la LOMLECrim no obliga a que la Policía Judicial o el Ministerio Fiscal aludan a tales datos asociados a la comunicación en la solicitud de autorización judicial, cit. p. 179.

[116] Esto es, está dando soporte a las exigencias del sistema SITEL, sobre el que se había pronunciado en TS en diversas Sentencias, entre otras *vid.* la Sentencia del Tribunal Supremo 250/2009, de 13 de marzo. 737/2009, 756/2009, de 29 de junio, 176/2009, de 12 de marzo

cia con una jurisprudencia del Tribunal Supremo ya consolidada sobre esta materia, a la que nos hemos referido con anterioridad.

El apartado 3 del artículo 588 ter d contempla, asimismo, la intervención en los casos de urgencia en investigaciones relacionadas con bandas armada y elementos terroristas, en los mismos términos de la Ley 4/1988, de 25 de mayo, LECrimm (legislación antiterrorista).

Por último, en este orden, destacar que regula el controvertido tema[117], por las repercusiones que había tenido, de las Comunicaciones Abogado-Cliente. En efecto, el artículo 118.4 proclama que las comunicaciones entre el investigado o encausado y su abogado tendrán carácter confidencial[118]. Determinando que el juez proceda a eliminación de la grabación o la entrega al destinatario de la correspondencia detenida, dejando constancia de estas circunstancias en las actuaciones, en el caso de que estas conversaciones o comunicaciones hubieran sido captadas o intervenidas durante la ejecución de alguna de las diligencias reguladas en esta ley. No siendo de aplicación cuando se constate la existencia de indicios objetivos de la participación del abogado en el hecho delictivo investigado o de su implicación junto con el investigado o encausado en la comisión de otra infracción penal.

4. Además, la LOMLeCrim acaba con otro vacío normativo, ordenando el registro de dispositivos informáticos de almacenamiento masivo[119]; acotando un listado *numerus clausus* los delitos que la pueden habilitar, limitando su duración temporal por mes prorrogable como máximo por iguales periodos de tiempo hasta los tres meses.

Este registro de dispositivos informáticos[120], ciertamente, no estaba previsto en la legislación, y, por tanto, por afectar a datos propios del ámbito de la comu-

[117] STS 79/2012, de 9 de febrero, inhabilitación por el conocido caso Gürtel.

[118] Consecuencia de la Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de liberta

[119] Capítulo VIII, artículos 588 sexies.a-588 sexies.c). Que como señala López-Barajas Perea, I. era una materia en la que reinaba el vacío normativo, salvo lo dispuesto en el Convenio de Budapest de 2001 sobre delincuencia, publicado en el BOE de 17 de septiembre de 2010, prevé como medida de investigación el registro y decomiso de los datos informáticos almacenados. «Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos», *Revista de Internet, Derecho y Política (IDP)*, núm. 24/2017, p. 67

[120] Richard Gonzalez, M.: «La investigación y prueba de hechos y dispositivos electrónicos», *Revista General de Derecho Procesal*, núm. 43/2017. Advierte que en este caso la Ley no establece requisitos del delito o pena para acordar esta diligencia, lo cual no es objetable, ya que esta

nicación requería dicha ordenación (ordenadores, discos duros, memorias, etc.) sobre todo, porque, como advierte Zoco Zabala, «la incautación del ordenador para la intervención de correos electrónicos o las comunicaciones instantáneas a través de internet (chats, videoconferencias, comunicaciones con vídeo y voz) previa resolución judicial motivada en las sospechas de la presunta comisión de un delito grave queda protegido por el artículo 18.3»[121]. Adviértase que el acceso a estos dispositivos, en muchos casos, está protegido por claves o contraseñas, y, por consiguiente entra en la esfera de protección del este precepto.

Recuérdese que ya el Tribunal Supremo se había enfrentado al tema de registro de los dispositivos con ocasión de un registro domiciliario[122]; ahora la Ley no lo permite, salvo resolución judicial motivada (art. 588 sexies.a). «Se pone así fin a una práctica jurisprudencial que hacía extensiva la autorización judicial concedida para la intromisión en el domicilio a la aprensión de todos los soportes informáticos que pudieran encontrarse en el interior de los mismo»[123]. El precepto recoge la jurisprudencia para proteger el entorno tecnológico, cerrando el paso a la legitimación derivada, haciendo frente a una situación en la que mediante la resolución judicial de entrada en el domicilio se amparaba cualquier injerencia, incluso la de los dispositivos electrónicos. Por tanto, la incautación de dichos dispositivos tras un registro domiciliario no basta para su utilización, pues no se contagia de la orden judicial de entrada en el domicilio. La resolución se hace extensiva, también, para el acceso a la información de los dispositivos encontrados fuera del domicilio (588 sexies.b).

