NUEVAS TECNOLOGÍAS E INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS

Alfonso López Feria
Comandante auditor

Resumen

La regulación de la interceptación de las comunicaciones ha adquirido una especial relevancia en los últimos años como consecuencia de la irrupción de las nuevas tecnologías en la vida de los ciudadanos, y, especialmente, debido a los nuevos sistemas de comunicación utilizados, dando origen a la proclamación de un nuevo derecho del ciudadano denominado «derecho del individuo al entorno digital». El objeto del presente estudio es analizar las características que ha de reunir una comunicación para que pueda ser acreedora de la protección del derecho al secreto de las comunicaciones, en qué supuestos se puede acordar la restricción de este derecho, para una vez perfilado lo anterior, determinar si los mensajes de wasap gozan de la protección del derecho al secreto de las comunicaciones y el procedimiento de incorporación de dichos mensajes al proceso judicial.

Abstract

The regulation of the interception of communications has acquired a special relevance in recent years as a result of the emergence of new technologies in the lives of citizens, and, especially, due to the new communication systems used, giving rise to the proclamation of a new right

of the citizen called "Right of the individual to the digital environment". The purpose of the present study is to analyze the characteristics that a communication must gather so that it can be creditor of the protection of the right to the secrecy of communications, in which cases the restriction of this right can be agreed, so once the above is outlined, determine if whatsapp messages enjoy the protection of the right to secrecy of communications and the procedure for incorporating said messages into the judicial process.

Palabras clave: interceptación, comunicaciones, nuevas tecnologías, wasap.

Keywords: Interception, Communications, New Technologies, Whatsapp.

SUMARIO

1. INTRODUCCIÓN

La regulación de la interceptación de las comunicaciones ha adquirido una especial relevancia en los últimos años como consecuencia de la irrupción de las nuevas tecnologías en la vida de los ciudadanos, y, especialmente, debido a los nuevos sistemas de comunicación utilizados. Los correos electrónicos, los sistemas de mensajería instantánea como el SMS (*Short Message Service*), los MMS *(Multimedia Messaging System*), y muy especialmente, plataformas de comunicación específica como WhatsApp han supuesto un aumento considerable de la interactividad de los usuarios.

La aparición de las nuevas tecnologías y la utilización de estas en nuestro día a día, ha dado origen a la proclamación de un nuevo derecho fundamental, que ha de entenderse englobado dentro del catálogo de derechos fundamentales y libertades públicas protegidos en nuestra

norma fundamental, recibiendo la denominación actual, ya recogida por nuestro Tribunal Supremo, de «Derecho del individuo al entorno digital».

Tanto los ordenadores como los denominados teléfonos inteligentes (los llamados *smartphone*) almacenan gran cantidad de datos con múltiples funcionalidades. Este derecho del individuo al entorno digital se configura como un derecho de nueva generación, dentro del cual encontramos distintos escalones de protección jurisdiccional.

En la actualidad, en un *smartphone*, existen diferentes tipos de datos que pueden incidir en el derecho a la intimidad del artículo 18.1 de nuestra Constitución, como por ejemplo los contactos, las fotografías o los archivos personales; en el derecho al secreto de las comunicaciones del artículo 18.3, tal podría ser el caso del contenido de los mensajes enviados por los sistemas de mensajería instantánea; y en el derecho a la protección de datos del artículo 18. 4, como determinados datos personales y de geolocalización.

Resulta frecuente, durante la fase de instrucción del procedimiento penal, que las partes soliciten la práctica de pruebas que pueden afectar al derecho fundamental al secreto de las comunicaciones y relacionados con estos nuevos sistemas de comunicación. Tales pruebas, en muchas ocasiones, son solicitadas al juez de instrucción por los letrados intervinientes en los procedimientos, bien por el letrado defensor, al objeto de incorporar al procedimiento pruebas que favorezcan la defensa de su defendido y le eximan de responsabilidad; o bien por la acusación particular, al objeto de incorporar al procedimiento pruebas determinantes de la responsabilidad penal del investigado. Además, en no pocas ocasiones, se solicita la práctica de las pruebas no ya en relación con el investigado, sino en relación con terceras personas ajenas al procedimiento judicial y que no son parte propiamente dicha en el procedimiento.

Por tanto, el objeto del presente estudio es delimitar:

1. Las características que ha de reunir una comunicación para que pueda ser acreedora de la protección del artículo 18.3, a través de una delimitación negativa de la misma.
2. En qué supuestos el juez de instrucción puede acordar la restricción del derecho fundamental al secreto de las comunicaciones.
3. Perfilado lo anterior, si el contenido de las conversaciones de wasap goza de la protección del artículo 18.3.
4. La incorporación del contenido de los wasaps al procedimiento judicial, tanto en fase de instrucción como en fase de juicio oral.

2. CARACTERÍSTICAS QUE HA DE REUNIR UNA COMUNICACIÓN PARA QUE PUEDA SER ACREEDORA DE LA PROTECCIÓN DEL ARTÍCULO 18.3 DE LA CONSTITUCIÓN

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, ha introducido una regulación detallada de la interceptación de las comunicaciones telefónicas y telemáticas como diligencia de investigación que limita el derecho fundamental al secreto de las comunicaciones, introduciendo una nueva regulación contenida en el capítulo V, del título VIII, del libro II, en los artículos 588 ter a) y siguientes.

El punto de partida de la interceptación de las comunicaciones es el derecho fundamental al secreto de las comunicaciones, recogido en el artículo 18.3 de la Constitución: «Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

La previsión contenida en la Ley de Enjuiciamiento Criminal, tras la reforma llevada a cabo por la Ley Orgánica 13/2015, de 5 de octubre, se extiende a las comunicaciones telefónicas y telemáticas. Por comunicaciones telemáticas habría que entender aquellas que emplean la informática para la transmisión de información. En consecuencia, el criterio distintivo entre ambos tipos de comunicación debe residir en el medio que se utiliza para llevar a cabo la comunicación: telefónica, cuando se utilice un teléfono para generar el mensaje que se comunica; y telemática, cuando se utilice un sistema informático. No obstante, nos encontramos con que hoy en día los teléfonos inteligentes (*smartphones*) mezclan en un mismo dispositivo las capacidades de un teléfono y de un ordenador y, por tanto, podrían ser catalogadas como comunicaciones mixtas. No obstante, ambas comunicaciones son objeto de regulación unitaria en la Ley de Enjuiciamiento Criminal, por lo que estamos en presencia de una mera distinción.

Nuestro Tribunal Supremo ha ido perfilando las características que ha de reunir una comunicación para que pueda ser acreedora de la protección del artículo 18.3 de la Constitución. Partiendo de una delimitación negativa del derecho al secreto de las comunicaciones, y siguiendo la jurisprudencia del Alto Tribunal, podemos enumerar una serie de supuestos que no estarían comprendidos en la protección del artículo 18.3 de nuestra norma fundamental:

a) Las conversaciones grabadas o difundidas por uno de los interlocutores.

La Sentencia del Tribunal Supremo 214/2018, de 8 de mayo, Sala de lo Penal, Sección 1.ª, señala que «La jurisprudencia de esta Sala ha declarado la no afectación al derecho al secreto de las comunicaciones y el derecho a la intimidad cuando una persona, graba sus propias conversaciones con terceros, con exclusión de aquellos supuestos relacionados con la provocación delictiva o su empleo como medio de indagación desde estructuras oficiales de investigación delictiva, o que afectan al núcleo de la intimidad. También ha de añadirse los supuestos en los que el contenido de lo grabado es divulgado, ocasionando un daño a la intimidad para lo que habría de estarse al contenido, íntimo o no, de lo que se divulga y ha sido obtenido de forma irregular. Salvados esos escollos, de provocación, de empleo por parte de una institución pública de investigación, o de vulneración del derecho a la intimidad, su utilización podrá ser considerada inapropiada, o cuestionada éticamente, pero no supone una vulneración del derecho al secreto de las comunicaciones…».

