VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO DE FIN DE GRADO

GRADO EN DERECHO

Departamento: Derecho Administrativo, Financiero y Procesal

Área de conocimiento: Derecho Procesal

Curso 2017/2018

Una visión panorámica del SITEL: fundamentos técnicos y jurídicos

Alejandro González Hernández

Tutora: D.ª Alicia González Monje

Julio de 2018

TRABAJO DE FIN DE GRADO

GRADO EN DERECHO

Departamento: Derecho Administrativo, Financiero y Procesal

Área de conocimiento: Derecho Procesal

Una visión panorámica del SITEL: fundamentos técnicos y jurídicos

An overview of SITEL: technical and legal foundations

Alejandro González Hernández
alejandrock3@usal.es

Tutora: D.ª Alicia González Monje

RESUMEN

La intervención de comunicaciones siempre ha sido una de las bazas policiales en la investigación de los delitos. Sin embargo, el paso del tiempo y la modernización de los medios de comunicación obligan a las Fuerzas y Cuerpos de Seguridad del Estado a actualizarse, bajo la amenaza de quedarse fuera de juego, obsoletos. Con esa idea nace el Sistema Integrado de Interceptación Legal de Telecomunicaciones (SITEL), el cual nos permite captar, siempre que medie autorización judicial, distintos tipos de informaciones en el ámbito telefónico. El SITEL goza de un armazón técnico o físico repartido por todo el territorio español, así como de una regulación reciente que, si bien últimamente ha conseguido situarse en una posición no tan desventajosa, sigue avanzando lenta y pesadamente con el riesgo de volverse a ver superada por la realidad social. La diligencia de interceptación legal de comunicaciones y, por tanto, el SITEL, se encuentra frente al reto de ir abriéndose paso por un terreno aún no consolidado, así como de articular el respeto o la coordinación entre sí mismo y el derecho fundamental al secreto de las comunicaciones. Los últimos avances, como las aplicaciones de telefonía móvil, no hacen más que servir de examen al SITEL, evaluando su capacidad de adaptación.

PALABRAS CLAVE: Sistema Integrado de Interceptación Legal de Telecomunicaciones, SITEL, derecho al secreto de las comunicaciones, diligencias de investigación, proceso penal.

ABSTRACT

The intervention of communications has always been one of the police assets in the criminal investigations. However, to stand the test of time and due to the mass media modernization, State Security Forces need to be updated, under threat of being out of play, obsolete. That is the reason why the Integrated Telecommunications Interception System (SITEL) arises, which allows us to capture different types of telephone informations, once a judicial authorization is executed. The SITEL has a technical or physical framework distributed throughout the Spanish territory, as well as a recent regulation that, although lately has managed to place itself in a not so disadvantageous position, it continues moving slowly and heavily with the risk of being overcome by the social reality. In addition, the legal interception of communications task and, therefore, the SITEL, is facing the challenge of breaking through a not yet consolidated field, and attaining respect or coordination among themselves as well as the fundamental right to the secret communications. With regard to this, latest developments, such as mobile applications, test SITEL by evaluating its adaptability.

KEYWORDS: Integrated Telecommunications Interception System, SITEL, right to secrecy of communications, investigation diligences, criminal process.

Í N D I C E

ABREVIATURAS

Art. ---------- Artículo

CE ---------- Constitución Española

CEDH---------- Convenio Europeo de Derechos Humanos

CD---------- *Compact Disc*

CP ---------- Código Penal

DUDH --------- Declaración Universal de los Derechos Humanos

DVD ---------- *Digital Versatile Disc*

GSM ---------- *Global System for Mobile communications*

IMEI ---------- *International Mobile Station Equipment Identity*

LEC ---------- Ley de Enjuiciamiento Civil

LECrim -------- Ley de Enjuiciamiento Criminal

LO---------- Ley Orgánica

SITEL---------- Sistema Integrado de Interceptación Legal de Telecomunicaciones

STC ---------- Sentencia del Tribunal Constitucional

STS---------- Sentencia del Tribunal Supremo

STEDH -------- Sentencia del Tribunal Europeo de Derechos Humanos

TFG ---------- Trabajo de Fin de Grado

1. INTRODUCCIÓN

El Sistema Integrado de Interceptación Legal de Telecomunicaciones, que da nombre a este trabajo, será el principal objeto de estudio en el mismo. Con el ánimo de concebir una visión general sobre éste, trataremos aspectos de muy diferente naturaleza. Tanto es así, que comenzaremos con una retrospectiva del derecho al secreto de las comunicaciones, haciendo hincapié tanto en sus límites, como en los hitos más importantes de su desarrollo hasta llegar a nuestros días. La necesidad de la que emana la utilización de este sistema, su funcionamiento o sus características más estrictamente técnicas, tampoco faltarán en el desarrollo de este TFG. Obviamente, los aspectos jurídicos estarán presentes en tanto en cuanto este trabajo se proyecta bajo la luz de las diligencias de investigación en el proceso penal y, por tanto, del Derecho Procesal.

La intención es, como ya hemos señalado, la de dar una visión en conjunto. Para ello, se intentará elaborar una exposición lógica y ordenada de los temas anteriormente descritos, no ya sólo para trazar un desarrollo teórico de la materia, sino a fin de establecer de forma consolidada los fundamentos del SITEL y dar buena cuenta de su utilización práctica. Utilización práctica que, siempre y en todo caso, circunscribiremos al ámbito territorial español y a las actuaciones de nuestras Fuerzas y Cuerpos de Seguridad del Estado[1].

Con tal fin nos apoyaremos, además de en diversas fuentes bibliográficas, en una multitud de referencias jurisprudenciales que nos ayudarán a llenar los vacíos de una normativa que, si bien ha hecho algún movimiento en pos de situarse al lado de la realidad social y sus demandas, ha necesitado de las continuas aportaciones de los tribunales para afianzarse.

La intervención de las comunicaciones no es algo novedoso. Sin embargo, la importancia que ostenta hoy en día es exponencialmente superior a la de años atrás. Este hecho, sumado al generalizado desconocimiento sobre el SITEL –tanto a pie de calle como entre los mismos alumnos del Grado en Derecho– y a un interés personal por la Policía Judicial, me ha hecho decantarme por este asunto. Por todo ello, la idea de realizar un trabajo en el cual se situase la información clave sobre el SITEL, a modo de fundamentos del sistema, me parece un acierto y algo adecuado en virtud del contexto.

[1] Respecto a la intervención de comunicaciones cuando concurra una nota de transnacionalidad, véase GONZÁLEZ MONJE, A., *Cooperación jurídica internacional en materia penal e intervención de comunicaciones como técnica especial de investigación*, BUJOSA BADELL, L. M. (pr.), Comares, Granada, 2017.

2. EL DERECHO FUNDAMENTAL AL SECRETO DE LAS COMUNICACIONES

2.1. Breve referencia al origen del derecho al secreto de las comunicaciones

Si quisiésemos bucear a lo largo de la historia en busca del origen de este derecho, obviando lo relativo a la privacidad entendida en el sentido más personal, deberíamos remontarnos más de doscientos años atrás; concretamente, hasta la Revolución Francesa. El precedente que se dibuja en este contexto no deja de ser, a todas luces, un mero embrión de lo que actualmente conocemos como el derecho al secreto de las comunicaciones; podemos afirmar tal cosa sin riesgo de infravalorarlo pues, lo que los franceses antaño denominaron como *le secret des lettres*[2], tan sólo protegía la privacidad de la comunicación en el ámbito de la correspondencia postal[3].

Adentrándonos en nuestro sistema jurídico en particular, debemos hacer algunos altos en el camino antes de llegar a la Constitución Española de 1978. Para ser más precisos debemos analizar, en primer lugar, uno de los artículos presentes en la Constitución Española de 1869[4], cuyo artículo 17 establece lo siguiente: «en ningún caso podrá detenerse ni abrirse por la Autoridad gubernativa la correspondencia confiada al correo, ni tampoco detenerse la telegráfica. Pero en virtud de auto de juez competente podrán detenerse una y otra correspondencia, y también abrirse en presencia del procesado la que se le dirija por correo»[5]. Es apreciable, por tanto, ese primer paso que llevaría a nuestro país hasta el reconocimiento, tiempo después, del derecho al secreto de las comunicaciones.

Una reproducción similar al fragmento que acabamos de citar reposa en el mismo ordinal de otro cuerpo legal, concretamente de la Constitución Española de 1876[6]: «no podrá detenerse ni abrirse por la autoridad gubernativa la correspondencia confiada al correo». Pero en su artículo 8 nos dice algo más, añadiendo el deber de

---

[2] La Asamblea Nacional francesa, en un Decreto de 1970, con fecha de 10 de agosto, reconoció este derecho al afirmar que *le secret des lettres est inviolable*.

[3] CASANOVA MARTÍ, R., *Problemática de las intervenciones telefónicas en el proceso penal: una propuesta normativa*, PICO I JUNOY, J. (dir.), Publicacions URV, Tarragona, 2014, p. 31.

[4] Producto de la Revolución 1868 y considerada como la primera constitución democrática española, puso fin al reinado de Isabel II a favor de Amadeo de Saboya. Si bien con altibajos, podemos decir que mantuvo una relativa vigencia hasta el comienzo de la Restauración borbónica, cuyo comienzo se vincula al pronunciamiento de Martínez Campos.

[5] Original disponible en http://www.congreso.es/docu/constituciones/1869/1869_cd.pdf y transcrita en, entre otros, RICO LINAGE, R., *Constituciones históricas*, Publicaciones de la Universidad de Sevilla, Sevilla, 1999, p. 140.

[6] Promulgada el 30 de junio de 1876 por Cánovas del Castillo, se trata de un texto no demasiado extenso, formado por 89 artículos, que facilita la alternancia de los partidos en el poder. Íntimamente ligada a la Restauración borbónica en España, estuvo en vigor 55 años, hasta la llegada de la Segunda República en 1931.

motivación: «todo auto de prisión, de registro de morada o de detención de la correspondencia, será motivado»[7].

Para finalizar con esta introducción a sus orígenes y con el ánimo de no extenderme demasiado en aquello que no es el objeto principal de este trabajo, así como de situarnos rápidamente en el actual marco normativo, me limitaré a señalar que este derecho se irá reconociendo de forma sistemática en las constituciones posteriores tras abrirse la veda en el año 1869, incluyendo –de forma *sui generis* y como ejemplo más anecdótico que merecedor de una verdadera importancia– el Fuero de los Españoles de 1945, cuyo artículo 13 decía reconocer y garantizar la libertad y el secreto de la correspondencia[8].

2.2. El derecho al secreto de las comunicaciones en la actualidad

Hemos de irnos hasta la Sección 1.ª del Capítulo II de la Constitución Española de 1978 para encontrar el precepto correspondiente, algo que es obvio en tanto en cuanto hablamos de un derecho fundamental. En el artículo 18 de nuestra carta magna podemos apreciar el reconocimiento de varios derechos, todos ellos muy vinculados al objeto de este trabajo. Sin embargo, en el apartado tercero se afirma que «se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial». Aunque salta a la vista que este precepto es el protagonista por excelencia del tema que nos ocupa, resulta difícilmente discutible el hecho de que los derechos reconocidos a lo largo del artículo 18 tienen mucho en común, en la medida en que no dejan de suponer distintas vías, distintos caminos y posibilidades para salvaguardar el derecho a la intimidad –entendido en sentido amplio–, el cual puede ser, a su vez, atacado mediante actos de diferente naturaleza[9].