---

es una medida invasiva pero concretada en el tiempo y puede permitir esclarecer delitos, en principio, menos graves pero de gran trascendencia social», p. 18.

[121] Zoco Zabala, C.: *Nuevas tecnologías y control de las comunicaciones*, ob. cit, p. 7

[122] El acceso a los contenidos de cualquier ordenador ha de contar con el presupuesto habilitante de una autorización judicial, sin que esta esté incluida en la resolución que autoriza la entrada en el domicilio (STS 19/05/2016)

[123] López-Barajas Perea, I: *Nuevas tecnologías aplicadas a la investigación penal…,* p. 69. Refiriéndose la autora a la STS 2809/2008, de 14 de mayo, «entendió que la orden de entrada y registro habilitaba a la policía para la incautación, entre otras cosas, del material informático que pudiera encontrarse. Por su parte, la STS 4745/2002, 27 de junio, admitió como lícita la lectura de un mensaje grabado en un móvil por considerar que se encontraba bajo la cobertura de la autorización judicial de la entrada y registro. Entendió que los requisitos de validez no eran los propios de una intervención de comunicaciones, sino los que rigen el hallazgo de documentos ya en poder del destinatario». En el mismo sentido, Fernandez-Gallardo Fernandez-Gallardo, J. A.: «Registro de dispositivos de almacenamiento masivo de información», *Dereito*, vol. 25, núm. 2/2016, p. 36. Estudio en el que el autor aborda también los temas relativos al proceso de volcado, pp. 40-41, la necesidad o no de la presencia del secretario judicial, así como un minucioso estudio de otras exigencias establecidas en la nueva ordenación de la LeCrim.

Entre los puntos más débiles de esta regulación puede señalarse que aunque en ambos casos, por razones de urgencia en que se aprecie un interés constitucional legítimo se permite el uso por la policía de la información, deberá comunicarlo inmediatamente al juez, en todo caso en un en un plazo máximo de 24 horas, por escrito motivado (588 sexies.c). Sin concretar más extremos. Aunque debe entenderse que se trata de la información contenida en los equipos que se corresponda con el derecho a la intimidad o a la protección de datos; y no cuando estemos hablando de material protegido por el artículo 18.3, como por ejemplo los correos electrónicos o los servicios que requieran clave de acceso[124].

Con la ordenación de este precepto se supera, como advierte Lopez Baraja, «la jurisprudencia que consideraba legítimo el acceso a la memoria del teléfono móvil por los agentes de política cuando no hubiera un proceso de comunicación en marcha»[125], ya que en ella se equiparaba la agenda electrónica del aparato de telefonía con cualquier otra agenda en la que el titular pudiera guardar números de teléfono y anotaciones sobre las llamadas realizadas.

5. El registro remoto de equipos informáticos[126] (588 septies.a) regula la utilización de los denominados troyanos sujeta a una serie de exigencias. De hecho, ésta ya venía practicándose amparada en el la LOPD 15/1999, de 13 de diciembre. La nueva ordenación de dicho precepto establece los presupuestos[127], así como las garantías.

Sin embargo se ha venido alertando de los problemas técnicos que la instalación de este tipo de software puede acarrear para los equipos informativos; así como los derivados de la solicitud al investigado para revelar sus claves y contraseña con el objeto de facilitar la instalación de troyanos o desactivar los cortafuegos o antivirus y su posible colisión con el derecho a no declarar contra si mismo[128].

---

[124] En este sentido *vid.* También Rivero Sánchez-Covisa, F. J.: *Revisión del concepto constitucional del secreto de las comunicacione*s, Dykison, Madrid, 2017, p. 11

[125] López Barajas, I: *Nuevas tecnologías…,* p. 69

[126] Capítulo IX, artículos 588 septies.a)-588 septies.c).

[127] Delitos cometidos en el seno de organizaciones criminales, delitos de terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional; delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicios de comunicación

[128] Dennis Miranda Wallace: «Registro remoto de equipos informáticos. Comentario crítico al artículo 588 Septies LeCrim», *Revista General de Derecho Procesal,* núm. 42/2017. Trabajo en el que alerta de los posibles daños que puede provocar en el equipos informáticos y la responsabilidad que puede derivar del artículo 32 de la Ley 40/2015, de 1 de octubre, de Régimen

6. Regula novedosamente en el ámbito de la investigación tecnológica la figura del Agente encubierto[129], que ya venía utilizándose, aunque de una parte se prevé la posibilidad de que los agentes encubiertos puedan obtener imágenes y grabar conversaciones, siempre que recaben específicamente una autorización judicial para ello; y de otra, se regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación y que a su vez, requerirá una autorización especial para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación.