La Sentencia 214/2018, recogiendo la doctrina del propio Tribunal Supremo, del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos, sienta las siguientes conclusiones:

1. La utilización en el proceso penal de grabaciones de conversaciones privadas grabadas por uno de los interlocutores, no vulnera en ningún caso el derecho constitucional al secreto de las comunicaciones.
2. Tampoco vulnera el derecho constitucional a la intimidad, salvo casos excepcionales en que el contenido de la conversación afectase al núcleo íntimo de la intimidad personal o familiar de uno de los interlocutores.
3. Vulneran el derecho fundamental a no declarar contra sí mismo y a no confesarse culpable, y en consecuencia incurren en nulidad probatoria, cuando las grabaciones se han realizado desde una posición de superioridad institucional (agentes de la autoridad o superiores jerárquicos) para obtener una confesión extraprocesal arrancada mediante engaño, salvo los supuestos de grabaciones autorizadas por la autoridad judicial conforme a los arts. 588 y siguientes de la Ley de Enjuiciamiento Criminal.
4. No vulneran el derecho fundamental a no declarar contra sí mismo y a no confesarse culpable, cuando se han realizado en el ámbito particular.

5. Pueden vulnerar el derecho a un proceso con todas las garantías, cuando la persona grabada ha sido conducida al encuentro utilizando argucias con la premeditada pretensión de hacerle manifestar hechos que pudieran ser utilizados en su contra, en cuyo caso habrán de ponderarse el conjunto de circunstancias concurrentes.

La doctrina jurisprudencial prescinde de calificar las manifestaciones realizadas por el inculpado en estas grabaciones como confesión, utilizando las grabaciones como ratificación de las declaraciones de los demás intervinientes en la conversación, que tienen el valor de testimonio de referencia sobre las declaraciones del inculpado.

Desde lo expuesto ninguna lesión se produce cuando el inicio de las actuaciones resulta de las grabaciones que una persona aporta a la investigación y son objeto de la pesquisa policial y judicial, sujeta a los principios y garantías propios de un sistema procesal observante de los derechos fundamentales.

b) Las comunicaciones por radio.

El Tribunal Supremo (Sala de lo Penal, Sección 1.ª), Sentencia 695/2013 de 22 julio, afirma que «Como decíamos en la STS 1397/2011 de 22 de diciembre, con citación de la STS 209/2007, de 9 de marzo, y en un supuesto muy similar al de autos, donde dicha captación tiene lugar, también en el curso de otra investigación, las captaciones de conversaciones radiotelegráficas, en frecuencia de uso público, no precisan autorización judicial, porque precisamente por ser de uso público y siendo esto conocido por los usuarios, ello implica una implícita aceptación de la posibilidad de captación».

c) Datos contenidos en la agenda de contactos de un teléfono móvil.

Nuestro Tribunal Constitucional, Sentencia 115/2013 de 9 mayo, ha declarado lo siguiente: «No estamos, por tanto, ante un supuesto de acceso policial a funciones de un teléfono móvil que pudiesen desvelar procesos comunicativos, lo que requeriría, para garantizar el derecho al secreto de las comunicaciones (art. 18.3 CE), el consentimiento del afectado o la autorización judicial, conforme a la doctrina constitucional antes citada. El acceso policial al teléfono móvil del recurrente se limitó exclusivamente a los datos recogidos en la agenda de contactos telefónicos del terminal —entendiendo por agenda el archivo del teléfono móvil en el que consta

un listado de números identificados habitualmente mediante un nombre—, por lo que debe concluirse que dichos datos "no forman parte de una comunicación actual o consumada, ni proporcionan información sobre actos concretos de comunicación pretéritos o futuros" (STC 142/2012 FJ 3), de suerte que no cabe considerar que en el presente caso la actuación de los agentes de la Policía Nacional en el ejercicio de sus funciones de investigación supusiera una injerencia en el ámbito de protección del artículo 18.3 CE.

En efecto, con el acceso a la agenda de contactos del teléfono móvil del recurrente los agentes de policía no obtuvieron dato alguno concerniente a un proceso de comunicación emitida o recibida mediante dicho aparato, sino únicamente a un listado de números de teléfono introducidos voluntariamente por el usuario del terminal, equiparable a los recogidos en una agenda de teléfonos en soporte de papel (STC 70/2002, FJ 9). Por tanto, "siendo lo determinante para la delimitación del contenido de los derechos fundamentales garantizados por los artículos 18.1 y 18.3 CE […] no el tipo de soporte, físico o electrónico, en el que la agenda de contactos esté alojada", ni "el hecho […] de que la agenda sea un aplicación de un terminal telefónico móvil, que es un instrumento de y para la comunicación, sino el carácter de la información a la que se accede" (STC 142/2012, FJ 3), debe descartarse que el derecho al secreto de las comunicaciones (art. 18.3 CE) se haya visto afectado en el presente caso por la actuación policial descrita».

Y, respecto al derecho a la intimidad del artículo 18.1, la misma sentencia[1] señala que no queda afectado el derecho a la intimidad cuando se den los siguientes requisitos:

[1] La STC 115/2013 señala en relación a la posible vulneración del derecho a la intimidad lo siguiente: «Debemos, por tanto, examinar seguidamente, pues la presente es una Sentencia de caso concreto, si en el supuesto que nos ocupa, como también se alega en la demanda de amparo, el acceso policial a la agenda de contactos del teléfono móvil del recurrente sin su consentimiento y sin previa autorización judicial supone una intromisión ilegítima en su derecho a la intimidad (art. 18.1 CE), pues sostiene el recurrente que no concurrían en el presente caso las razones de urgencia, necesidad y proporcionalidad que hubieran podido justificar, conforme a la doctrina constitucional, la injerencia en dicho derecho fundamental.

Ciertamente, como ya se dijo, el acceso policial limitado a los datos recogidos en el archivo electrónico o agenda de contactos telefónicos de un terminal móvil —sin afectar al registro de llamadas entrantes y salientes, ni a ningún otro archivo o enlace que pudiera contener el terminal móvil— constituye una injerencia en el derecho a la intimidad personal (art. 18.1 CE), al igual que lo es la apertura de una agenda en soporte de papel y la lectura de los papeles encontrados en ella (STC 70/2002 FJ 9), pues la agenda de contactos telefónicos contenida en un teléfono móvil (entendiendo por tal el archivo elaborado por el titular de dicho teléfono que, como también ya hemos dicho, recoge una relación de números telefó-

1. Existencia de un fin constitucionalmente legítimo. Dicho fin existe en los supuestos de interés público propio de la investigación de un delito y descubrimiento del delincuente. A través de este bien se defienden otros tales como la paz social y la seguridad ciudadana (artículo 10.1 y 104 de la Constitución).
2. Existencia de cobertura legal. Tiene lugar cuando los agentes actúan con el apoyo legal del artículo 282 de la Ley de Enjuiciamiento Criminal, artículo 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de

---

nicos identificados habitualmente mediante un nombre) ofrece información que pertenece al ámbito privado de su titular, siendo aplicable nuestra doctrina según la cual el artículo 18.1 CE garantiza al individuo un ámbito reservado de su vida "vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio" (SSTC 127/2003, de 30 de junio, FJ 7, y 89/2006, de 27 de marzo, FJ 5, entre otras). La protección de ese ámbito reservado confiere a la persona, así, el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre FJ 5; 70/2009, de 23 de marzo, FJ 2, y 241/2012, FJ 3, entre otras muchas).

No obstante, también constituye doctrina reiterada de este Tribunal que el derecho a la intimidad no es absoluto —como no lo es ningún derecho fundamental—, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el límite que aquel haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo y sea proporcionado (SSTC 57/1994, de 28 de febrero, FJ 6; 143/1994, de 9 de mayo, FJ 6; 98/2000, de 10 de abril, FJ 5, 186/2000, de 10 de julio, FJ 5, y 156/2001, de 2 de julio, FJ 4).

Así mismo, hemos señalado, como antes se dijo, que a diferencia de lo que sucede en el caso del derecho garantizado por el artículo 18.3 CE, el artículo 18.1 CE no prevé la misma garantía de autorización judicial respecto de las intervenciones que afectan al derecho a la intimidad, de modo que excepcionalmente se ha admitido la legitimidad constitucional de que en algunos casos y con la suficiente y precisa habilitación legal, los agentes policiales pueda realizar en el ejercicio de sus funciones de investigación determinadas actuaciones que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, SSTC 123/2002, FJ 4; 281/2006, FJ 4; 173/2011 , FJ 2, y 142/2012 , FJ 2).