Podemos afirmar, entonces, que de ese objetivo compartido que es la defensa de la intimidad emanan distintos derechos que convierten dicha protección en algo más especializado y, es de suponer, más preciso. La concreta tarea del apartado tercero del artículo que estamos tratando podemos apreciarla en una sentencia del Tribunal Constitucional[10], en la cual se refleja la posición del Abogado del Estado interviniente: «debe destacarse que, aunque sus distintos apartados tienen una indiscutible trabazón,

[7] Original disponible en http://www.congreso.es/docu/constituciones/1876/1876_cd.pdf; véase a este respecto PUY MUÑOZ, F., *Los derechos del constitucionalismo histórico español*, Servicio de Publicacións e Intercambio Científico, Universidade de Santiago de Compostela, 2002, p. 120.
[8] TEJERINA RODRÍGUEZ, O., *Seguridad del Estado y privacidad*, Reus Editorial, Madrid, 2014, p. 186.
[9] ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, Iustel Publicaciones, Madrid, 2007, p. 38.
[10] STC 114/1984, de 29 de noviembre.

cada uno de ellos posee su propia función protectora, siendo la de su número 3 la de garantizar que nadie ajeno al emisor y al receptor de la comunicación entre en conocimiento del contenido de la misma sin la autorización de los comunicantes».

Tras hacer una somera referencia a esa correlación entre los distintos apartados del artículo 18, damos un paso más allá y, casi involuntariamente, pasamos a referirnos al contenido mismo del derecho al secreto de las comunicaciones. Como acabamos de mencionar, y citando de nuevo al Abogado del Estado, «se trata de que nadie ajeno al emisor y al receptor de la comunicación entre en conocimiento del contenido de la misma sin la autorización de los comunicantes»[11].

En palabras de BELDA PÉREZ-PEDRERO, el derecho al secreto de las comunicaciones es «una garantía sobre uno de los aspectos esenciales de la vida privada, como es la libertad de relacionarse con otra u otras personas distantes, a través de un medio destinado al efecto, sin que transcienda el contenido del proceso comunicativo»[12].

Siendo así, resulta necesario destacar una diferencia con respecto del resto de los derechos del artículo 18; si bien ya hemos mencionado que todos salvaguardan el derecho a la intimidad, sea siguiendo uno u otro cauce dependiendo del apartado en cuestión, el derecho al secreto de las comunicaciones goza de un rasgo característico. La ya citada STC 114/1984, de 29 de noviembre, cuyo ponente fue DÍEZ-PICAZO Y PONCE DE LEÓN, nos dice en su fundamento jurídico séptimo que, en efecto, «el concepto de "secreto" en el art. 18.3 tiene un carácter "formal", en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado». En definitiva, el apartado tercero no se limita a proteger aquello que material u objetivamente pertenezca a la vida íntima de la persona, sino que adopta un carácter formal que supone que lo protegido sea la información que discurra o se transfiera durante el proceso de la comunicación, bien se considere íntima para la persona o no. Imaginemos, exagerando y con ánimo ejemplificativo, una conversación telefónica entre dos personas; una de ellas confiesa a la otra ciertas experiencias relativas a su esfera más personal (referentes, por ejemplo, a su vida sexual) y, tras ello, comienzan a alcahuetear sobre cuestiones de escasa importancia. De no existir ese carácter formal, tan sólo esas confesiones realizadas en primer lugar

[11] STC 114/1984, de 29 de noviembre.
[12] BELDA PÉREZ-PEDRERO, E. *El derecho al secreto de las comunicaciones* [en línea]. Dialnet: La Rioja, p. 170 [consulta: 08/03/2018]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/197133.pdf

estarían protegidas por el derecho al secreto de las comunicaciones. En cambio, en la práctica, esa parte de la conversación que no parece realmente ligada a la esfera privada o íntima de la persona también estará protegida por este derecho fundamental del artículo 18.3 de la Constitución Española. De este modo, podríamos afirmar que el concepto de «secreto» se amplía al mensaje en su conjunto, sea lo que sea lo que se esté diciendo; se presume *iuris et de iure* que todo aquello que está siendo objeto de comunicación es secreto. Y no sólo el contenido del mensaje en sí mismo, sino también otras dimensiones de la comunicación como pueden ser, por ejemplo, los interlocutores[13].

El artículo 18.3 de nuestra Constitución determina que se garantiza el secreto de las comunicaciones, haciendo hincapié en aquellas que son postales, telegráficas y telefónicas. No hay duda, gracias ese enunciado abierto, de que este artículo no intenta descartar otros tipos de comunicación, pero fácilmente nos surge una pregunta: ¿qué concretos medios de comunicación son los protegidos por este apartado?, ¿todos? Resultaría lógico incluir los nuevos cauces que utilizamos hoy en día fruto de la, en apariencia perenne, revolución tecnológica (aplicaciones de móvil tales como *WhatsApp* o *Line*, correos electrónicos, etcétera), entre otras cosas por la dificultad de legislar al día respecto de los mismos. Pero, ¿y el resto? Tengamos en cuenta que en la época que vivimos es posible comunicarse por infinidad de vías: desde programas como *Skype*[14], que ya podríamos hasta considerar «tradicionales», hasta el chat de un juego en línea.

Afortunadamente, el rango de protección de este precepto camina de la mano con la lógica que hemos aplicado en el párrafo anterior. En esta línea, incluiríamos cualquier comunicación siempre que ésta se efectúe a través de lo que ELVIRA PERALES denomina «algún medio o artilugio técnico»[15]. Afirmamos tal cosa debido a que la mayoría de los autores se inclina por pensar que en la intervención de una comunicación directa lo vulnerado sería, en su caso, el derecho a la intimidad del apartado primero y no el derecho al secreto de las comunicaciones. A este respecto, el Tribunal Constitucional dictó sentencia afirmando que se protege únicamente la comunicación llevada a cabo en canales cerrados[16]. Merece la pena recordar, retrotrayéndonos al alegato del Abogado del Estado en la STC 114/1984, que requerimos de la existencia de un tercero, es decir, no estaríamos ante una vulneración

[13] Véanse a este respecto las SSTC 114/1984, de 29 de noviembre, y 115/2013, de 9 de mayo.
[14] Diseñado en 2003 por Janus Friis y Niklas Zeenström, se catalogó de revolucionario junto con otros *software* como *MSN Messenger*. Hoy en día es algo totalmente asentado y para nada novedoso.
[15] ELVIRA PERALES, A., *Derecho al secreto…*, op., cit., p. 42.
[16] STC 170/2013, de 7 de octubre.

de este derecho si es uno de los intervinientes en la conversación el que levanta el secreto; si bien en este caso podríamos hablar, de nuevo, de una violación del derecho a la intimidad.

Si quisiéramos, con los datos que hemos recopilado hasta ahora, explicar o dar una definición amplia sobre lo que supone el derecho al secreto de las comunicaciones, podríamos decir lo siguiente: «es el derecho a que, en el marco de la comunicación entre dos o más personas a través de cualquier medio de carácter cerrado, el contenido del mensaje no sea conocido por un tercero ajeno –salvo que medie autorización judicial–, bien forme parte este contenido de la esfera personal o íntima de la persona, bien no»[17]. Parece una definición enrevesada –y quizá lo sea–, pero mi idea es desmarcarme de otras afirmaciones realizadas por autores como CASANOVA MARTÍ pues, según mi opinión, no debemos atribuir a este derecho competencias que no le sean propias. Esta autora define el derecho al secreto de las comunicaciones como «un derecho fundamental que permite que una persona pueda comunicarse libremente con cualquier otra a través de un medio de comunicación cerrado, y sin que sea conocido el contenido de la comunicación por terceros ajenos a la misma»[18].

Expuesto lo anterior, decir que el derecho que nos ocupa no es tan amplio como de esta definición podríamos inferir pues, en mi opinión y en virtud de lo estudiado para realizar este trabajo, tan sólo protege la privacidad o el secreto del mensaje; no es un derecho amplio que incluya en su contenido la libertad de comunicarse con un tercero en sentido general.

Para finalizar con este apartado, una brevísima mención a los ámbitos europeo e internacional: hay que tener en cuenta los artículos 8 y 12 del Convenio Europeo de Derechos Humanos[19] y de la Declaración Universal de los Derechos Humanos[20] respectivamente. Si bien estos preceptos se refieren a la intimidad en sentido amplio y, más concretamente, tan sólo a la correspondencia, hemos de entenderlos de forma inclusiva debido a los enormes avances tecnológicos de los últimos años[21].

[17] Definición propia.
[18] CASANOVA MARTÍ, R., *Problemática…*, PICO I JUNOY, J. (dir.), op., cit., p. 36.
[19] Art. 8.1 CEDH: «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia».
[20] Art. 12 DUDH: «nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».
[21] No mencionamos el art. 17 del Pacto Internacional de Derechos Civiles y Políticos por entenderlo subsumido en la Carta Internacional de Derechos Humanos en virtud de la DUDH.

2.3. Los límites del derecho fundamental al secreto de las comunicaciones

Es una verdad indiscutible el hecho de que todos[22] los derechos, incluidos los fundamentales, están sujetos a límites, pues la coexistencia con otros derechos o valores jurídicos –que han de ser igualmente protegidos– obliga a ello. En el artículo 4 de la Declaración de los Derechos del Hombre y del Ciudadano[23] ya se determinó, por aquel entonces y en este mismo sentido, que «el ejercicio de los derechos naturales de cada hombre tan sólo tiene como límites los que garantizan a los demás miembros de la sociedad el goce de estos mismos derechos»[24]. Estos derechos, en palabras de CEA ENGAÑA, «jamás tienen alcance absoluto, pues si lo poseyeran se convertirían en prerrogativas típicas de un déspota que obra, sin castigo, con rasgos ilícitos o abusivos»[25].

Admitir este carácter limitado no supone, ni mucho menos, relegarlos de su posición privilegiada; el Tribunal Constitucional camina por esta misma senda al afirmar que «en efecto, no existen derechos ilimitados. Todo derecho tiene sus límites que […] establece la Constitución por sí misma en algunas ocasiones, mientras en otras el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos»[26].

Como bien expone IGLESIAS BÁREZ[27], la idea de «límite» siempre ha de estar ligada al concepto de garantía. Hablamos de la necesidad de que ese límite exista para, tal como expresa el Tribunal Constitucional y retrotrayéndonos a lo ya dicho anteriormente, «proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos». Si bien la regla general es que todos los derechos están limitados, existen excepciones tales como la prohibición absoluta de las torturas y de los tratos inhumanos o degradantes[28].

Sea como fuere, y siguiendo de nuevo las explicaciones que nos brindó la profesora IGLESIAS BÁREZ, nos topamos con distintos tipos de límites.

---

[22] Con excepciones puntuales, como veremos a continuación.
[23] La *Déclaration des droits de l'homme et du citoyen*, que cuenta con diecisiete artículos, fue aprobada el 26 de agosto de 1789 por la Asamblea Nacional Constituyente en el contexto de la Revolución Francesa.
[24] Original disponible en http://www.elysee.fr/la-presidence/la-declaration-des-droits-de-l-homme-et-du-citoyen; traducción al castellano disponible en https://www.tendencias21.net/derecho/attachment/93029
[25] CEA ENGAÑA, J. L., *Derecho constitucional chileno: Tomo II*, Ediciones UC, Santiago, 2012, p. 62.
[26] STC 2/1982, de 29 de enero.
[27] En sus clases para la asignatura «Derechos fundamentales y organización territorial del Estado».
[28] Para más información, véase BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, Editorial Dykinson, Madrid, 2004, pp. 37 y ss.

En una primera clasificación podríamos distinguir entre límites reconocidos en la Constitución Española y aquéllos que reposan en la ley. Los primeros son fruto de la actividad del constituyente y no pueden ser sometidos al control del Tribunal Constitucional; en cambio, los límites establecidos por parte del legislador sí que pueden ser objeto de control por parte del sumo intérprete de la Constitución.