V. CONSIDERACIONES FINALES

1. Tras la entrada en vigor de la Constitución española de 1978 no se cumplió el mandato constitucional de desarrollar el derecho fundamental al secreto de las comunicaciones, ni en su dimensión sustantiva ni en la procesal; máxime cuando una ley que cumpliera las garantías de certeza, seguridad, abstracción y generalidad constituía una garantía esencial de nuestro Estado de Derecho.

Los problemas generados por la persistente ausencia de una ley que desarrollara este derecho han abocado a que tanto su contenido material como las exigencias de su intervención —esto es su limitación— se hayan construido con la presencia del juez y la ausencia de legislador. Por tanto, nos encontramos con un derecho que se ha construido a golpe de Sentencias, y a múltiples bandas: Tribunal Europeo de Derechos Humanos, Tribunal de Justicia de la Unión Europea, Tribunal Constitucional y Tribunal Supremo.

2. Ciertamente, dicha construcción pretoriana ha permitido conferir un amplio contenido al derecho que muy escuetamente aparece regulado en el artículo 18.3 de la Constitución, protegiendo las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. Su protección se ha ido extendiendo no solo a estos medios previstos en el texto constitucional, sino también a todos los que han ido apareciendo y puedan aparecer en el futuro.

Sin embargo, la doctrina constitucional que limita la protección del secreto de las comunicaciones únicamente al proceso en marcha de la comunicación nos

Jurídico del Sector Público que prevé el derecho de los particulares a ser indemnizados por la lesiones que sufran en sus bienes y derechos, en particular, pp. 10 y ss.

[129] Regulando su actuación en dos nuevos apartados (6 y 7) del artículo 282 bis, que añaden dos nuevos apartados 6 y 7 al artículo 282 bis

parece muy cuestionable, ya que afecta al contenido esencial del derecho. Su configuración más certera, desde nuestro punto de vista, se ha de centrar en la protección de las comunicaciones con clave de acceso.

3. En el marco laboral, la intervención de las comunicaciones de los trabajadores ha encontrado cobertura en diversas sentencias del Tribunal Constitucional. Amparándose en las facultades de auto organización, dirección y control del empresario la doctrina constitucional ha acuñado los conceptos de canal cerrado y de expectativa de privacidad como criterios para permitir o no tal intervención. Aunque, es cierto que el Tribunal estableció una serie de garantías centradas, esencialmente, en el juicio de proporcionalidad. La reciente Sentencia del Tribunal Europeo de Derechos humanos de 5 de septiembre de 2017 (*Caso Barbalescu contra Rumania*), exigirá incorporar a nuestro ordenamiento nuevas exigencias en orden a intervenir las comunicaciones en el marco de la empresa: señaladamente la determinación de los motivos concretos que justifican la intervención, y el alcance de dicha vigilancia. Su relevancia es incuestionable.

4. El uso y desarrollo de las nuevas tecnologías aporta, por un lado nuevas formas de comunicación; pero por otro, nuevas formas también de delinquir, y en consecuencia, nuevas formas de investigación de los nuevos delitos. Su vertiginoso avance plantea constantes retos a los que el legislador responde con lentitud debido a su complejidad. Y, aunque, tanto jurisprudencial como legalmente se han ido reconociendo y regulando estas nuevas formas de comunicación, los retos constantes que plantean distan mucho de soluciones claras y terminantes. La apertura de «puertas traseras», el acceso a los terminales y el encriptado de mensajes constituyen un claro exponente, y la respuesta a los mismos desde el ordenamiento jurídico dista, también, de ser pacífica, ya que solo puede encontrarse respetando un equilibrio entre seguridad y derechos fundamentales.

5. Si bien la reforma de la LOMLEC es loable por varias razones, sin embargo, no agota todos los temas concertientes a la dimensión material del secreto de las comunicaciones; precisamente porque una ley de carácter procesal no es la que esta llamada a ordenar el contenido sustantivo de este derecho.

Tras cerca de cuarenta años de vigencia constitucional, el legislador ha abordado la ordenación de la interceptación de las comunicaciones siguiendo las exigencias de la doctrina constitucional. Al menos, se aprecia su ordenación detalla-

da[130], de modo que, hasta la fecha, ha merecido una valoración positiva[131]. Aunque pueden destacarse algunas carencias significativas como, por ejemplo, el que apenas explicite el significado de la verdadera *ratio decidendi* de la intervención: los indicios racionales en que se funda la medida[132]. Pero la certera valoración de la norma estará condicionada por los avances que en la práctica se aprecien[133].

Al menos, desde el punto de vista constitucional su relevancia reside en haber abordado una parte del contenido esencial del derecho fundamental como es el establecimiento de sus límites mediante la intervención judicial prevista en el texto constitucional.