Precisando la anterior doctrina, hemos venido estableciendo como requisitos que proporcionan una justificación constitucional objetiva y razonable a la injerencia policial en el derecho a la intimidad (art. 18.1 CE), los siguientes: a) la existencia de un fin constitucionalmente legítimo, considerando como tal el interés público propio de la prevención e investigación del delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal; b) que la medida limitativa del derecho a la intimidad esté prevista en la ley (principio de legalidad); c) que, en caso de no contar con autorización judicial (o consentimiento del afectado), la actuación policial se atenga a la habilitación legal, teniendo en cuenta que la ley puede autorizar a la policía la práctica de inspecciones, reconocimientos e incluso intervenciones corporales leves, siempre y cuando se respete el principio de proporcionalidad, concretado en tres exigencias o condiciones: idoneidad de la medida, necesidad de la misma y juicio de proporcionalidad en sentido estricto (por todas, STC 173/2011, FJ 2, y la jurisprudencia allí citada)…».

Fuerzas y Cuerpos de Seguridad del Estado y artículo 14 de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana, que conforman una habilitación legal específica que faculta a la policía para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente. Entre estas diligencias se encuentra la de examinar o acceder al contenido de esos instrumentos o efectos, así como a los documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que ello sea necesario de acuerdo con una estricta observancia de los requisitos dimanantes del principio de proporcionalidad.

3. Necesidad de la intervención policial para la averiguación del delito, el descubrimiento de los delincuentes o la obtención de pruebas incriminatorias, siempre que se respete el principio de proporcionalidad. Estas razones de urgencia y necesidad vienen avaladas por la flagrancia del delito, circunstancia que refuerza la necesidad de intervención inmediata de la policía.
4. Existencia de proporcionalidad. Es decir, que permita la detención del delincuente, que no exista otra medida más moderada, y que se deriven de dicha medida más beneficios y ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, dada la naturaleza y gravedad del delito investigado y la leve injerencia que comporta en el derecho a la intimidad del recurrente el examen de la agenda de contactos de su teléfono móvil (juicio de proporcionalidad en sentido estricto).

En consecuencia, se concluye que el acceso policial a la agenda de contactos telefónicos del terminal móvil, sin el consentimiento del usuario y sin previa autorización judicial, no vulnera el derecho a la intimidad personal cuando se den tales requisitos.

d) Los datos contenidos en la agenda telefónica, visionado de la pantalla de un teléfono para identificar una llamada de teléfono entrante o la comprobación de la memoria del teléfono o el registro de llamadas.

El Tribunal Supremo (Sala de lo Penal, Sección 1.ª), Sentencia 264/2018 de 31 mayo, ha señalado que «una razón más justifica la desestimación del reproche. De acuerdo con la jurisprudencia imperante al

tiempo en que se produjo el volcado del teléfono (que, insistimos, se llevó a cabo a presencia de la autoridad judicial, del usuario entonces detenido y de su defensa letrada) los datos obtenidos en el volcado y a los que se refiere el oficio (tanto la agenda telefónica como el contenido de los mensajes) no afectan al secreto de las comunicaciones del investigado, sino al derecho a su intimidad, sin que fuera preciso, en tales supuestos y en todo caso, la previa autorización judicial. La STS 41/2010, de 26 de enero, explica como "la jurisprudencia ha venido considerando que no existe intromisión en el derecho al secreto de las comunicaciones (sino intervención en el derecho a la intimidad) en los supuestos de acceso por la policía a una carta abierta que el detenido llevaba consigo en el momento de la detención (STC 70/2002, de 3 de abril); examen por la policía de la pantalla de un teléfono fijo para identificar una llamada entrante o comprobación de la memoria del aparato (STS 3-3-2000); examen de los mensajes SMS registrados en un teléfono móvil intervenido (SSTS 27-6-2002, 30-11-2005); examen del registro de llamadas de un teléfono móvil (SSTS 25-9-2003, 25-7-2003 y 30-11-2005; STC 56/2003, de 24 de marzo)».

e) La conversación escuchada por terceros o agentes policiales a través de aparatos amplificadores de uno de los interlocutores que presta su consentimiento.

La Sentencia 214/2018, de 8 de mayo, ha declarado que *«... quien* emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera *íntima del interlocutor, pudiesen constituir atentados al derecho garantizado en el art. 18.1 CE…».*

Y nuestro Tribunal Supremo (Sala de lo Penal, Sección 1.ª), Sentencia 589/2015 de 28 septiembre, afirma que «… en consecuencia, si la que realiza las llamadas telefónicas voluntariamente es la propia coimputada […] y la misma está de acuerdo en que sus conversaciones sean oídas por terceras personas, en este caso los Mossos d'Esquadra, es indudable que no existe vulneración del secreto de las comunicaciones, ni delito provocado, porque la intención del referido sujeto era recoger aquello que había transportado […] , luego no se le indujo a llevar a cabo ninguna actividad que no fuera aquella que tenía previamente intención de realizar».

3. PRESUPUESTOS. SUPUESTOS EN LOS QUE EL JUEZ DE INSTRUCCIÓN PUEDE ACORDAR LA RESTRICCIÓN DEL DERECHO FUNDAMENTAL AL SECRETO DE LAS COMUNICACIONES

3.1 Ámbito objetivo

La Ley de Enjuiciamiento Criminal dedica el artículo 588 ter a), el primero con el que se abre el capítulo V, al principio de proporcionalidad, que impone limitar el uso de la medida a la investigación de aquellos hechos que, por su especial gravedad, justifiquen la limitación de los derechos fundamentales. Dice el precepto que *«*La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*»*.

Y, por su parte, el artículo 579.1 establece que «El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos:

1. Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
2. Delitos cometidos en el seno de un grupo u organización criminal.
3. Delitos de terrorismo».

Como se puede observar, el artículo 579.1 fija el marco legal mínimo para la interceptación de las comunicaciones, de manera que dicho marco ha de respetar los principios rectores para la adopción de la medida que establece el artículo 588 bis a), dentro de las disposiciones generales, de manera que la resolución judicial ha de recoger la plena sujeción a los principios de especialidad, idoneidad, excepcionalidad y necesidad. E igualmente, dicho marco también ha de completarse con los criterios de ponderación que establece el artículo 588 bis a) 5 para justificar la concurrencia del principio de proporcionalidad en un supuesto concreto, es decir, la gravedad del hecho, su trascendencia social o el ámbito tecnológico de

producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

Igualmente, se ha de hacer una precisión respecto de los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. El fundamento de su inclusión reside en que los delitos cometidos a través de las nuevas tecnologías, difícilmente pueden investigarse a través de otros medios, de suerte que, la interceptación de las comunicaciones y, en particular las telemáticas, puede ser en ocasiones la única vía de investigación criminal de los ilícitos que se cometen a través de la red, de manera que, en este caso, el fundamento de la proporcionalidad no es la gravedad del delito, sino el medio a través del cual se comete el mismo[2].

---

[2] En relación a dicha cuestión, el Auto 170/2018 de 3 abril, de la Audiencia Provincial de Huelva, por el que se estima el recurso de apelación interpuesto por el Ministerio Fiscal contra el auto de sobreseimiento provisional de las actuaciones, por considerar que no se trata de un delito grave, señala lo siguiente: *«...* En cuanto a la cuestión de la gravedad, a la vista del contenido de la denuncia, los hechos *prima facie* parecen encajar en el tipo previsto en el artículo 183 ter, apartado 2 , del Código Penal: "El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años", y si bien dicho delito está castigado con una pena máxima de dos años de prisión, y sin perjuicio de que de la investigación pudieran resultar delitos más graves, en el momento procesal inicial a la hora de acordar la media hay que recordar que el artículo 588 ter a. de la LECrim. al establecer los presupuestos de las medidas como la que aquí nos ocupa, dispone que la autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley (delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; delitos cometidos en el seno de un grupo u organización criminal y delitos de terrorismo) o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación, es decir, el principio de proporcionalidad no se vulnera en este segundo supuesto en la medida en que la investigación recae precisamente sobre los medios o instrumentos empleados por el autor para la comisión de los hechos…».