No obstante, hay otra forma de clasificarlos, y ésta es en límites expresos e implícitos. Respecto a los primeros, los expresos, decir que están reconocidos en la Constitución de forma manifiesta, evidente. A su vez, éstos pueden ser clasificados o divididos en límites generales, los cuales están recogidos esencialmente en el artículo 10.1 de la Constitución[29], y en límites específicos, que se van reconociendo a lo largo de los distintos derechos fundamentales[30]. En cuanto a los límites implícitos, huelga decir que se trata de aquéllos deducidos de otros derechos fundamentales o de la interpretación de la Constitución Española como un todo[31]. Para finalizar esta breve referencia a los tipos de límites antes de centrarnos en los del derecho que nos ocupa, deberíamos –como mínimo– mencionar lo relativo a los límites internos de los derechos fundamentales, que no son más que las restricciones con las que ya nacen los mismos[32].

En el caso del derecho al secreto de las comunicaciones hay un límite que se nos pone de manifiesto con la mera lectura del precepto, el cual concluye con la expresión «salvo resolución judicial». Estamos, por tanto, ante un límite reconocido de forma expresa en la propia Constitución Española. Por consiguiente, este derecho al secreto de las comunicaciones podrá ser limitado por medio de una resolución judicial, aunque sólo cuando medie un interés u objetivo constitucionalmente legítimo, tal como la prevención, investigación o punición de los delitos.

Esta última afirmación la extraemos de la STS de 19 de junio de 2013, en la cual se rechaza el carácter absoluto de este derecho al secreto de las comunicaciones y se exponen ciertos requisitos que han de cumplirse para llevar a cabo su restricción, al

[29] Art. 10.1 CE: «la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social».
[30] Tendríamos, entre otros, el orden público sito en el art. 16 CE o, yéndonos hasta el art. 20, el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
[31] Son realmente escasos: el Tribunal Constitucional tiene una jurisprudencia asentada en virtud de la cual efectúa un reconocimiento muy restringido de los límites implícitos. Ello es debido a que el hecho de que no sean notorios o expresos puede provocar un exceso interpretativo a la hora de dotarlos de significado.
[32] Al reconocerse el derecho de reunión y de manifestación en el art. 21 CE, se determina que ha de ser pacífica y sin armas; no es un límite en sí mismo, pero si no se cumple con ese requisito no entrará en juego la protección constitucional de dicho artículo.

señalar que: «no tiene carácter absoluto, pues puede estar sujeto a limitaciones y restricciones, que deben estar previstas por la ley en función de intereses que puedan ser considerados prevalentes según los criterios propios de un Estado democrático de Derecho. […] es preciso que, partiendo de la necesaria habilitación legal, existan datos que en cada caso concreto pongan de manifiesto que la medida restrictiva del derecho es proporcional al fin pretendido, que este fin es legítimo y que es necesaria en función de las circunstancias de la investigación y del hecho investigado. Ello implica una valoración sobre la gravedad del delito, sobre los indicios de su existencia y de la intervención del sospechoso, y sobre la necesidad de la medida»[33]. Si bien nos dice que, efectivamente, no tiene carácter absoluto, también nos introduce una nueva idea, un nuevo concepto: «los límites de los límites», valga la redundancia. Hablamos de requisitos o principios que han de cumplirse para poder limitar o restringir ese derecho al secreto de las comunicaciones.

Parece obvia la necesidad de restringir esas limitaciones respecto a los derechos fundamentales. El Tribunal Constitucional establece que se trata de «límites que habrá que ponderar en cada caso, pues en cuanto restringen derechos fundamentales, han de ser interpretados a su vez restrictivamente»[34].

En resumen: en la Constitución observamos un límite expreso al derecho al secreto de las comunicaciones (pues se puede restringir por medio de resolución judicial), que a su vez supone una autolimitación para la propia función de restricción, ya que nos está diciendo que tan sólo puede ser acotado por medio de esa resolución judicial. Además de este límite –que, como hemos dicho, se «autorrestringe» también a sí mismo– existen otros localizados fuera de la Constitución Española, tales como los sitos en el artículo 588 *bis* «a», apartado primero, de la Ley de Enjuiciamiento Criminal[35].

Respecto al ámbito internacional cabe mencionar que, si bien en la Declaración Universal de los Derechos Humanos no encontramos límite expreso alguno, en el art. 8.2 CEDH sí que se nos dice que «no podrá haber injerencia […] sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones

[33] STS de 19 de junio de 2013.
[34] STC 81/1983, de 10 de octubre.
[35] Hablamos de los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. Nos referiremos a los mismos con posterioridad en este trabajo.

penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás»[36]. Encontramos pues, tanto esa posibilidad de limitar el derecho cuando se cumplan ciertas circunstancias, como la enumeración de esos requisitos o principios que han de respetarse para poder ejercer dicha restricción, es decir, los límites de los límites.

3. LA ARROLLADORA EVOLUCIÓN TECNOLÓGICA: APARICIÓN DEL SITEL

3.1. El Estado de Derecho, un paso por detrás: necesidad de nuevas medidas

La sociedad ha estado siempre evolucionando, era tras era y siglo tras siglo. Ahora bien, los ritmos de este continuo e imparable desarrollo no han sido siempre los mismos; los avances tecnológicos de los últimos tiempos no son comparables, ni mucho menos, a los que han ido sucediéndose siglos atrás.

Muchas veces nos encontramos con situaciones en las que el Derecho no es capaz de seguir el ritmo de la realidad social y podríamos afirmar que, refiriéndonos al tema que nos ocupa, ésta sería una de ellas. Señalamos lo anterior debido a que hechos como la aparición de la telefonía y su posterior desarrollo, o la eclosión de Internet y su implacable expansión pocos años más tarde, no han tenido una respuesta satisfactoria en el marco normativo español.

Dicho lo cual podemos asegurar, sin miedo a equivocarnos, que la aparición de las nuevas tecnologías desbordó por completo las previsiones del legislador sitas en la Ley de Enjuiciamiento Criminal[37]. Tanto es así que hubo que esperar hasta el año 1988 para que dicha normativa reflejase en alguno de sus preceptos lo relativo a las comunicaciones telefónicas[38]; con anterioridad tan sólo se ocupaba de las de carácter postal o telegráfico, cuya utilización resulta ínfima tanto por el ciudadano de a pie como por aquél que delinque.

Si bien, como acabamos de mencionar, en el año 1988 se dio una respuesta normativa más o menos válida –aunque tardía– al tema de las vulgarmente conocidas como «escuchas telefónicas», ésta no ha tenido su reflejo con otras vías de comunicación más modernas. La sociedad continúa evolucionando y el Derecho ha

[36] Disponible en https://www.echr.coe.int/Documents/Convention_SPA.pdf
[37] Aprobada por el Real Decreto de 14 de septiembre de 1882 y actualizada, por última vez, en el año 2015.
[38] En virtud de la Ley Orgánica 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1988-12909

vuelto a quedarse atrás; finalmente, y de forma muy desafortunada, vemos cómo el legislador ha terminado por abandonar su función, cediéndosela a los tribunales[39] y diciendo «adiós» a principios tales como la reserva de ley.

La huida del legislador no ha de preocuparnos en exceso para el estudio de esta materia ya que, como hemos mencionado anteriormente, la reforma operada por la Ley Orgánica 4/1988, de 25 de mayo, se ocupa de las intervenciones telefónicas en el proceso penal. El art. 579.2 LECrim señalaba que «asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa»[40].

Sea como fuere, y una vez vista la enorme evolución tecnológica que ha golpeado a nuestra sociedad actual, podemos afirmar sin tapujos que los medios policiales de investigación han de caminar de la mano de tal desarrollo. Hemos de tener en cuenta que la intervención de las comunicaciones es una de las bazas más importantes para nuestras Fuerzas y Cuerpos de Seguridad en cuanto a la investigación de delitos se refiere, por lo que parece lógico –además de un hecho contrastado– el que los delincuentes utilicen las más modernas tecnologías a fin de evitar que sus comunicaciones sean interceptadas. «Inútil» o «anacrónico» serían dos adjetivos que quizá viniesen a nuestra cabeza si pensásemos en contrarrestar los medios de comunicación actuales con técnicas antiguas: «pinchar» un cable y volcar cientos y cientos de horas de conversaciones en cintas magnetofónicas[41], para luego escucharlas indiscriminadamente, no parece un buen método hoy en día.

Involuntariamente podemos pensar, al relacionar crimen y tecnología, en la delincuencia organizada. Es cierto que este tipo de delincuencia se caracteriza, en muchas ocasiones, por hacer uso de los medios técnicos más modernos a su alcance para la perpetración de sus actividades criminales con mayor facilidad, pero no es menos cierto el hecho de que, hoy en día, casi todo el mundo dispone de un teléfono inteligente o *smartphone*.

---

[39] Algo que hemos podido comprobar fácilmente en las primeras páginas de este trabajo, en las cuales hemos acudido a sentencias varias ante la inexistencia de preceptos legales que desarrollen este tema.

[40] Y utilizamos el pasado, «señalaba», pues dicho artículo ha sido objeto de reformas (véase la Ley Orgánica 13/2005, de 5 de octubre): hoy en día encontramos la regulación que nos interesa en los artículos 588 bis «a» y siguientes.

[41] Se trata de un medio de almacenamiento, capaz de almacenar distintos tipos de información como datos, audio o vídeo, cuya grabación se lleva a cabo sobre la banda plástica que posee gracias a un material magnetizado tal como óxido de hierro o distintos tipos de cromato.

3.2. El SITEL: concepto y origen

En un primer momento –cuando tan sólo teníamos telefonía fija– la intervención de comunicaciones telefónicas se basaba en el «pinchado» físico de sus redes. Había que trasladarse hasta determinado lugar para, a través de la manipulación de la línea, comenzar a grabar las conversaciones. Con la aparición de la telefonía móvil analógica se comenzó a interceptar dichas comunicaciones vía radio, siendo aún necesaria cierta proximidad con el objetivo en cuestión. Finalmente aparece la telefonía digital GSM[42] y, si bien en un principio se interceptaba desviándola a una línea fija, pronto apareció el instrumento objeto de este trabajo.

Con el fin de paliar las carencias que derivaron de la revolución tecnológica y ante unos instrumentos cada vez más modernos en manos de los delincuentes, surge el SITEL o Sistema Integrado de Interceptación Legal de Telecomunicaciones. Esta herramienta tiene capacidad no sólo para realizar escuchas telefónicas, sino que es capaz de geolocalizar[43] un aparato determinado –esté o no en el transcurso de una conversación telefónica–, así como de apropiarse de una gran cantidad de datos accesorios, tales como el número IMEI[44], la duración de las llamadas o los mensajes de texto.

La mecánica de este sistema se basa en el enlace entre centros de monitorización y las propias redes de los operadores de telecomunicaciones. Dichas redes ya cuentan con las facilidades pertinentes para aunar la información recibida en esos centros, en los cuales se procesará la misma y se pondrá a disposición del juzgado correspondiente. Veremos el funcionamiento de este sistema con mayor exactitud en el punto siguiente.

Como bien expuso BARRADO CASADO, antes de la entrada en juego del SITEL el número de interceptaciones no era muy voluminoso, pues éstas estaban acotadas; hay que tener en cuenta que había una serie de líneas de desvío, así como un número limitado de equipos a disposición policial. Además, el hecho de que tan sólo se pudiese grabar la voz, sin la posibilidad de hacerse con datos tales como los dispuestos

[42] *Global System for Mobile communications* o sistema global para las comunicaciones móviles. Para más información, véase https://es.wikipedia.org/wiki/Sistema_global_para_las_comunicaciones_móviles
[43] Para más información, véase http://kzgunea.blog.euskadi.eus/blog/2017/03/31/geolocalizacion-que-es/
[44] Se trata de un identificador único con el que cuenta cada *smartphone*. Está formado por quince dígitos (en ocasiones catorce) y nos aporta información tal como el país de fabricación, el fabricante del dispositivo o el número de serie. Con este número IMEI puede incluso bloquearse el teléfono en casos de pérdida o robo.

en el párrafo anterior, resultaba ser una pérdida de información para las Fuerzas y Cuerpos de Seguridad del Estado que hoy en día sería juzgada como «dramática»[45].