6. Pero el derecho fundamental al secreto de las comunicaciones no solo se garantiza cabalmente a través de su ordenación estatal, pues su protección trasciende las fronteras estatales, de forma que su dimensión trasnacional es innegable. Los escudos de privacidad frente a vigilancias masivas, que exigen una actuación sin fronteras, constituyen, hoy en día, uno de los retos esenciales a los que se enfrenta la privacidad frente a la seguridad, y, en definitiva, la libertad. La búsqueda de los equilibrios entre ambas constituye hoy uno de los retos esenciales a los que se enfrentan los derechos fundamentales.

---

[130] Como indica Cavero Forradellas, G.: «La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal», se ha sustituido la parquedad de la regulación anterior, los tres (3) párrafos en un único articulo, el 579 de la LECr, por una normativa extraordinariamente prolija. Grosso modo, el cuerpo normativo que regula la materia de las intervenciones telefónicas se ha multiplicado casi por veinte (19,172), es decir, ha sufrido un incremento cuantitativo del 1.917 %.

[131] Inmaculada López-Barajas Perea: «Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley», *Revista de Derecho Político* núm. 98/2017, pp. 91-119, que, analizando los principios sobre los que se sustenta, se plantea si la nueva Ley define las modalidades y la extensión del ejercicio del poder otorgado con la suficiente precisión para aportar al individuo una protección adecuada contra la arbitrariedad».

[132] Zoco Zabala, C.: *Nuevas tecnologías y control de las comunicaciones*, Aranzadi, Madrid, 2015. Advierte la autora que «La regulación legal de los criterios que el juez tienen que argüir para intervenir las comunicaciones en los supuestos generales omite, sin embargo, los requisitos de intervención de las comunicaciones en supuestos que por ser especiales, precisan criterios diferentes de argumentación», resaltando los casos relativos al interceptación de las comunicaciones en el trabajo, y en otros la solicitud de interceptación por los servicios de inteligencia, incluso las razones de interceptación del orden público para intervenir las comunicaciones en el casos de estados de excepción y sitio., pp. 27-28.

[133] Cavero Forradellas, G.: «La nueva regulación…» ob. cit. Tras una primera lectura de la reforma realiza una valoración positiva, se plantea una serie de cuestiones pendientes de respuesta que perfectamente podríamos suscribir:»¿va a mejorar la situación actual? ¿Se acabaran por fin las anulaciones escandalosas? ¿Podrán de una vez los Jueces de Instrucción y los Fiscales saber donde se encuentra el fundamento suficiente para una intervención telefónica valida? ¿La ley establece finalmente los mínimos para autorizar una interceptación de las comunicaciones?

Title:

The absent legislator of Article 18.3 of the Constitution.

Summary:

I. Introduction. II. Framing constitutional. III. The jurisprudential construction of the substantive dimension of the right to the secret of communications. 1. Configuration of the right to secrecy of communications 2. Extend of the right to secrecy of communications. IV. The jurisprudential construction of the requirements for the intervention of communications. 1. Insufficiency of the norm and jurisprudential fixation of the intervention requirements. 2. Persistence in not legislating. 3. The insufficiency of the precept not by what it says, but by he stops saying. 4. The requirement of motivation of the intervention as part of the essential content of the right. V. The required reform of the criminal procedure law. VI. Final considerations.

Resumen:

Este trabajo aborda los problemas jurídicos generados por persistente ausencia de una ley de desarrollo del derecho fundamental al secreto de las comunicaciones acorde con las exigencias constitucionales. Centrándonos en el estudio de cómo, mediante la presencia del juez y la ausencia del legislador, se ha producido una construcción pretoriana de este derecho, tanto en su dimensión procesal, como en la sustantiva. Y, finalmente, abordamos en qué medida, siguiendo la doctrina constitucional, la recientemente reforma de la Ley de Enjuiciamiento Criminal ha venido a colmar el vacío normativo; quedando pendiente la exigencia de regular, con la garantías que ofrece la ley, el contenido material de este derecho.

Abstract:

This paper addresses the legal problems generated by the persistent lack of a Law on the secrecy of communications, as demanded by the Constitution. This article studies how there was a praetorian construction of this right, both in its procedural and in its substantial dimensions, due to the presence of the judge and the absence of the legislator. It also analyses to what extent, (following the constitutional jurisprudence) the last reform of the Criminal Procedure Law fulfilled the normative vacuum regarding the secret of communications. Nevertheless, it rests pending to regulate, as legally requested, the substantial content of the right including the due legal guaranties.

Palabras clave:

Secreto de las comunicaciones; interceptación de las comunicaciones; derechos fundamentales; garantías constitucionales.

Key words:

Secrecy of communications; interception of communications, fundamental rihts, constitutional guarantees.