Por su parte, el Auto 484/2019, de 26 de junio, de la Audiencia Provincial de Orense, establece lo siguiente: *«... en* consecuencia no habiéndose practicado las diligencias de investigación pertinentes y útiles para dictar cualquiera de las resoluciones del art. 777, ha de revocarse el auto recurrido siendo esta diligencia imprescindible al objeto de determinar la autoría de los hechos investigados, teniendo tal diligencia pleno acomodo en el art. 598 ter a) de la LECRm, el cual respecto a los delitos que autorizan la interceptación de las comunicaciones telefónicas y telemáticas no contempla solamente los del art. 579.1 sino que utilizando la conjunción alternativa "o" la permite también para "los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la comunicación o servicio de comunicación" independientemente respecto a este segundo grupo de la pena con la que estén castigados, de manera que se viene a cercenar la impunidad que supone denegar tal medio de investigación cuando los medios tecnológicos son utilizados para cometer el delito*».*

En cuanto al ámbito objetivo de la interceptación de las comunicaciones, aparece recogido en el artículo 588 ter b):

> *«*1. Los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado.
>
> 2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario.
>
> También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.
>
> A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga*»*.

Como se observa, el precepto contempla que el juez autorice no solo el acceso al contenido de las comunicaciones, sino también a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento. De modo que si el juez instructor considera necesario el acceso no solo al contenido de la comunicación, sino también al resto de datos, deberá determinarlo y recogerlo de manera precisa en la resolución judicial habilitante y que se dicte al efecto[3].

[3] La Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas (*BOE* n.º 70, de 22 de marzo de 2019), páginas 11 y 12, señala al respecto lo siguiente*: «*En palabras del preámbulo de la LO 13/2015, se pretende con ello que sea el propio juez, ponderando la gravedad del hecho que está siendo objeto de investigación, el que determine el alcance de la injerencia del Estado en las comunicaciones particulares.

Se termina, de esta manera, con una práctica que se había venido generalizando con anterioridad a la reforma LECrim consistente en la inclusión sistemática, en las resoluciones que acordaban la intervención de comunicaciones, de todos los datos de tráfico o asociados que pudieran ser aportados por el operador telefónico y, todo ello, sin fundamen-

tación alguna que lo justificara. Este indebido modo de proceder, puesto ya de manifiesto por algún pronunciamiento jurisprudencial a partir del voto particular a la STS n*º 316/2011, de 6 de abril, resultaba poco respetuoso con los principios esenciales* fundamentadores de la limitación del derecho fundamental.

Por lo tanto, deberá precisar el juez si la intervención queda limitada a las comunicaciones orales que puedan sostenerse a través del terminal telefónico o se incluyen también los intercambios de mensajes cortos (SMS), correo electrónico o mensajes multimedia (MMS). Igualmente deberá precisarse si la intervención se extiende, además de al contenido de la comunicación, a los datos de tráfico o asociados, o a aquellos que se produzcan con independencia del establecimiento de una comunicación».

Por su parte, el voto particular formulado por el magistrado D. Manuel Marchena Gómez a la Sentencia del Tribunal Supremo 316/2011, de 6 de abril, señala lo siguiente: «Mi discrepancia con el criterio de mis compañeros surge ante la necesidad de poner de relieve lo que, a mi juicio, constituye un entendimiento excesivamente convencional del derecho al secreto de las comunicaciones proclamado por el art. 18.3 de la CE.

Hago mía la cita de la jurisprudencia constitucional y del TEDH acerca de los requisitos de necesidad y proporcionalidad de la medida de injerencia en el ámbito del derecho a la inviolabilidad de las comunicaciones. Sin embargo, nuestra sentencia solo pondera uno de los aspectos ligados a la reivindicada quiebra del derecho al secreto de las comunicaciones, sin detenerse en el dato decisivo que se desprende del auto judicial, que no se limita a autorizar la intervención de las conversaciones telefónicas, sino que va mucho más allá, intensificando el grado de injerencia en el espacio de privacidad de los imputados.

En efecto, la parte dispositiva del auto dictado por el Juzgado de Instrucción n.º 3 de Guecho, Vizcaya, autoriza "... la intervención y escucha por el sistema SITEL, de los teléfonos [...] pertenecientes a los abonados Carlos Alberto y Eutimio, s e autoriza la captación del tránsito de llamadas recibidas y realizadas con los teléfonos número NUM006 y NUM007 pertenecientes a la compañía Movistar, así como el contenido de los mensajes de texto o SMS, identificación y localización de los repetidores, identificación de los números que interaccionan con el intervenido (llamante o llamado) IMEI correspondientes a los teléfonos intervinientes, identidad del titular de los teléfonos que interactúan [...]. Debiendo, igualmente, remitir la titularidad de los referidos teléfonos, caso de no ser tarjeta prepago, así como los listados de llamadas efectuadas y entrantes, con identificación de los titulares de las mismas, en el período de tiempo entre el inicio y la finalización de la intervención telefónica, incluyéndose las prórrogas que en su momento se pudieran autorizar".

La lectura de esa parte dispositiva pone de manifiesto, sin necesidad de mayores esfuerzos argumentales, que la intromisión del poder público en las comunicaciones de quienes fueron considerados sospechosos de dedicarse al tráfico de drogas, fue mucho más allá de la escucha y grabación de los flujos de comunicación verbal entre el ciudadano observado y sus interlocutores. La resolución cuestionada permitió a la policía el acceso sin límites, no ya a la completa identidad de los terceros que contactaban con los sospechosos —tuvieran o no relación con el delito investigado—, sino a todos los mensajes de texto, voz o imagen emitidos desde los terminales intervenidos y, por si fuera poco, a los datos de ubicación geográfica de quienes mantenían una conversación telefónica.

No cuestiono que esos datos electrónicos, generados durante una conversación telefónica mantenida mediante telefonía móvil, pueden llegar a ser de vital interés para el éxito de las investigaciones. Tampoco pongo en duda, la legitimidad de su sacrificio cuando judicialmente se considere que la restricción de ese derecho está justificada con arreglo a los principios que informan la investigación penal en una sociedad democrática. Pero, lo que no puedo avalar, es que la resolución que autoriza el menoscabo del derecho al secreto de las comunicaciones no dedique una sola línea a explicar el porqué de su necesidad y, además, silencie el ineludible juicio de proporcionalidad. Es aquí donde sitúo mi discrepan-

Actualmente, la LECRIM recoge ya esta exigencia en el artículo 588 ter d):

*«*1. La solicitud de autorización judicial deberá contener, además de los requisitos mencionados en el artículo 588 bis b, los siguientes:

a) la identificación del número de abonado, del terminal o de la etiqueta técnica,
b) la identificación de la conexión objeto de la intervención o
c) los datos necesarios para identificar el medio de telecomunicación de que se trate.

2. Para determinar la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos:

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 asociado o no asociado, pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos*»*.

Por otra parte, por datos electrónicos de datos de tráfico o asociados se entiende, según el artículo 588 ter b, último párrafo: «… todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga». Para distinguir entre datos de tráfico y datos asociados debemos acudir al Convenio sobre Ciberdelincuencia, hecho en Budapest el 23 de noviembre de

---

cia respecto de mis compañeros de Sala. Toda decisión judicial que acuerde, además de las escuchas telefónicas de los sospechosos, el control por la policía de otros datos generados durante la conversación, pero con incidencia sustantiva en el ámbito definido por el art. 18 de la CE, ha de motivar, con el mismo nivel de exigencia que venimos imponiendo para validar las escuchas, las razones que explican y legitiman el sacrificio añadido de otros aspectos íntimamente ligados a la privacidad*»*.

2011[4] cuyo artículo 1 establece que «a los efectos del presente Convenio: d) por "datos sobre el tráfico" se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente».

Por su parte, el artículo 1 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativas a las comunicaciones electrónicas y a las redes públicas de comunicaciones, señala que *«*1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará 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.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas*»*[5].

---

[4] Instrumento de ratificación publicado en el *BOE* Nº 226, de 17 de septiembre de 2010.

[5] El artículo 3 de la Ley 25/2007, de 18 de octubre, establece que *«*1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.

ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.

ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.

iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.

ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.

ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1° *Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.*

2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.

ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1° *Con respecto a la telefonía de red fija y a la telefonía móvil*. El servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).

2° *Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.*

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1º *Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.*

2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.

ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.

iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1° *La etiqueta de localización (identificador de celda) al inicio de la comunicación.*

Se trata, en suma, de datos que no afectan exclusivamente al secreto de las comunicaciones proclamado en el artículo 18.3 de la Constitución, sino que se incluyen también otros datos que afectarían a la esfera del derecho a la intimidad del artículo 18.1 o del derecho a la protección de datos del artículo 18.4.