El Sistema Integrado de Interceptación Legal de Telecomunicaciones fue diseñado por la empresa danesa *ETI A/S*, experta en desarrollar soluciones informáticas para fuerzas policiales. Lo hizo en virtud de un encargo del Ministerio de Interior (2001), bajo el Gobierno de José María Aznar y con la firma de Mariano Rajoy, por aquel entonces Ministro de Interior.

Por dicho mandato se desembolsó una cantidad cercana a los diez millones de euros (9.825.975 €)[46]. Entró en funcionamiento en el año 2004, si bien la idea era que lo hiciera un año antes[47]. No estuvo plenamente operativo hasta 2005.

4. FUNCIONAMIENTO DEL SITEL: RASGOS TÉCNICOS Y PROCEDIMENTALES

4.1. Estructura técnica del sistema

Para hablar sobre el funcionamiento del SITEL de forma adecuada hemos de hacer mención, obligatoriamente, a su estructura[48].

En primer lugar tendríamos las redes de los operadores de telecomunicaciones, que recopilan la información objeto de investigación. Hay que dejar claro desde el primer momento que son los propios operadores los que compilan esa información.

Tras ello, ésta se envía a un centro de monitorización situado en Madrid[49], donde se procesarán y almacenarán las comunicaciones que hayan sido objeto de interceptación, es decir, las conversaciones en sentido estricto: los archivos de audio, los mensajes de texto, etcétera. Junto a éstas, se anexarán las informaciones accesorias o vinculadas a las mismas, sobre las cuales ya hemos hablado con anterioridad: los números de teléfono y de IMEI, las fechas y horas, la duración de las llamadas…

---

[45] BARRADO CASADO, M. A., «La captación de datos e intervención de las comunicaciones. Una visión técnico policial», *Interceptación de las comunicaciones y nuevas tecnologías*, Cuadernos Digitales de Formación, Consejo del Poder Judicial, Madrid, 2010, n.º 43, p. 131.

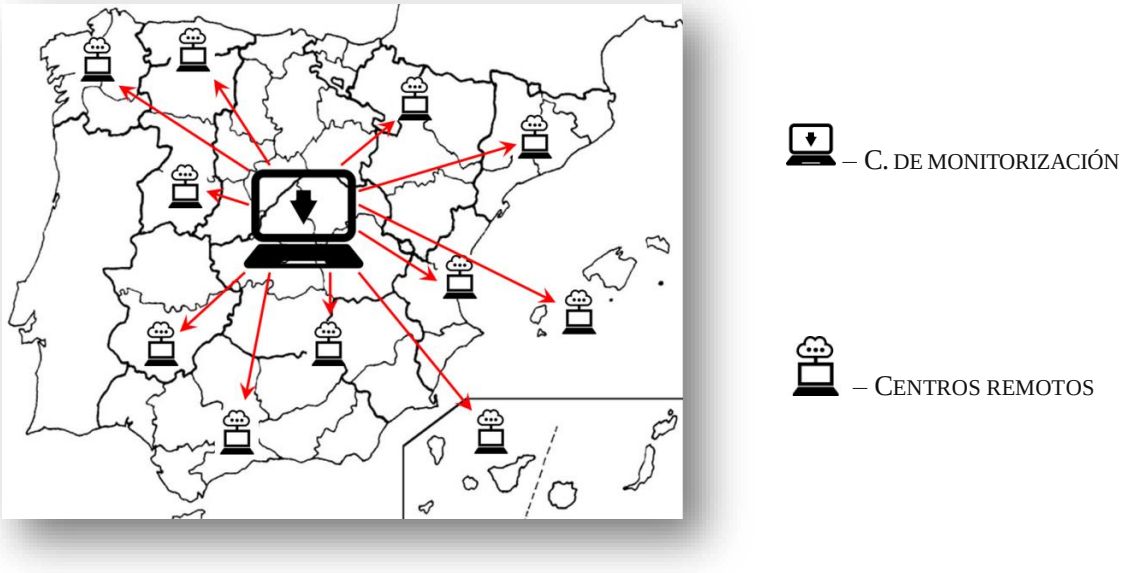
[46] Aunque otras tras fuentes indican cantidades mayores, cercanas a los trece millones de euros.

[47] CASTILLEJO MANZANARES, «R. Medios de Investigación en la lucha contra la criminalidad organizada. SITEL», *Revista General de Derecho procesal* [en línea], Iustel, 2012, n.º 27, p. 13 [consulta: 02/04/2018]. Disponible en: http://www.iustel.com/v2/RevIstas/detalle_revista.asp?id_noticia=411909

[48] FERNÁNDEZ FERNÁNDEZ, F., «El sistema policial de interceptación de las comunicaciones: SITEL», *La interceptación de las comunicaciones telefónicas y telemáticas* [en línea], CEJ, 2016, p. 6 [consulta: 05/04/2018]. Disponible en: http://www.cej-mjusticia.es/cej_dode/flash/ebook/assets/img/cejponencia1470209527604/cejponencia1470209527604.pdf

[49] Realmente hay dos centros de monitorización, similares pero independientes: uno funciona en el ámbito del Cuerpo Nacional de Policía y otro en relación a la Guardia Civil, estando ambos en Madrid. Cabe resaltar que el SITEL también es utilizado por el Centro Nacional de Inteligencia.

Para finalizar tendríamos los «centros remotos», que no son más que salas de monitorización distribuidas por toda la geografía española. En estas salas los agentes autorizados tomarán la información interceptada y harán uso de ella; CASTILLEJO MANZANARES los denomina «agentes facultados», definiéndolos como «aquellos agentes que se encargan de recepcionar y transmitir a la autoridad judicial la información que a su vez le facilite el operador de telecomunicaciones»[50].



El Tribunal Supremo afirma que el SITEL no sólo se basa en una relación triangular, sino que también se articula en torno a tres principios.

a) El primero sería el de centralización, según el cual el centro de monitorización se encuentra localizado en una sede principal o central, como ya hemos visto.

b) Tras éste, estaría el principio de seguridad, que podemos dividir en dos niveles: el primero haría referencia al centro de monitorización principal, el cual cuenta con un nivel extremo de seguridad, así como con trabajadores de mantenimiento formados específicamente; por otro lado tendríamos los aparatos periféricos o centros remotos, cuyo acceso está protegido por claves de usuario, contraseñas y un sistema de conexión de alta seguridad.

c) Como último criterio estaría la automatización, en virtud del cual se pretende reducir costes y espacio de almacenamiento, ganar en seguridad y contar con un sistema capaz de evolucionar[51].

[50] CASTILLEJO MANZANARES, R., «Medios de investigación…», *Revista General...*, op., cit., p. 19. Véase también la definición de «agente facultado» del artículo 84 del Real Decreto 424/2005, de 15 de abril.
[51] STS de 13 de marzo de 2009.

4.2. La interceptación legal de comunicaciones: concepto

Lo primero que hemos de preguntarnos es qué entendemos por «interceptación legal de las comunicaciones».

Encontramos una primera definición en el art. 84 del Real Decreto 424/2005, de 15 de abril[52]. Según esta disposición, se trata de una «medida establecida por ley y adoptada por una autoridad judicial que acuerda o autoriza el acceso o la transmisión de las comunicaciones electrónicas de una persona, y la información relativa a la interceptación, a los agentes facultados, sin perjuicio de lo establecido en el artículo 579.4 de la Ley de Enjuiciamiento Criminal». Podemos apreciar rápidamente que, si bien este Real Decreto continúa en vigor, su remisión al art. 579.4 LECrim necesita de una actualización tras la reorganización de dicha Ley a manos de la LO 13/2005[53].

Por otra parte, LÓPEZ FRAGOSO define la interceptación legal de comunicaciones de una manera, a mi juicio, más completa: se refiere a «aquellas medidas instrumentales restrictivas del derecho fundamental al secreto de las comunicaciones privadas, ordenadas y ejecutadas en la Fase Instructora de un proceso penal bajo la autoridad del órgano jurisdiccional competente, frente a un imputado, u otros sujetos de los que éste se sirva para comunicarse, con el fin de, a través de la captación del contenido de lo comunicado o de otros aspectos del proceso de comunicación, investigar determinados delitos, averiguar al delincuente y, en su caso, aportar al juicio determinados elementos probatorios»[54].

Así mismo, tenemos la aportación de GIMENO SENDRA, según el cual se trata de «todo acto de investigación, limitativo del derecho fundamental al secreto de las comunicaciones, por el que el Juez de Instrucción, en relación con un hecho punible de especial gravedad y en el curso de un procedimiento penal, decide, mediante auto especialmente motivado, que por la policía judicial se proceda al registro de las llamadas y/o a efectuar la grabación magnetofónica de las conversaciones telefónicas del imputado durante el tiempo imprescindible para poder preconstituir la prueba del hecho punible y la participación de su autor»[55].

---

[52] Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios. Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2005-6970

[53] Hoy en día este artículo tan sólo indica cuándo no necesitaremos autorización en el ámbito de la correspondencia.

[54] LÓPEZ-FRAGOSO ÁLVAREZ, T., *Las intervenciones telefónicas en el proceso penal*, COLEX, Madrid, 1991, pp. 12 y ss.,

[55] GIMENO SENDRA, J. V., *Derecho procesal penal*, Civitas, Navarra, 2012, p. 476.

A lo largo del trabajo hemos ido esbozando la idea de que el concepto de intervención legal de las comunicaciones no es nuevo; a su vez, ha quedado patente que su escenario sí que ha cambiado de forma trascendental. Las definiciones, algunas relativamente antiguas, siguen siendo válidas dado que la esencia de la interceptación no cambia, pero sí que varía la forma de proceder –que veremos sin más dilación– y los medios técnicos para llevarla a cabo, todo ello en tanto en cuanto evoluciona la tecnología en su conjunto.

4.3. Rasgos procedimentales de la interceptación legal de comunicaciones

En virtud de lo dispuesto hasta el momento, y encaminándonos ya hacia el estudio del procedimiento en sí mismo, decir que nos situaremos ante un mecanismo bien ordenado, sometido a esa doble tríada de sujetos y principios mencionados en el punto anterior, e irremediablemente necesitado de la cooperación diligente de los operadores de telecomunicaciones.

4.3.1. Solicitud de los datos identificativos

El inicio del procedimiento tendría lugar al solicitar los datos de identificación de aquellos sujetos a investigar a fin de introducirlos en la petición al órgano judicial. Dicha petición partiría de las Fuerzas y Cuerpos de Seguridad del Estado e iría destinada al operador, el cual se encuentra en la obligación de cooperar[56].

El art. 89.1 del ya citado Real Decreto 424/2005, de 15 de abril[57], nos habla de la información previa a la interceptación: «los sujetos obligados […] pondrán a disposición de la autoridad que lleve a cabo dicha investigación, con carácter previo a la interceptación legal, información actualizada relativa a los datos a que hace referencia el artículo 90». Este artículo 90 al que se nos remite enumera, entre otras, las siguientes informaciones: la identificación del abonado, la ubicación del punto de terminación de la red[58] o una identificación del mismo.