3.2 Ámbito subjetivo

La Ley de Enjuiciamiento Criminal, regula en los artículos 588 ter b) y 588 ter c), la delimitación subjetiva de la medida de interceptación de las comunicaciones telefónicas y telemáticas. En el artículo 588 ter b) el derecho fundamental que se limita es el del investigado. Y también recoge el supuesto de la intervención de los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.

En el artículo 588 ter c) se limita el derecho fundamental de un tercero con fundamento en su relación con el delito a través del investigado. Precepto que enlaza con el artículo 588 bis h) que admite de manera genérica que las medidas de investigación tecnológica de la Ley de Enjuiciamiento Criminal puedan afectar a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas.

Podemos, en consecuencia, distinguir tres supuestos:

1. Utilización por el investigado de terminales o medios de comunicación ajena.

Nuestro Tribunal Supremo ha venido admitiendo la posibilidad de la interceptación de las comunicaciones no solo de las personas sobre las que existen indicios de responsabilidad criminal, sino también de las comunicaciones ajenas. En estos supuestos, lo determinante y relevante es la persona que utiliza el medio de comunicación, de manera que es lícita la intervención del medio de comunicación que usa el investigado, independientemente de que sea o no el titular de la línea.

2° *Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.*

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley».

Y, en el mismo sentido, artículo 39 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

A este respecto, la Sentencia del Tribunal Supremo, 242/2014, de 27 de marzo, señala lo siguiente:

> *«*… El hecho de no haberse acreditado que la acusada fuera titular del teléfono utilizado que se interviene, no debe afectar a la regularidad de la intervención, toda vez que la compañía telefónica no lo facilita. En ese sentido, conviene recordar —como expone el fiscal— la doctrina vigente en esta Sala y en el Tribunal Constitucional.
>
> La S.T.S. de 23-1-2013 nos dice: "Lo cierto es que el art. 579 L.E.Cr. admite como objeto de interceptación las comunicaciones del procesado o [...] de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos". Y la normalidad de un acto jurisdiccional de injerencia respecto de un teléfono que no es titularidad del investigado, no puede ser cuestionada, más allá de la exigencia —no planteada por el recurrente— de un reforzamiento de la motivación en el momento de ponderar la concurrencia de los principios de proporcionalidad, necesidad y especialidad. El criterio favorable a la posibilidad de que la persona investigada no sea la titular del terminal objeto de injerencia ha sido expresado en numerosos precedentes judiciales (cfr. SSTC 49/1999, 5 de abril; 299/2000, 11 de diciembre;17/2001, 19 de enero; 136/2006, 8 de mayo; y SSTS 474/2012, 6 de junio; 759/1995, 3 de junio; 118112000, 3 de julio;934/2004, 15 de julio ; 463/2005, 13 de abril ;918/2005, 12 de julio y 1154/2005, 17 de octubre) (STS 23-1-2013).
>
> Por ello, en todo caso, lo relevante es la determinación de la persona que usa el teléfono, siendo así que cabe la intervención del número utilizado por quien resulta sospechoso de la participación en el delito investigado, con independencia de que sea el titular formal de la línea. En el caso presente, los agentes tienen determinada la identidad de la usuaria de ese número, resultando ser la acusada Fátima, lo que, como señala la Sala de instancia, queda también constatado con el contenido de las conversaciones, y las referencias familiares, además de ser conforme con los seguimientos efectuados*»*.

Lo relevante, en consecuencia, en estos casos, para fundamentar la medida no es la relación de la titularidad del investigado con el terminal o medio de comunicación, sino su relación con el usuario[6].

[6] La Circular 2/2019, de la Fiscalía General del Estado, páginas 16 y 17, señala lo siguiente: *«*... En cualquier caso, la intervención de terminales o medios de comunicación

Respecto a la intervención de las comunicaciones en las que el investigado aparezca como receptor, aparece regulado en el artículo 588 ter b) 2.: «La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario»[7].

2. Intervención de terminales o medios de comunicación de la víctima

Aparece regulada en el artículo 588 ter b) 2, al señalar que «también podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad».

---

que figuren a nombre de terceros va a requerir un especial esfuerzo en la motivación del principio de idoneidad de la medida, que exigirá la exteriorización de indicios que justifiquen esa relación del sujeto investigado con el medio de comunicación de ajena titularidad que se pretende intervenir.

De esta manera, en los supuestos de utilización por el investigado de terminales o medios de comunicación que figuren a nombre de terceros, la necesaria identificación subjetiva de la medida pasará por justificar la relación del investigado con el teléfono y la existencia de indicios que pongan de manifiesto que utiliza ese terminal o medio de comunicación para sus fines delictivos. En estos casos, por lo tanto, la falta de identificación del titular formal del medio no resultará trascendente para valorar la legalidad de la medida, habiendo señalado la STS n.º *48/2013, de 23 de enero: "esa disociación entre el titular o abonado y el usuario de los servicios de telefonía encuentra también reflejo en la Ley 32/2003, 3 de noviembre, en cuyo art. 38.4 se reconoce un estatuto específico a los usuarios que no tengan la condición de abonados, admitiendo el hecho incuestionable de una utilización de las terminales telefónicas disociada de la titularidad del servicio. En consecuencia, el hecho de que en el auto inicial no se especificara quién era el titular de los teléfonos intervenidos, limitándose a hacer mención a uno de los usuarios, identificado como Ramón* —otro de los coacusados finalmente condenados—, no afecta a la legitimidad de la medida».

[7] La Circular 2/2019, de la Fiscalía General del Estado, página 17, señala, respecto a esta cuestión que *«...* la jurisprudencia no ha tenido objeciones en admitir la legalidad de la limitación del derecho fundamental del interlocutor no investigado como consecuencia de la interceptación de las comunicaciones del verdaderamente investigado ("recogida de arrastre", en palabras de la STS n.º 419/2013, de 14 de mayo). De manera muy elocuente señala el Tribunal Constitucional (STC n.º 219/2009, de 21 de diciembre): "No puede considerarse constitucionalmente ilegítima la intervención de las conversaciones de las personas que comunican o con las que se comunican aquellas sobre las que recaen inicialmente los indicios, en la medida en que tales conversaciones estén relacionadas con el delito investigado, correspondiendo al juez, a través del control de la ejecución de la medida, la identificación de las conversaciones relevantes"».

3. Intervención de terminales o medios de comunicación de terceras personas. Aparece condicionado en el artículo 588 ter c) a tres supuestos[8]:

[8] El Auto del Tribunal Supremo de 24 de julio de 2018 (caso independencia de Cataluña, señala que «Este precepto dispone que podrá acordarse la intervención judicial de las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona siempre que: "2º el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad".

En este caso, el instructor ponderó que algunas personas que estaban vinculadas con las instituciones de autogobierno podían estar colaborando con el sector secesionista, ampliando el espectro de los afectados por la medida a ese ámbito que aparece previsto en el art. 588 ter c) de la LECrim, ante la posibilidad de descubrir actos de colaboración con respecto a personas que aparecían incardinadas en sectores oficiales vinculados al proyecto secesionista.

El referido precepto brinda ciertamente esa posibilidad de investigación; sin embargo, también conviene advertir que se trata de una norma que genera algunos interrogantes que no tienen una fácil respuesta.

Nos referimos con ello a que si una persona colabora con otra investigada en sus fines ilícitos es muy plausible que a la primera también deba asignársele la condición procesal de investigada. Frente a ello puede replicarse que es posible que se trate de una colaboración meramente objetiva, sin que el sujeto sea consciente de la ilicitud punible que conlleva su colaboración. Sin embargo, esa presunción de falta de dolo, al margen de la dificultad para su determinación al inicio de una investigación, en la práctica, supone excluir las garantías procesales inherentes a la condición de investigado, presumiendo así en su favor algo que realmente le acaba perjudicando más que favoreciendo. De forma que se le otorga un estatus procesal meramente virtual (investigado en potencia) a pesar de que, de facto, se le cercenan sus derechos fundamentales.