Aún situados ante el art. 89 del Real Decreto 424/2005, exponer que su apartado segundo declara que los operadores facilitarán información sobre los servicios que otorgan a los sujetos objeto de la medida de interceptación, así como –si es posible– sus nombres,

[56] Véanse los sujetos obligados a cooperar en el art. 85 del Real Decreto 424/2005, de 15 de abril.
[57] […] por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios.
[58] Con «punto de terminación de red» nos referimos a un cajetín, cuyas medidas suelen ser de unos siete centímetros de largo por cinco de ancho, que separa la red propia o interior del usuario de la común o exterior.

números de documento nacional de identidad, tarjeta de residencia o pasaporte y, si se tratase de personas jurídicas, la denominación o el código de identificación fiscal.

Cabe mencionar que encontramos una obligación similar en el contexto de la LECrim, pues ésta indica, en su art. 588 *ter* «e», que todos los operadores de telecomunicaciones han de colaborar. De hecho, éstos están «obligados a prestar al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones». Así mismo, habrán de guardar secreto y, de incumplir lo dispuesto en este párrafo, podrían incurrir en delito de desobediencia.

Sin embargo, si bien ambos artículos parecen tener un contenido similar, el artículo de la Ley de Enjuiciamiento Criminal, cuya rúbrica es «deber de colaboración», no funciona tan sólo en el marco de esta solicitud de datos identificativos, sino que opera en el proceso en su conjunto, imponiendo una obligación de cooperación que va más allá de esta primera fase. En cambio, del artículo 89 no emana una obligación generalizada, sino que se encuentra focalizado en la etapa que nos ocupa como bien se deduce de su título: «información previa a la interceptación».

4.3.2. Solicitud de la interceptación legal a la autoridad judicial y su concesión

En segundo lugar, las Fuerzas y Cuerpos de Seguridad del Estado procederían a solicitar la interceptación legal a la autoridad judicial correspondiente[59].

FERNÁNDEZ FERNÁNDEZ[60] nos remite a un informe de la Secretaría Técnica de la Fiscalía General del Estado, de 5 de octubre de 2005[61], en el cual se especifica lo siguiente: «es por ello que, para asegurar el adecuado ejercicio de la función que constitucionalmente corresponde a la autoridad judicial competente para autorizar medidas limitativas del derecho fundamental al secreto de las comunicaciones garantizando, no obstante, el mínimo sacrificio posible de dicho derecho, estimamos necesario que la solicitud policial de intervención telefónica, además de los datos y razonamientos que justifiquen la petición, concrete de forma específica, el sistema de interceptación que se estima conveniente utilizar, sus parámetros y la información

[59] En casos especiales el Ministerio Fiscal también podrá ser solicitante, aunque no lo trataremos debido a su ínfima trascendencia real. Véase el primer apartado del art. 588 *bis* «b» LECrim.
[60] FERNÁNDEZ FERNÁNDEZ, F., «El sistema policial…», *La interceptación...*, op., cit., p. 9.
[61] La Secretaría Técnica de la Fiscalía General del Estado apoya de forma continua al Fiscal General del Estado por medio de investigaciones, estudios o informes como el que nos ocupa. Éste, en concreto, recibe el título de «Consideraciones sobre el sistema SITEL de interceptación de comunicaciones».

susceptible de obtenerse en cada caso, a fin de que la autoridad judicial pueda resolver de forma razonada sobre todo ello y mantener el control que le corresponde asumir en la intervención».

En resumidas cuentas: la solicitud policial, aparte de la justificación de esa medida de interceptación, deberá adjuntar el concreto sistema de interceptación, el alcance del mismo, la información que se desea adquirir, etcétera; de esta manera se intenta evitar que la afectación o el daño al derecho al secreto de las comunicaciones sea desproporcionado respecto del fin perseguido, así como garantizar un mayor control por parte de la autoridad judicial.

El legislador español ha avanzado en esa dirección y, en la misma línea, la Ley de Enjuiciamiento Criminal, en su art. 588 *bis* «b», apartado segundo, establece que la petición a la autorización judicial deberá contener, necesariamente, las siguientes informaciones: «la descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales resulten conocidos; la exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 *bis* "a", así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia; los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida; la extensión de la medida con especificación de su contenido; la unidad investigadora de la Policía Judicial que se hará cargo de la intervención; la forma de ejecución de la medida; la duración de la medida que se solicita; [y, en último lugar,] el sujeto obligado que llevará a cabo la medida, en caso de conocerse».

Así mismo, el art. 588 *ter* «d» LECrim, en su apartado primero, nos dice que la solicitud deberá contener, además de lo dispuesto en el artículo que acabamos de tratar, los siguientes requisitos: «la identificación del número del abonado, del terminal o de la etiqueta técnica; la identificación de la conexión objeto de la intervención o los datos necesarios para identificar el medio de telecomunicación de que se trate».

Finalmente, y en virtud del art. 588 *bis* «c» LECrim, el juez de instrucción autorizará o denegará por medio de un auto, el cual ha de ser motivado consecuentemente. El plazo del que dispondrá la autoridad judicial para tomar su decisión será de

veinticuatro horas, pero éste podrá ser mayor en el caso de que tenga dudas sobre cómo resolver, en cuyo caso solicitará más datos o la aclaración de los ya existentes en la solicitud.

El apartado tercero del último precepto al que hemos hecho referencia enumera los datos que, como mínimo, ha de contener dicha autorización judicial. Si bien no los transcribiremos por ser la mayoría de ellos similares a los sitos en el art. 588 *bis* «b», sí creo oportuno mencionar, a fin de posteriores referencias en este trabajo, la obligatoriedad de dejar patente la duración de la medida en la autorización judicial[62].

Como resultado, si la solicitud por parte de las Fuerzas y Cuerpos de Seguridad cumple con lo dispuesto hasta ahora y la autoridad judicial lo considera pertinente, se concederá la autorización para llevar a cabo la interceptación legal de comunicaciones. Si así sucediese, pasaríamos a la siguiente fase del procedimiento.

4.3.3. Comunicación al operador de la orden de interceptación legal

Hablaríamos ya, en tercer lugar, de trasladar al operador de telecomunicaciones esa orden de interceptación, anexando la autorización que se ha conseguido en la fase anterior. Es necesario recordar que, como ya hemos mencionado y con fin de no afectar en exceso a ese derecho al secreto de las comunicaciones, se procederá a especificar o acotar determinados datos a conseguir, evitando así una especie de carta de libertad que justifique la recopilación indiscriminada de información.

El operador responderá a dicha solicitud afirmando haber recibido la orden judicial y estableciendo cuándo comenzará la interceptación. Acerca de esto último, aclarar que normalmente el inicio es casi instantáneo, pues el mandato judicial no suele posponer la entrada en funcionamiento de la interceptación. De haber cualquier tipo de retraso, éste tan sólo estaría justificado en tanto en cuanto sea producto de dificultades reales en las gestiones técnicas por parte de los operadores, jamás por razones de otra índole.

4.3.4. La interceptación legal de comunicaciones

Una vez cumplidas las fases anteriores, estaremos ante el comienzo de la interceptación legal en sí misma. Durante esta etapa, las informaciones que emanen de dicha interceptación –tanto las propias comunicaciones como los datos accesorios que

[62] Para lo demás nos remitimos al artículo 588 *bis* «b» de la Ley de Enjuiciamiento Criminal.

hayan sido considerados merecedores de adquisición en pos del éxito de la investigación– serán transferidas al centro de monitorización, donde serán almacenadas y procesadas. Posteriormente viajarán hasta el centro remoto correspondiente, donde el agente facultado tendrá acceso a ellas y hará uso de las mismas.

Hay que tener en cuenta un rasgo importante respecto del envío de las comunicaciones, aunque después lo trataremos en profundidad: se envían en formato de «sólo lectura»[63], lo que supone que los agentes no puedan alterarlas.

Una vez llegados hasta este punto podemos preguntarnos qué informaciones se pueden recopilar. Con ánimo meramente explicativo, partimos de la Resolución COM 96/C 329/01[64], según la cual nuestras fuerzas policiales pueden hacerse con los siguientes elementos, a título de ejemplo: señal de entrada, números telefónicos tanto del receptor como del emisor –sin la necesidad de que se llegue a establecer la conexión–, señales tales como el desvío de llamadas, el inicio y el fin de las comunicaciones –junto con su duración, obviamente– y, en último lugar, la localización del aparato[65]. A estos elementos sitos en el glosario hemos de sumar alguno más, como los números IMEI tanto del teléfono investigado como de los que se pongan en contacto con el mismo, la identidad de los titulares, el repetidor en uso, información contenida en el dispositivo tal como carpetas de audio o contactos guardados, etcétera.

Si acudimos al art. 88 del Real Decreto 424/2005 encontramos una enumeración más detallada. En esta disposición, que lleva por rúbrica «información relativa a la interceptación», vislumbramos todas aquellas informaciones que los operadores de telecomunicaciones están obligados a transferir a los agentes facultados, siempre y cuando así lo disponga la autorización judicial. Entre ellas estarían, por ejemplo, el número de cuenta asignada por el proveedor de servicios de Internet o el correo electrónico del sujeto investigado.

Esta lista no la he añadido con el ánimo de exponer unos *numerus clausus* o unas categorías tasadas, ya que la tecnología sigue evolucionando y quizá, dentro de unos años, este sistema se vea obligado a ir un paso más allá y recopilar datos hasta ahora

[63] No confundir con la memoria de sólo lectura. Véase https://es.wikipedia.org/wiki/Memoria_de_solo_lectura
[64] Anexo de la Resolución COM 96/C 329/01 del Consejo de la Unión Europea, de 17 de enero de 1995. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31996G1104&from=ES
[65] A lo cual se hace referencia en el mismo Anexo, aunque de una forma un tanto enrevesada; nos habla de «interfaces de interceptación» en el punto quinto del glosario.

inexistentes; aún así, nos sirve para darnos cuenta del alcance del SITEL y del tipo de informaciones que se extraen, con relativa asiduidad, gracias a éste[66].

4.3.5. Terminación de la interceptación legal y traslado de la información

En cuanto a la terminación de la interceptación legal, diremos que ha de ser comunicada al operador. Éste, posteriormente, deberá confirmar el cese de la misma.

Este cese puede producirse por el transcurso del período de tiempo especificado en el auto judicial o, también, por el esclarecimiento de los hechos investigados[67], en cuyo caso estaríamos ante otro mandato judicial. CASANOVA MARTÍ habla de una tercera posibilidad, la relativa a la desaparición de las circunstancias por las cuales se autorizó dicha interceptación[68].

El art. 588 *ter* «g» LECrim establece tres meses, a contar desde la fecha de autorización por parte de la autoridad judicial, como la duración máxima inicial de la intervención. Esto no quiere decir que la interceptación legal de comunicaciones no pueda superar esos tres meses, sino que el génesis de dicha medida de investigación, es decir, la autorización judicial, no podrá establecer un plazo mayor *a priori*.

Siendo así, ¿cómo es posible superar esos tres meses? Tal cosa se posibilitará mediante la existencia de prórrogas; el mismo artículo señala que esos tres meses serán «prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses». Si acudimos al art. 588 *ter* «h» LECrim veremos cómo a la hora de solicitar dicha prórroga, la Policía Judicial deberá aportar pasajes de las conversaciones con el fin de probar dos cosas: que, efectivamente, la medida está surtiendo efecto; y, como consecuencia obvia de lo anterior, que sería necesario y satisfactorio para los fines de la investigación no interrumpir dicha interceptación.

Por otro lado, y además de lo expuesto hasta ahora, cabría tanto una ampliación –prorrogando el plazo inicialmente dado– como un cambio de criterios –ampliando la orden de interceptación al añadir, por ejemplo, la geolocalización–. Estas acciones no pondrían fin a la interceptación legal pero sí que supondrían la terminación de esos parámetros iniciales en virtud de los que fue concebida.

[66] Para más información, nos remitimos al Anexo I de este trabajo, donde se establece una enumeración de las informaciones accesibles a este respecto.
[67] Véase la STS de 15 de julio de 2013, según la cual el juez «podrá ordenar el cese en el momento en que claudiquen los motivos que la determinaron» a fin de no afectar de forma excesiva al artículo 18.3 CE.
[68] CASANOVA MARTÍ, R., *Las intervenciones telefónicas en el proceso penal*, J.M. Bosch Editor, Barcelona, 2014, p. 241. Véase también el art. 588 *bis* «j» LECrim, relativo al cese de la medida.

Para finalizar, se dará traslado al órgano judicial respecto de las informaciones recopiladas que resulten pertinentes. Cabe mencionar que la forma de entrega será siempre en formato CD o DVD; profundizaremos sobre este asunto en el siguiente punto.

4.4. La información en su última etapa: garantías y admisibilidad probatoria

4.4.1. La recepción por la autoridad judicial y sus garantías: la firma electrónica

Pongámonos en la siguiente situación: el operador de telecomunicaciones, cumpliendo mandato judicial, envía la información al servidor central del SITEL. Se lleva a cabo el proceso anteriormente expuesto y las grabaciones telefónicas realizadas pasan al CD o DVD en cuestión[69], con el fin de trasladar el resultado de las investigaciones al órgano judicial. Si bien la pérdida de información[70] en este tipo de formatos no es algo que ocurra con frecuencia, descartarla por completo sería, quizá, algo aventurado; puede haber una anomalía en el soporte, producirse un fallo en el grabado, un daño físico en la superficie del disco, un error humano a la hora de su reproducción o, por qué no, podría mediar dolo. Por estas y otras razones, tanto de carácter técnico como procedimental, la información se almacenará en el centro de monitorización hasta que el órgano judicial ordene su destrucción[71].

Yendo más allá, y haciéndonos caso de lo dicho hasta el momento, podrían surgir más que razonables dudas sobre las garantías que nos llega a ofrecer este sistema: ¿cómo estar seguros de que en el CD o DVD consta el contenido íntegro y no ha habido ningún tipo de alteración? En cuanto a las primeras fases del procedimiento no hay discusión entre la doctrina, pues los elementos de seguridad en la relación entre operadores de telecomunicaciones y centro de monitorización se tornan en apariencia indiscutibles. Ahora bien, tal como expone CASTILLEJO MANZANARES, «el sistema quiebra en lo que se refiere a la relación con el Juzgado, al no arbitrarse un interfaz seguro entre éste y el Servidor Central del agente facultado donde se recibe la comunicación intervenida de la operadora para comprobar la integridad de la comunicación y discrepar de la presunción de autenticidad del CD/DVD, el que se vuelca por el agente facultado el archivo informático para entregarlo al Juzgado»[72].

---

[69] CD y DVD de tipo WORM: *write one, read many*, conocidos como «soportes no repudiables».
[70] El CD o DVD de mayor calidad del mercado no suele superar los diez años de durabilidad, aunque éste ni siquiera se utilice. Incluso las partículas del polvo, una nimiedad a nuestros ojos, se tornan enemigas acérrimas cuando hablamos de estos soportes, pudiendo reducir su durabilidad de forma considerable.
[71] SSTS de 5 y 12 de noviembre de 2009.
[72] CASTILLEJO MANZANARES, R. «Medios de investigación…», *Revista General...*, op., cit., p. 27.

En este ambiente de cierta desconfianza, y con el objetivo de paliar la misma, surge la firma electrónica[73]. Este proceso no consiste en la incorporación de la firma por parte del agente, sino que se hace por la misma máquina y de forma desasistida, es decir, sin la intervención de persona alguna[74]. La autenticidad del contenido, por tanto, no depende de la presumida diligencia del agente al cargo, sino del sistema en sí mismo e, indirectamente, de los prestadores de servicios de certificación[75].

En consecuencia, el agente se limita a volcar el fichero con la información en el CD o DVD en cuestión, fichero que ya vendrá con la firma electrónica incorporada. Ese mismo soporte es el que se entrega a la autoridad judicial, con la precisión formal de que se hará en un archivo ejecutable por cualquier ordenador a fin de poder practicar fácilmente la prueba y verificar la autenticidad de la misma sin dilaciones indebidas. En consonancia con lo dispuesto hasta el momento, podemos afirmar que el proceso de firma electrónica que se lleva a cabo en el marco operacional del SITEL es sinónimo de garantía, habiendo recibido el visto bueno del Ministerio de Industria[76].

Nos reafirmamos en lo anterior debido a que la firma electrónica no sólo significa la imposibilidad de alterar la información, sino que además implica la integridad del contenido. Podríamos pensar que, si bien es imposible modificar la información, el agente facultado podría obviar determinados datos sitos en el centro de monitorización y no dar parte de éstos a la autoridad judicial. Sin embargo, esto no es posible: el Tribunal Supremo manifestó que «la firma electrónica garantiza igualmente que lo grabado en el soporte entregado es precisamente el contenido íntegro de lo que consta en el ordenador central, y que no puede ser posteriormente alterado»[77]. Un hipotético intento de falsear la información pasaría, obligatoriamente, por la creación de ficheros falsos; en estos casos siempre cabrá el acudir a la información primigenia que, como ya hemos dicho, permanecerá en el centro de monitorización.

---

[73] Se trata de un acervo de datos que acompañan a un archivo de carácter electrónico y en virtud del cual se identifica al autor de la firma y se asegura la integridad del documento en cuestión. Podríamos decir que este método es al archivo o documento electrónico lo que la firma manuscrita es al documento físico.

[74] FERNÁNDEZ FERNÁNDEZ, F., «El sistema policial…», *La interceptación...*, op., cit., p. 15.

[75] Estos «prestadores de servicios de certificación» llevan a cabo certificados electrónicos, los cuales vinculan cada instrumento de firma electrónica con la identidad del usuario que hace uso del mismo. No vale cualquier firma electrónica, sino que se ha de cumplir con lo estipulado en los artículos 28 y siguientes del Reglamento n.º 910/2014 (UE) del Parlamento Europeo y del Consejo, de 23 de julio, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

[76] Respecto a la regulación general de la firma electrónica, véase la Sección 4.ª del ya citado Reglamento (UE) n.º 910/2014, de 23 de julio, así como la Ley 59/2003, de 19 de diciembre, de firma electrónica.

[77] STS de 7 de junio de 2011.

Antes de entrar en cuestiones procesales, hemos de decir que a efectos legales y en virtud del artículo 26 del Código penal[78], este tipo de soporte tendrá la consideración de «documento». En la misma línea se expresó el Tribunal Supremo al declarar que «el concepto de documento no puede reservarse y ceñirse en exclusividad al papel reflejo y receptor por escrito de una declaración humana […]; un disco o una cinta magnetofónica, los disquetes informáticos, portadores de manifestaciones y acreditamientos, con vocación probatoria, pueden ser susceptibles de manipulaciones falsarias al igual que el documento escrito»[79].

Por su parte, el artículo 3.5 de la Ley 59/2003[80] nos dice que «se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado». Su trascendencia es, para nosotros, más bien escasa, ya que su tratamiento es similar al del documento tradicional.

4.4.2. Admisibilidad y carga de la prueba: posiciones doctrinales encontradas

La opinión generalizada respecto a la autenticidad ofrecida por el SITEL es claramente favorable. Si bien encontramos distintos mecanismos dedicados a ésta, la garantía más importante es la firma electrónica. A este respecto y de acuerdo al mismo, la Agencia Española de Protección de Datos[81] declaró que los «procedimientos de firma electrónica implantados en el momento en que la información se incorpora al sistema, su grabación en otros soportes y su transmisión a la autoridad judicial, garantizan los principios de exactitud e integridad previstos en la LOPD»[82].

Sin embargo, a raíz del voto particular formulado en la STS de 30 de diciembre de 2009[83], surge un sector que, reticente de la autenticidad que emana del SITEL, expone su criterio: «[la credibilidad del SITEL] no puede consistir en un acto de fe inspirado por las excelencias del software del que se valen los agentes».

---

[78] Artículo 26 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código penal: «a los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica».
[79] STS de 19 de abril de 1991.
[80] […] de 19 de diciembre, de firma electrónica. Disponible en http://noticias.juridicas.com/base_datos/Admin/l59-2003.t1.html
[81] Organismo público con sede en Madrid y cuya fecha de creación data de 1993. Su cometido es velar por el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Desde 2015 está siendo dirigida por Mar España Martí, primera mujer en llegar a tal puesto.
[82] Véanse las conclusiones de su inspección sobre SITEL, de 19 de enero de 2010.
[83] Disponible en https://supremo.vlex.es/vid/-211683883. Esta línea crítica ha sido seguida por otros votos particulares posteriores, concretamente los dirigidos a las SSTS de 20 de enero y de 2 de octubre, ambas del año 2012, así como por la STS de 13 de julio de 2012.

De la misma manera se posicionan a la hora de establecer que «los DVD aportados a un proceso penal por agentes de policía no pueden aspirar a un régimen privilegiado frente a la autenticidad afirmable de esos mismos soportes electrónicos cuando tienen distinto origen»[84]. MARCHENA GÓMEZ, uno de los magistrados que formulan el voto particular, manifiesta que «la autenticidad de los DVD no puede situarse fuera de la órbita de las exigencias que son propias de toda fuente de prueba, sustituyéndose por una aceptación incondicional que carece en nuestro sistema de cobertura jurídica»[85]. Así mismo, tampoco se podría afirmar la presunción de autenticidad de los DVD en tanto en cuanto, según dicha posición crítica, la firma electrónica no es un instrumento que cumpla con los requisitos necesarios para ello.

Siendo así, para que esta presunción de autenticidad fuera posible, habría que exigir que, justo después de haberse realizado el proceso de grabación, una certificación autentificase los siguientes tres hechos: que, desde que se transfirieron los archivos hasta que los recibió el juzgado, el CD o DVD no haya sido abierto; que, en virtud de lo anterior, no haya habido riesgo alguno de alteración del contenido; y, en último lugar, que el garante de la integridad del archivo sea el agente facultado. Por tanto, y transcribiendo las palabras del Tribunal Supremo, «lo decisivo […] no son las características técnicas del disco sobre el que se vuelcan los datos, sino las garantías de sellado que acompaña a los soportes que son ofrecidos a la autoridad judicial»[86].

Como hemos podido vislumbrar, la principal desavenencia entre ambas posiciones doctrinales no es otra que el diferente grado de credibilidad que les ofrece el SITEL, lo cual repercute seriamente a la hora de establecer unos estándares sobre la responsabilidad de la carga de la prueba. Siendo así y situados ante la disconformidad de alguien que impugne alegando la alteración del contenido sito en el CD o DVD, ¿a quién le correspondería la carga de la prueba?

La corriente que podemos calificar como satisfecha con la seguridad y credibilidad que deriva del SITEL entendería que, al menos cuando estemos en presencia de esa firma electrónica, será aquél que alegue cualquier alteración en el contenido del

[84] Y ponen un ejemplo: «el DVD aportado por los agentes no puede gozar de una autenticidad, irrazonablemente aventajada, frente al DVD en el que se contienen, por ejemplo, escrituras públicas y está custodiado por un Notario».
[85] MARCHENA GÓMEZ, M., «Proceso penal: nuevos problemas, viejas soluciones», *La Ley Penal*, LA LEY, 2015, n.º 100, p. 8.
[86] STS de 13 de julio de 2012.

soporte el que deba probarlo. A este sujeto habría que exigirle, si bien no llegar a probar de manera completa su alteración, sí el crear una duda objetivamente razonable[87].