En el caso no consta que alguno de esos sujetos haya impugnado la resolución y tampoco se han acreditado los efectos generados por una medida de esa índole dentro del proceso, desconociéndose si se derivaron perjuicios concretos para sujetos sometidos a una situación procesal de esa naturaleza indefinida. En el supuesto de que se acreditaran siempre podría declararse la nulidad de una medida de esa naturaleza cuando la aplicación del art. 588 ter c) 2º cercenara las garantías que amparan a un sujeto cuyos derechos fundamentales hayan sido indebidamente restringidos».

Igualmente, la Sentencia 709/2015, de 16 de octubre, señala respecto a esta medida que «*p*or *último*, y respecto a la queja de que no se tuviera en cuenta que la mujer de uno de los investigados fuera quien realmente utilizaba el teléfono del que este era titular, carece de la pretendida trascendencia puesto que se autoriza la intervención de un teléfono cuyo titular es el investigado, no siendo imputable al juez, el hecho de que su mujer voluntariamente lo utilizara. Esa disociación entre el titular o abonado y el usuario de los servicios de telefonía encuentra también reflejo en la Ley 32/2003, 3 de noviembre, en cuyo art. 38.4 se reconoce un estatuto específico a los usuarios que no tengan la condición de abonados, admitiendo el hecho incuestionable de una utilización de las terminales telefónicas disociada de la titularidad del servicio (STS 48/2013). La nueva LO 13/2015, dispone en su art. 588 bis h) la afectación de terceras personas, en el sentido de que "podrán acordarse las medidas de investigación reguladas en los siguientes capítulos aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas". Y en el art. 588 ter c), relativo a la afectación a tercero, que podrá acordarse la intervención judicial de las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona siempre que: 1.º exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o 2.º el titular colabore con la persona investigada en sus fines ilícitos o se be-

1º) que exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información; 2º) el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad; y 3º) uso malicioso del dispositivo por parte de terceros.

4. WASAP E INTERCEPTACIÓN DE LAS COMUNICACIONES. DERECHOS PROTEGIDOS

Como se dijo anteriormente, en un *smartphone* se pueden encontrar diferentes tipos de datos que pueden incidir en el derecho a la intimidad del artículo 18.1 de la Constitución, el derecho al secreto de las comunicaciones del artículo 18.3 y en el derecho a la protección de datos del artículo 18. 4.

La naturaleza que pueden tener los mensajes de wasap es determinante a la hora de precisar las normas aplicables para su tratamiento y regulación:

a) Si consideramos que el contenido de los wasap afecta al derecho del secreto de las comunicaciones, su interceptación e intervención deberá regirse por la regulación contenida en los artículos 588 ter a) y siguientes de la Ley de Enjuiciamiento Criminal (relativa a la interceptación de las comunicaciones telefónicas y telemáticas).
b) Si entendemos que el contenido de los wasap afectan al derecho a la intimidad del artículo 18.1 de nuestra norma fundamental, la regulación será la contenida en los artículos 588 sexies a) y siguientes (relativos al registro de dispositivos masivos de información).

Nuestro Tribunal Supremo, Sala de lo Penal, Sentencia 462/2019, de 14 de octubre, considera que la solución depende del momento de la intervención del mensaje. La sentencia en cuestión se refiere tanto a los correos electrónicos como a los sistemas de mensajería instantánea y a la plataforma de wasap, recogiendo las siguientes conclusiones:

1. Si el mensaje no ha llegado a su destinatario todavía o si habiendo llegado no ha sido abierto, nos encontramos ante un proceso de co-

---

neficie de su actividad. También podrá autorizarse dicha intervención cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular».

municación no concluido, afectando, en consecuencia, al derecho al secreto de las comunicaciones del artículo 18.3.

2. Si el contenido del mensaje de wasap ha sido ya leído y posteriormente almacenado, el conocimiento de su contenido, por similitud con la intervención de una carta de correo postal ya abierta y almacenada en el domicilio del investigado, afectaría al derecho a la intimidad y no al secreto de las comunicaciones.

Nuestro Tribunal Supremo, había seguido una línea vacilante en esta materia, pudiendo citarse al respecto la Sentencia 884/2012, de 8 de noviembre que catalogaba los mensajes SMS como un correo electrónico y consideraba que entraba de lleno en el contenido de la inviolabilidad de las comunicaciones y participando de la misma naturaleza el MMS (Multimedia Messaging System).

Así, dice la referida Sentencia, que «… el contenido de los mensajes SMS está constitucionalmente protegido no es cuestionable. El art. 2.h) de la Directiva 2002/58 CE, 12 de julio, del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, proporciona un concepto legal de correo electrónico. Por tal debe entenderse "todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que este acceda al mismo".

A la vista de esa delimitación conceptual no puede existir duda alguna acerca de la catalogación del mensaje SMS como correo electrónico. Es cierto que no todos los contenidos imaginables de mensajería mediante teléfono móvil pueden aspirar al mismo grado de protección constitucional. No faltan casos en que el SMS se utiliza con una finalidad distinta a la transmisión de un pensamiento o de una imagen. Pensemos en su extendida utilización como forma de aviso, de comunicación, de participación en concursos, como receptor de alarmas o de titulares de un medio de comunicación. Pero lo que no es cuestionable —más allá de los matices que podrían hacerse en función del momento en el que se produce la injerencia, si esta tiene lugar cuando el texto ya ha sido leído y simplemente está archivado— es que el mensaje de texto (Short Message System) entra de lleno en el contenido de la inviolabilidad de las comunicaciones. También participa de la misma naturaleza el MMS (Multimedia Messaging System), esto es, el mecanismo técnico que permite el envío de imágenes entre teléfonos móviles».

Por su parte, la Sentencia del Tribunal Supremo 342/2013, de 17 de abril, aborda directamente la naturaleza del contenido de los mensajes, cuando estos ya han sido abiertos, considerando que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por el destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito propio de la inviolabilidad de las comunicaciones. En este caso, la comunicación ya ha culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad protegida en el artículo 18.1 de nuestra Constitución, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad del domicilio.

Dice al respecto la Sentencia 342/2013, que «el acceso de los poderes públicos al contenido del ordenador de un imputado no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar —de hecho, normalmente albergará— información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones.

En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al

imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal».

Ahora bien, lo que resulta evidente, es que una vez se ha producido la aprehensión física del teléfono, en un *smartphone*, pueden existir mensajes de wasap leídos o escuchados, pero también, se podrían encontrar contenidos de wasap no leídos o escuchados. En consecuencia, a mi juicio, la resolución judicial, que autorice la medida, no solo ha de recoger los criterios necesarios para el registro de los dispositivos masivos de información contenida en los artículos 588 sexies a) y ss. (en relación a los wasaps leídos u oídos), sino también los criterios necesarios para la interceptación de las comunicaciones (en relación a los registros no leídos u oídos) contenida en los artículos 588 ter a) y ss. De esta manera, los derechos afectados serían no solo el derecho a la intimidad (artículo 18.1), sino también, el derecho al secreto de las comunicaciones (artículo 18.3).

No obstante, la regulación contenida en la Ley de Enjuiciamiento Criminal, tras la reforma operada por la Ley Orgánica 13/2015, exige en ambos casos resolución judicial motivada, de manera que en dicha resolución habrá de recoger los criterios necesarios para la restricción de ambos derechos fundamentales.

5. INCORPORACIÓN DEL CONTENIDO DE LOS WASAPS AL PROCEDIMIENTO JUDICIAL

En cuanto al procedimiento para incorporar el contenido de los mensajes de wasap a un proceso judicial, debemos de distinguir entre la fase de instrucción y la fase de juicio oral.

a) Fase de instrucción.

Nuestros Tribunales de Justicia[9] han ido perfilando el procedimiento para la incorporación del contenido de los wasaps a un proceso judicial en fase de instrucción como medio de prueba.

[9] Audiencia Provincial de Guadalajara (Sección 1.) Auto 328/2018 de 30 noviembre; Audiencia Provincial de Málaga (Sección 2.ª) Sentencia 495/2017 de 13 diciembre; Au-

Con carácter previo, ha de señalarse, en relación con el contenido de los mensajes de wasap, que los mismos han de cumplir dos presupuestos para su admisibilidad como prueba en un procedimiento judicial. De una parte, cualquier medio de prueba que las partes propongan y que el juez de instrucción acuerde ha de ser obtenido de forma que, ya sea directa o indirectamente, no se violen derechos fundamentales y libertades públicas, de manera que el primer presupuesto de la aceptación del contenido de un wasap como prueba en un determinado procedimiento judicial, es que su obtención se haya llevado a cabo respetando, de un lado, el derecho a la intimidad, y, de otro, el derecho al secreto de las comunicaciones.