Por otra parte y de manera antagónica, se sostiene, en virtud del voto particular al que nos hemos referido con anterioridad, que «la atribución de eficacia probatoria a esos DVD –expresamente impugnados en su autenticidad por la defensa de uno de los recurrentes–, supone un retroceso respecto del estado actual de las garantías constitucionales. […] Nuestra respuesta no puede consistir en un acto de fe inspirado por las excelencias del software del que se valen los agentes. Tampoco podemos incorporar al objeto del debate el grado de confianza institucional que a la Sala le merezca el trabajo de las Fuerzas y Cuerpos de Seguridad del Estado»[88]. Sin embargo, a pesar de lo expuesto, se mantiene la opinión de que es necesario el planteamiento de una «duda fundada y razonable que haga precisa la necesidad de la prueba pericial o cotejo», es decir, no vale con una impugnación general o programática.

En opinión de RODRÍGUEZ LAINZ, estas cuestiones podrían hallar una solución si se exigiese la aportación al juzgado de «una serie de informaciones que permitieran realizar un contraste de autenticidad e inalterabilidad sin necesidad de entrar en el juego de impugnaciones más o menos fundadas»[89], que podrían ir incluidas en el mismo CD o DVD o, si se estima oportuno, en distinto soporte. A modo de ejemplo, podríamos nombrar las siguientes informaciones: la certificación de la fecha en que se genera el archivo –junto con su identificación numérica–, la identificación de los agentes con acceso al fichero, así como de los accesos en sí mismos[90].

Sea como fuere, y dejando de lado el duelo doctrinal, la posición prevalente y la que ha de interesarnos a efectos prácticos es la tomada por el Tribunal Supremo en su sentencia de 2 de octubre de 2012, según la cual «la posibilidad de manipulación o alteración es prácticamente imposible y en todo caso dejaría rastro informático de la misma»[91]. Y es que, si bien el voto particular tratado se me antoja de gran importancia a la hora de conocer esa contraparte en la opinión relativa al SITEL, no hemos de perder de vista que no es la dirección que el Tribunal Supremo –en la mayoría de los casos– ha

[87] RODRÍGUEZ LAINZ, J. L., «SITEL: nuevas tendencias, nuevos retos», *Diario La Ley*, LA LEY, 2013, n.º 8.082, p. 9.
[88] STS de 30 de diciembre de 2009.
[89] RODRÍGUEZ LAINZ, J. L., «SITEL: nuevas…», *Diario…*, op., cit., p. 12.
[90] Recopilaremos estas recomendaciones de RODRÍGUEZ LAINZ en el Anexo II del trabajo.
[91] Las informaciones que nos ocupan tan sólo podrían ser falseadas o modificadas por técnicas realmente avanzadas. Si aun así, tal cosa sucediese, aquél que modificar el contenido estaría obligado a ingresar en el sistema utilizando una contraseña y, por tanto, dejando de forma irremediable una huella en el sistema.

optado por tomar, ya que tanto en esa misma sentencia como en otras tantas[92], la corriente mayoritaria se ha pronunciado a favor del reconocimiento a las garantías del SITEL.

Dicho lo cual –y, en este caso, de acuerdo a ambas posiciones doctrinales–, si por la razón que fuese alguna de las partes realizase una impugnación, habría de motivar suficientemente tal acto. Esto cobra aún más sentido al pensar que, con esa alegación referente a la alteración del contenido, se está acusando, de forma más o menos directa, al agente facultado. En la hipótesis de que tuviera lugar la impugnación y de que ésta fuera de la mano con sospechas fundamentadas e indicios razonablemente objetivos, llevaría a la necesidad de cotejar la información sita en el soporte con la contenida en el centro de monitorización.

Podríamos pensar que todo esto sería fácilmente solucionable si contásemos directamente con los archivos originales y no con el volcado de los mismos realizado por el agente. La cuestión es que el núcleo del SITEL, su disco duro, está totalmente integrado en lo que conforma el centro de monitorización. Resulta prácticamente imposible trasladar dicho núcleo a la sede de la autoridad judicial, no ya sólo por las dificultades físicas o técnicas, que son enormes, sino porque supondría el cese del resto de interceptaciones.

Como consecuencia lógica de todo lo anterior podríamos dar un paso más y afirmar, ahora ya sí, que la autenticidad del SITEL es una presunción *iuris tantum*[93], pues «el sistema de escuchas telefónicas que se plasma en un documento oficial obtenido con autorización judicial y autenticado su contenido por la fe pública judicial goza de valor probatorio»[94]. Para ello podemos apoyarnos también en el artículo 318 de la Ley de Enjuiciamiento Civil[95], así como en varias sentencias del Tribunal Supremo[96].

Obvia y lógicamente, la posibilidad de impugnar siempre estará presente. Además, si una vez finalizado el proceso se demostrase, por el método que fuera, que ha habido una alteración del contenido de los CD o DVD, sería posible una revisión de la sentencia.

---

[92] Véase, entre otras, la STS de 6 de julio de 2010.
[93] Siempre con la posibilidad de alegar la no autenticidad del contenido del CD o DVD.
[94] STS de 30 de diciembre de 2009.
[95] Artículo 318 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil: «los documentos públicos tendrán la fuerza probatoria establecida en el artículo 319 si se aportaren al proceso en original o por copia o certificación fehaciente, ya sean presentadas éstos en soporte papel o mediante documento electrónico, o si, habiendo sido aportado por copia simple, en soporte papel o imagen digitalizada, conforme a lo previsto en el artículo 267, no se hubiere impugnado su autenticidad».
[96] Como ejemplo ilustrativo podemos quedarnos con la STS de 9 de julio de 2013.

5. ASPECTOS JURÍDICOS DEL SITEL

5.1. Cobertura legal

En primer lugar nos referiremos a la Resolución COM 96/C 329/01 del Consejo de la Unión Europea, de 17 de enero de 1995[97], texto que tratamos anteriormente al ejemplificar algunas de las informaciones que se podían recopilar por parte de las Fuerzas y Cuerpos de Seguridad del Estado. En dicha Resolución se establece que «la interceptación legalmente autorizada de las telecomunicaciones constituye un instrumento importante para la protección de los intereses nacionales y, en particular, para la seguridad nacional y la investigación de delitos graves».

En el cuerpo principal tan sólo encontramos algunas consideraciones como la que acabamos de ver, por lo que hemos de ir hasta su Anexo para ver las características más importantes de esta Resolución. Aparte de las informaciones accesibles a las que nos referimos en su momento, nos encontramos con –entre otras cosas– los requisitos que se han de cumplir para proceder a la interceptación legal de comunicaciones. No nos detendremos más en este cuerpo legal pues, como bien se establece en el mismo, siempre gozará de primacía el Derecho interno de los Estados[98].

En cuanto al Derecho nacional tenemos, en primer lugar, la ya derogada Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones[99]. Concretamente hay que hablar de su artículo 33, cuyo apartado segundo señalaba que «los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal[100] […] y en otras normas con rango de ley orgánica». Desde este segundo inciso en adelante podíamos encontrar una regulación superficial que había de ser completada por disposiciones tales como el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado en virtud del Real Decreto 424/2005, de 15 de abril.

---

[97] Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31996G1104&from=ES

[98] Y así se estipula al comienzo del Anexo: «estos requisitos se entenderán sin perjuicio del Derecho nacional y deberán interpretarse de acuerdo con las disposiciones nacionales aplicables».

[99] Disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2003-20253. Esta Ley surge a raíz de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Ésta, a su vez, disponible en https://www.boe.es/doue/2006/105/L00054-00063.pdf

[100] En su antigua redacción. Recordemos que tal artículo ha sido reformado por la Ley Orgánica 13/2005, de 5 de octubre.

Como ya hemos adelantado, la por entonces Ley General de Telecomunicaciones ya no se encuentra en vigor. Hemos de irnos hasta la Ley 9/2014, de 9 de mayo, para encontrar su homónima vigente. El artículo 39 de esta nueva ley sería el equivalente al 33 de la anterior; eso sí, a pesar de que el precepto parece tener un contenido similar en cada uno de sus apartados, hay cambios que, si bien no los desarrollaremos demasiado, sí son merecedores de una breve mención.

En la nueva ley se añade un apartado en el octavo ordinal, lo cual supone que los incisos posteriores no coincidan con la numeración anterior. Sea como fuere, la redacción que se le da a este nuevo apartado es la siguiente: «los sujetos obligados deberán facilitar al agente facultado, de entre los datos previstos en los apartados 5, 6 y 7 de este artículo, sólo aquéllos que estén incluidos en la orden de interceptación legal». Esta novedad trata de remar hacia una mayor protección del derecho al secreto de las comunicaciones en el proceso de interceptación pues, si bien los apartados quinto, sexto y séptimo establecen las informaciones que los operadores han de transmitir a los agentes –o, más bien, al centro de monitorización–, sólo estarán obligados a hacerlo respecto a aquéllas incluidas de forma expresa en la orden de interceptación legal[101].

Esto nos recuerda, irremediablemente, a algo que ya tratamos tiempo atrás. FERNÁNDEZ FERNÁNDEZ nos remitía a un informe de la Secretaría Técnica de la Fiscalía General del Estado, de 5 de octubre de 2005, según el cual se ha de caminar en pos de buscar el menor sacrificio posible del derecho al secreto de las comunicaciones. Esto se podía lograr, según dicho informe, si «la solicitud policial de intervención telefónica, además de los datos y razonamientos que justifiquen la petición, concrete de forma específica, el sistema de interceptación que se estima conveniente utilizar, sus parámetros y la información susceptible de obtenerse en cada caso»[102].

Pero hemos de tener algo en cuenta, y es que en lo relativo a la regulación del SITEL hay un importante punto de inflexión. Concretamente nos referimos a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[103].

Antes de esta Ley, el artículo 33 de la Ley 32/2003 apenas tenía contenido. Para encontrar una regulación algo desarrollada había que ir hasta el Reglamento aprobado

[101] Esto tiene matices, como veremos en el Anexo I; hay informaciones que siempre son transferibles.
[102] FERNÁNDEZ FERNÁNDEZ, F., «El sistema policial…», *La interceptación...*, op., cit., p. 9.
[103] Disponible en http://noticias.juridicas.com/base_datos/Admin/l25-2007.html

por el Real Decreto 424/2005[104]. Debido a esto, y estimándose que la regulación del SITEL no podía establecerse de esa manera, sino que debía ir de la mano de una ley orgánica, se planteó un recurso contencioso-administrativo ante el Tribunal Supremo sobre el Capítulo II del Título V de dicho Reglamento[105]. El citado recurso se presentó el 29 de junio de 2005 y corrió por cuenta de la Asociación de Internautas[106].

Los recurrentes alegaban que, debido a la multitud de datos que los operadores estaban obligados a facilitar a los agentes facultados (identificación personal, domicilio, correo electrónico…), dicha cesión de información podía ir en contra no sólo del derecho al secreto de las comunicaciones, sino también del derecho a la intimidad personal[107]. En consecuencia, y según lo establecido en el artículo 81.1 CE[108], la regulación debería haberse articulado mediante una ley orgánica.

Tiempo después llegó la Ley 25/2007, de 18 de octubre, cuya disposición final primera modificaba el artículo 33 de la Ley 32/2003, anteriormente citado, es decir, el futuro artículo 39 de la Ley 9/2014. Lo que hizo fue coger parte del contenido del Reglamento y lo traspasó a la Ley 32/2003. Este trasvase, que incluyó a los artículos del 86 al 89, 95 y 96, supuso elevar el rango normativo de la regulación: lo que antes se apoyaba en las disposiciones del Reglamento ahora lo haría en la Ley 32/2003 y, más tarde, en la Ley 9/2014.