El segundo presupuesto de admisibilidad de mensajes de wasap, es la preservación de la cadena de custodia en la obtención y la conservación de la prueba, elemento fundamental para la validez y admisibilidad de la prueba, de modo que permita acreditar su autenticidad e integridad.

Sentado lo anterior, el protocolo debería integrarse por las siguientes actuaciones:

1. Aportación del dispositivo electrónico en el que se contenga el wasap (ya se haya aportado voluntariamente, o mediante intervención policial o judicial), garantizándose su cadena de custodia. Con los requisitos específicos de la misma establecidos en la jurisprudencia, entre otras, en la Sentencia del Tribunal Supremo 587/2014, de 18 de julio en la que se señala que *«*… la cadena de custodia constituye un sistema formal de garantía que tiene por finalidad dejar constancia de todas las actividades llevadas a cabo por cada una de las personas que se ponen en contacto con las evidencias*»*.
2. Transcripción de su contenido por la policía judicial —o bien por impresión del contenido de la pantalla, los denominados pantallazos— bien íntegra o bien de los aspectos relevantes que decida el instructor.

Como variante, también es posible, que se lleve a cabo el volcado del contenido del móvil por perito informático de alguno de los grupos de policía científica; siempre que esté autorizado por resolución judicial. En este caso la fuente de prueba se convertiría en un medio de prueba pericial, cuyo valor probatorio puede y debe conjugarse con otros como testificales, declaraciones de las partes o reconocimiento judicial.

---

diencia Provincial de Soria (Sección 1.ª) Sentencia 47/2018 de 21 mayo.

3. Cotejo, bajo la fe pública del secretario relator o letrado de la Administración de Justicia, de lo transcrito con el dispositivo que lo contenga, con citación de las partes —debe respetarse la contradicción— que deberán tener todo el material a su disposición.

Será este el momento más oportuno para la impugnación de la autenticidad o integridad de la comunicación; pero en todo caso deberá llevarse a cabo de manera que pueda practicarse la pericial oportuna por la parte que lo solicite.

Al margen del protocolo que han ido perfilando nuestros tribunales de justicia, no se debe olvidar que el derecho constitucionalmente protegido en estos supuestos no es solo, como hemos advertido, el derecho a la intimidad, sino que, en algunos supuestos quedaría afectado el derecho al secreto de las comunicaciones. De manera que, en dicho procedimiento deberían incorporarse las reglas establecidas en los artículos 584 a 588 de la Ley de Enjuiciamiento Criminal, relativos a la apertura de correspondencia.

b) Fase de juicio oral

La regulación contenida en la Ley de Enjuiciamiento Criminal que contienen los artículos 588 ter a) y siguientes, relativa a la interceptación de las comunicaciones telefónicas y telemáticas, no dedica precepto alguno a la introducción y práctica de esta prueba en el juicio oral.

Podemos establecer las siguientes premisas:

1. Estamos en presencia de una prueba que requiere ser introducida en el acto de juicio oral bajo los principios de oralidad, inmediación, publicidad y contradicción. En consecuencia, tratándose de wasap de audio, se podría proceder a la audición de las grabaciones o la lectura de sus transcripciones por el secretario relator o por el letrado de la Administración de Justicia.

La Sentencia del Tribunal Supremo 513/2010, de 2 de junio, señala que: «Es necesario dejar claro que el material probatorio son en realidad las cintas grabadas y no su transcripción, que solo tiene como misión permitir un más fácil manejo de su contenido. Lo decisivo, por lo tanto, es que las cintas originales están a disposición de las partes para que puedan solicitar, previo conocimiento de su contenido, su audición total o parcial. Las transcripciones, siempre que estén debidamente cotejadas bajo la fe

pública del secretario judicial, una vez incorporadas al acervo probatorio como prueba documental, puedan ser utilizadas y valoradas como prueba de cargo, siempre que las cintas originales estén a disposición de las partes a los fines antes dichos, de manera que puedan contradecir las afirmaciones y argumentaciones que sobre su contenido se presenten como pruebas de cargo. Así lo ha entendido esta Sala en SSTS. 960/99 de 15.6, 893/2001 de 14.5, 1352/2002 de 18.7, 515/2006 de 4.4 o como dice la STS. 1112/2002 "su introducción regular en el plenario lo será primordialmente mediante la audición directa del contenido de las cintas por el tribunal, fuente original de la prueba. Ahora bien, también es admisible mediante la lectura en el juicio de las transcripciones, diligencia sumarial documental, previamente cotejadas por el secretario con sus originales, e incluso por testimonio directo de los agentes encargados de las escuchas".

En definitiva, los requisitos relativos al protocolo de la incorporación de las escuchas para su posterior utilización como prueba en el juicio son:

1. La aportación de las cintas.
2. La transcripción mecanográfica de las mismas, bien íntegra o bien de los aspectos relevantes para la investigación, cuando la prueba se realice sobre la base de las transcripciones y no directamente mediante la audición de las cintas.
3. El cotejo bajo la fe del secretario judicial de tales párrafos con las cintas originales, para el caso de que dicha transcripción mecanográfica se encargue —como es usual— a los funcionarios policiales.
4. La disponibilidad de este material para las partes.
5. Y finalmente la audición o lectura de estas en el juicio oral, que da cumplimiento a los principios de oralidad y contradicción, previa petición de las partes, pues si estas no lo solicitan, dando por bueno su contenido, la buena fe procesal impediría invocar tal falta de audición o lectura en esta sede casacional.

Consecuentemente las transcripciones de las cintas solo constituyen un medio contingente —y por tanto prescindible— que facilita la consulta y constatación de las cintas, por lo que solo están las imprescindibles. No existe ningún precepto que exija la transcripción ni completa ni los pasajes más relevantes, ahora bien, si se utilizan las transcripciones su autenticidad solo valdrá si están debidamente cotejadas bajo la fe del secretario judicial (SSTS. 538/2001 de 21.3, 650/2000 de 14.9)».

Ha de señalarse que si bien la jurisprudencia reseñada hace referencia a las cintas magnetofónicas, en la actualidad, dicha doctrina ha de enten-

derse completada y referida a los nuevos soportes digitales de grabación de las comunicaciones mediante los sistemas de interceptación utilizados por la Policía Judicial (sistema SITEL), soportes de grabación a los que ya hace referencia el artículo 588 ter f) de la Ley de Enjuiciamiento Criminal, en la nueva redacción dada por la Ley Orgánica 13/2015, de 5 de octubre[10].

2. Se puede introducir también mediante declaración testifical o pericial de los agentes de la policía judicial que procedieron al volcado de los wasaps.

---

[10] En relación con el sistema SITEL, la Sentencia del Tribunal Supremo 524/2017, de 7 de julio, ha señalado lo siguiente: «La jurisprudencia de esta Sala, de la que también ha hecho cita exhaustiva la sentencia recurrida, ha refrendado el uso de tal sistema como suficiente de cara a considerar la autenticidad e integridad de lo grabado. Basta así reiterar, con la STS 358/2016 de 26 de abril (RJ 2016, 6530) que:

"Conviene recordar sobre el sistema SITEL que las acreditaciones individualizadas a los miembros de las unidades de investigación para acceder al sistema, autorizaciones que únicamente permiten visualizar el contenido, pero nunca modificarlo, son pues usuarios pasivos de la información. Y cumpliendo lo ordenado por la autoridad judicial proceden a volcar a un soporte, CD/DVD, el contenido de la intervención correspondiente, volcado que implica nueva certificación digital de cada soporte empleado con las siguientes precisiones:

a) Ese volcado se realiza desde los centros remotos y utilizando los terminales del SITEL.

b) Se verifica de fecha a fecha, es decir, que comienza con el primer día de la intervención e incorpora la totalidad de las conversaciones y datos asociados producidos hasta la fecha que se indique al sistema, que será la señalada por el juzgado para que se le dé cuenta (semanal o quincenalmente) o la necesaria para solicitar la prórroga de la intervención.

c) La realización de sucesivos volcados de la intervención a los soportes CD/DVD se lleva a cabo sin solución de continuidad, enlazando los perí*o*dos temporales hasta que finaliza la intervención, de forma que los CD/DVD aportados de esta manera al Juzgado contienen íntegramente la intervención correspondiente por lo que son los soportes que han de emplear para la solicitud de la prueba, en el caso de que sea necesario, para el acto del juicio oral. Desde un equipo remoto no es posible modificar ni borrar absolutamente nada del servidor central del SITEL. El soporte DVD en el que se vuelca la intervención telefónica se trata de un soporte de solo lectura, porque así lo han acordado llevar a cabo, es decir, se trata de un soporte en el que no se puede grabar sobre el mismo.

d) Las transcripciones de parte de las conversaciones no implican más que una herramienta de facilitación del trabajo al juez. El contenido de las conversaciones y datos asociados queda íntegramente grabado en el Servidor Central del SITEL, y no es posible su borrado sin autorización judicial específica, sin que sea posible su alteración porque queda registrado en el sistema cualquier intento de manipulación y ello de forma indeleble. La aportación de los soportes CD/DVD en los que se ha volcado la información, se efectúa por los responsables de las unidades de investigación y amparadas por la intervención que realiza el funcionario policial que actúa como secretario de estas.

e) En cualquier momento del proceso es posible la verificación de la integridad de los contenidos volcados a los soportes CD/DVD entregados en el juzgado, mediante su contraste con los que quedan registrados en el Servidor Central del SITEL a disposición de la autoridad judicial. Este contraste puede realizarse por el juzgado en los terminales correspondientes para acreditar su identidad con la "matriz" del servidor central…*»*.

Dice al respecto la Sentencia 112/2012, de 23 de febrero, en relación con las escuchas telefónicas que «tampoco esta tesis impugnatoria puede tener acogida. Conviene recordar que ni la jurisprudencia constitucional ni esta misma Sala han exigido como presupuesto de validez ni de suficiencia probatoria que las cintas hayan sido objeto de audición en el plenario. Con carácter general, la escuchas, debidamente autorizadas, sometidas a control judicial e inspiradas en los principios de necesidad, excepcionalidad y proporcionalidad, serán susceptibles de valoración jurisdiccional siempre que puedan convertirse en verdadera prueba. En efecto, las SSTS 363/2008, 23 de junio, 1778/2001, 3 de octubre y 807/2001, 11 de mayo, precisan que el contenido de esas escuchas, como medio de prueba plena en el juicio deberá ser introducido en el mismo regularmente, bien mediante la audición directa del contenido de las cintas por el Tribunal, fuente original de la prueba, mediante la lectura en el juicio de las transcripciones, diligencia sumarial documentada, previamente cotejadas por el secretario con sus originales, e incluso por testimonio directo de los agentes encargados de las escuchas, criterio también reiterado en las SSTS 1070/2003, 22 de julio y 112/2002, 4 de febrero».

3. Un tercer mecanismo de introducción sería su aportación como prueba documental de los mensajes de wasap transcritos, en el caso de que se dé por reproducida, no solicitando ninguna de las partes su audición (wasap de audio) o su lectura. La Sentencia del Tribunal Supremo 867/2014 11 de diciembre, establece lo siguiente: «Así nos hemos pronunciado ante supuestos similares al presente —prosigue diciendo la precitada sentencia del TC—, tales como los resueltos en el ATC 196/1992, de 1 de julio; o en la STC 128/1988, de 27 de junio. En la primera de las resoluciones citadas afirmamos que la no audición de las cintas en el juicio, así como que el secretario no leyera la transcripción de las mismas, no supone, sin más, que las grabaciones no puedan ser valoradas por el tribunal sentenciador. En efecto, las grabaciones telefónicas tienen la consideración de prueba documental (documento fonográfico), por lo que pueden incorporarse al proceso como prueba documental, aunque la utilización de tal medio probatorio en el juicio puede hacerse, claro está, de maneras distintas. Ahora bien, el hecho de que las grabaciones puedan reproducirse en el acto del juicio oral y someterse a contradicciones por las partes —bien de modo directo, mediante la audición de las cintas, bien indirectamente con la lectura de las transcripciones— no significa, como pretende la hoy recurrente, que la prueba documental fonográfica carezca de valor probatorio en los supuestos en los que haya sido incorporada como prueba documental y haya

sido dada por reproducida sin que nadie pidiera la audición de las cintas o la lectura de su transcripción en la vista oral (FJ 1). Y ya en la citada STC 128/1988, llegamos a idéntica conclusión bajo el argumento de que no habiéndose impugnado en todo o en parte la transcripción de las cintas, y habiéndolas dado por reproducidas, no se le puede negar valor probatorio a tales transcripciones».

Finalmente, y en relación con la trascendencia probatoria de los mensajes de wasap en la fase de juicio oral, el propio Tribunal Supremo, ha reconocido la posibilidad de manipulación de los sistemas de mensajería instantáneo. En este sentido, la Sentencia del Tribunal Supremo 300/2015, de 19 de mayo, ha señalado lo siguiente: «… y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales, mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido».

En consecuencia, mientras no se resuelvan dichos problemas de vulnerabilidad, el contenido de los mensajes wasap, siempre y cuando sean impugnados por la parte contraria, no pueden ser utilizados por sí solos y como único elemento con pleno valor probatorio en la fase de juicio oral, por no poder acreditarse su autenticidad e integridad. Por ello, lo necesario en estos casos será la valoración conjunta de todo el material probatorio llevado a cabo en la fase de juicio oral, atendiendo, en consecuencia, no únicamente al contenido de los mensajes de wasap, sino también al resto de pruebas practicadas, tales como las declaraciones testificales o periciales.

Ahora bien, también es cierto que nuestros tribunales de justicia[11] han considerado que ha de darse pleno valor probatorio a las conversaciones

[11] Audiencia Provincial de Guadalajara (Sección 1.ª) Auto 328/2018 de 30 noviembre; Audiencia Provincial de Málaga (Sección 2.ª) Sentencia 495/2017 de 13 diciembre; Audiencia Provincial de Soria (Sección 1.ª) Sentencia 47/2018 de 21 mayo.

de wasap convenientemente incorporadas al proceso, al menos en los casos siguientes:

a) En todo caso, en los supuestos de no impugnación por la parte opuesta, interlocutora en los mensaje.
b) Necesariamente en aquellos casos de reconocimiento expreso de la conversación y de su contenido (Sentencia de la Audiencia Provincial de Córdoba 159/2014 de 2 de abril).
c) De igual modo cuando así resultara en caso de cotejo con el otro terminal implicado (Sentencia de la Audiencia Provincial de Barcelona n.º 143/2014 de 7 de mayo).
d) En los casos de contradicción, cuando exista una prueba pericial que acredite la autenticidad y envío de la conversación de que se trate (Sentencia de la Audiencia Provincial de Madrid 51/2013 de 23 de septiembre de 2013).

6. CONCLUSIÓN

El derecho del individuo al entorno digital es un nuevo derecho que ha de entenderse englobado en el catálogo de derechos fundamentales y libertades públicas protegidos en nuestra norma fundamental, configurándose como un derecho de nueva generación con distintos escalones de protección jurisdiccional.

Los correos electrónicos, los sistemas de mensajería instantánea como el SMS (Short Message Service), los MMS (Multimedia Messaging System), y muy especialmente, plataformas de comunicación específica como WhatsApp han supuesto un aumento considerable de la interactividad de los usuarios, dando origen también a nuevas formas de delincuencia ligadas al uso de las nuevas tecnologías que desbordaban la regulación contenida en la Ley de Enjuiciamiento Criminal. Consciente de ello, 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, ha introducido una regulación detallada de la interceptación de las comunicaciones telefónicas y telemáticas como diligencia de investigación que limita el derecho fundamental al secreto de las comunicaciones. Dentro de estos nuevos sistemas de comunicación destaca la plataforma wasap como, probablemente, el sistema de comunicación más utilizado por los usuarios. El contenido de los mensajes de wasap afecta tanto al derecho a la intimidad como al derecho al secreto

de las comunicaciones, de manera que la resolución judicial que autorice la medida, no solo ha de recoger los criterios necesarios para el registro de los dispositivos masivos de información contenida en los artículos 588 sexies a y ss., sino también los criterios necesarios para la interceptación de las comunicaciones contenida en los artículos 588 ter a) y ss. de la Ley de Enjuiciamiento Criminal.