Cabe decir, respecto del recurso presentado contra el Capítulo II del Título V del Reglamento, que fue desestimado. El Tribunal Supremo entendió la no precariedad de la cobertura legal del SITEL al estimar que las Leyes de Enjuiciamiento Criminal y reguladora del Centro Nacional de Inteligencia[109], ambas orgánicas, regulaban de forma suficiente cuándo era legítima la interceptación de comunicaciones y cómo había que llevarla a cabo para que así lo fuese. Entienden, por tanto, que no se debe exigir la reserva de ley orgánica para todo lo relacionado con las interceptaciones: «la reserva de Ley

[104] […], de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.
[105] Lleva por rúbrica «la interceptación legal de las comunicaciones» y está formado por diecinueve artículos.
[106] Creada en España el 10 de octubre de 1998, se trata de una asociación sin ánimo de lucro cuyo objetivo principal era la reivindicación de una tarifa plana –o algo equivalente– asequible para todo el mundo. Para más información, véase https://www.internautas.org/pagweb/2.html
[107] Art. 18.1 CE: «se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen».
[108] Art. 81.1 de la CE: «son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución».
[109] Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. Al hablar del Centro Nacional de Inteligencia, más conocido como CNI, nos referimos al servicio de inteligencia español, sucesor del denominado Centro Superior de Información de la Defensa o CESID.

orgánica, sin embargo, no tiene por qué extenderse a todas y cada una de las cuestiones accesorias o instrumentales relacionadas con dichas interceptaciones […]. La Ley ordinaria puede, a nuestro juicio, regular y especificar los aspectos propiamente técnicos, operativos e instrumentales de la interceptación (pues resulta obvio que ha de contemplar, para ser eficaz, el desarrollo de las nuevas tecnologías) siempre que al hacerlo no invada el ámbito del derecho fundamental protegido por la reserva de ley orgánica»[110].

En resumen: la regulación del SITEL, diseminada en distintos textos, esquiva –malamente– las críticas provenientes de algunos sectores que manifiestan la existencia de un déficit normativo. Resulta imposible referirse a la cobertura legal del SITEL sin citar una retahíla de normas: la Ley General de Telecomunicaciones, el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas […], la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones…, y todo ello sin olvidarnos, por supuesto, de lo contenido en la Ley de Enjuiciamiento Criminal y, con menor trascendencia, en la Ley reguladora del Centro Nacional de Inteligencia.

Una vez dicho esto, resulta comprensible –se comparta o no– la posición de MARTÍNEZ FERRIZ[111]. Éste afirma que el SITEL no está conveniente regulado ya que, en el marco de un Estado de Derecho, lo relativo a la restricción de derechos fundamentales ha de ser tratado con sumo cuidado o, en sus palabras, con calidad y excelencia. Entiende, por tanto, que hechos como la dispersión o el rango normativo de los textos reguladores del SITEL no se acercan al estándar que podríamos considerar como adecuado o aceptable. En mi opinión, la importancia del tema que nos ocupa es de una índole tal que resulta extraño el no considerarlo merecedor de una mejor regulación, más ordenada, completa y eficaz, que aleje las críticas que sin duda hoy en día rondan al Sistema Integrado de Interceptación Legal de Telecomunicaciones.

5.2. El principio de proporcionalidad: requisitos subyacentes

Acabamos de aludir a la regulación del SITEL, pero hemos de tener muy presente que la utilización de dicho sistema supondrá, prácticamente en la totalidad de las ocasiones, un tira y afloja con el derecho al secreto de las comunicaciones. ¿Cuándo es lícita la interceptación legal de comunicaciones?, ¿qué líneas no han de ser traspasadas?

[110] STS de 5 de febrero de 2008.

[111] MARTÍNEZ FERRIZ, J. L. J., «La operatividad de SITEL: su discutida legalidad dentro de un Estado de derecho que actúa bajo el imperio de la ley», *Diario La Ley*, LA LEY, 2010, n.º 7.434, p. 8.

5.2.1. El principio de proporcionalidad en sentido amplio

Para dar respuesta a estos interrogantes el Tribunal Constitucional ha recurrido, no en pocas ocasiones, al principio de proporcionalidad[112]. Así, se establece que ha de haber una relación racional entre la finalidad buscada con la interceptación legal de comunicaciones y la interceptación en sí misma o, con otras palabras, que la vulneración del derecho al secreto de las comunicaciones del investigado no puede ser mayor que el beneficio que supondría dicha interceptación. No sería lógico, por ejemplo, vulnerar de forma flagrante y sistemática el derecho al secreto de las comunicaciones de una persona por sospechar que está cometiendo hurtos de pequeña enjundia.

Tanto la STC 154/2002, de 18 de julio, como COTINO HUESO, aglutinan y resumen de forma muy acertada lo expuesto por el Tribunal Constitucional en otros pronunciamientos: «todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean necesarias para conseguir el fin perseguido, ha de atender a la proporcionalidad entre el sacrificio del derecho y la situación en la que se halla aquél a quien se le impone y, en todo caso, ha de respetar su contenido esencial»[113].

Afirmaciones como la anterior no son más que un recordatorio pues, años antes, el sumo intérprete de la Constitución ya había ido un paso más allá al afirmar que «la desproporción entre el fin perseguido y los medios empleados para conseguirlo puede dar lugar a un enjuiciamiento desde la perspectiva constitucional cuando esa falta de proporción implica un sacrificio excesivo e innecesario de los derechos que la Constitución garantiza»[114].

Ahora bien, imaginemos que estamos en medio de una investigación y tenemos fundadas sospechas de que cierto individuo está relacionado con el tráfico de grandes cantidades de estupefacientes. Situados en este contexto, solicitaríamos la autorización pertinente a la autoridad judicial para llevar a cabo la interceptación legal de comunicaciones y, suponiendo que presentamos indicios con cierto peso, ésta nos concede dicha autorización. Pero, ¿y si finalmente resulta que se dedica al menudeo?

[112] El novedoso Diccionario del español jurídico, de la Real Academia Española en colaboración con el Consejo General del Poder Judicial, define la proporcionalidad en el ámbito procesal como la «nota característica del procedimiento de medidas cautelares en cuya virtud se adopta siempre la medida que resulte menos gravosa para el fin que se pretende». No hablamos de medidas cautelares, pero el grueso de la definición da buena cuenta de la esencia del concepto.
[113] STC 154/2002, de 18 de julio, así como COTINO HUESO, L., *Derecho constitucional II: derechos fundamentales*, PUV, Universitat de València, 2007, p. 211.
[114] STC 49/1999, de 5 de abril.

Puede que incluso, además de intervenir sus comunicaciones telefónicas, hayamos solicitado la geolocalización u otras informaciones conexas; ¿estaríamos sobrepasando el principio de proporcionalidad? Tomando lo expuesto hasta el momento, la respuesta lógica sería una rotunda afirmación.

En virtud de lo anterior, no parece razonable aplicar dichas medidas, vulneradoras del derecho al secreto de las comunicaciones, a un traficante de baja estofa. Ahora bien, en este caso, y siguiendo lo dispuesto por la STC 126/2000, de 16 de mayo, «se aprecia […] que, en el momento en que los órganos judiciales adoptaron la medida, la infracción podía no ser calificada como leve […]. En conclusión, la limitación del derecho al secreto de las comunicaciones fue motivada y proporcionada y, por lo tanto, conforme a la Constitución, por lo que no se ha producido la vulneración del derecho proclamado en el art. 18.3 CE».

En lo que se refiere a esta vía, partidaria de realizar el test o examen de proporcionalidad *ex ante*, decir que no sólo es la opción seguida por el Tribunal Constitucional, sino también por la mayoría de la doctrina. Ahora bien, esto no significa que no haya posiciones encontradas.

Resulta indispensable mencionar, a este respecto, a LÓPEZ BARJA DE QUIROGA[115], el cual cree más adecuado realizar ese test o examen de proporcionalidad *ex post*. Según esta postura, y extrapolándolo al derecho que a nosotros nos incumbe, la trascendencia no residiría en cuál es la concepción o creencia a la hora de establecer la interceptación legal de comunicaciones, sino que simplemente hemos de fijarnos en si se ha vulnerado de forma desproporcionada el derecho al secreto de las comunicaciones. No importa, por tanto, creer que cierta persona está cometiendo un delito mucho más grave de lo que al final resultó ser, sino que lo único trascendente es ese delito objetivamente cometido.

Según el Tribunal Constitucional en su sentencia 11/2006, de 16 de enero, para comprobar si determinada medida restrictiva de un derecho fundamental aprueba el examen de proporcionalidad, hemos de situarnos ante tres requisitos; estos requisitos hacen referencia al cumplimiento de los principios de idoneidad, necesidad y proporcionalidad en sentido estricto respectivamente. Los analizaremos más detenidamente a continuación.

[115] LÓPEZ BARJA DE QUIROGA, J., *Tratado de Derecho Procesal Penal, Tomo I*, Aranzadi, Navarra, 2012, p. 1.584.

5.2.2. Los principios de idoneidad, necesidad y proporcionalidad en sentido estricto

En cuanto al primero de los principios, la idoneidad, decir que ésta hace referencia a si la medida tomada es realmente adecuada para la consecución de un determinado objetivo. PERELLÓ DOMÉNECH la define tanto en sentido positivo como negativo, indicando que dicha restricción al derecho fundamental ha de ser útil para alcanzar el objetivo buscado o, dicho de otro modo, que la medida no puede resultar inútil para lograr tal fin[116]. En la STS de 15 de mayo de 2013 se corrobora lo hasta ahora expuesto al afirmar que la medida ha de ser «funcionalmente idónea para el resultado procurado».

La necesidad, por su parte, requiere que sea indispensable el adoptar dicha medida restrictiva, es decir, que no exista otra «medida igualmente idónea para la consecución del propósito pretendido que sea menos gravosa que la impugnada»[117]. Así mismo, en la misma sentencia que acabamos de tratar con respecto a la idoneidad[118], el Tribunal Supremo establece que la medida «ha de ser tenida por necesaria, al no ser sustituible por otra de injerencia menor». De dicho requisito se deduce una lógica obligación: se deberá optar siempre por la medida menos gravosa o menos vulneradora del derecho de que se trate, siempre que ésta también resulte idónea.

Respecto a la proporcionalidad en sentido estricto, la STC 11/2006, de 16 de enero, establece que ha de tratarse de una medida «ponderada, equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto». Su sentido se deduce fácilmente del apartado en que tratábamos el principio de proporcionalidad, aunque lo hiciéramos en sentido amplio, por lo que nos remitimos a lo dispuesto previamente.

He utilizado la STS de 16 de enero de 2006 para introducir lo relativo a los principios de idoneidad, necesidad y proporcionalidad en sentido estricto. Sin embargo, el apartado primero del art. 588 *bis* «a» LECrim nos obliga a tener en cuenta algunos conceptos más a la hora de poder establecer medidas de investigación tales como la interceptación legal de comunicaciones. Este precepto dispone que «durante la

[116] PERELLÓ DOMÉNECH, I., «El principio de proporcionalidad y la jurisprudencia constitucional», *Jueces para la democracia. Información y debate*, Unigraf, Móstoles, 1997, n.º 28, p. 70.
[117] STC 11/2006, de 16 de enero.
[118] STS de 15 de mayo de 2013. Así mismo, véase la STC 154/2002, de 18 de julio, en la cual el Tribunal Constitucional se expresa en la misma dirección: «todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean necesarias para conseguir el fin perseguido».

instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida». Habremos de hacer, como mínimo, una breve referencia a los principios de especialidad y excepcionalidad, obviando la proporcionalidad de la medida por entenderla cuasi idéntica a la proporcionalidad en sentido estricto.

5.2.3. Los principios de especialidad y excepcionalidad

La especialidad hace referencia a la imposibilidad de imponer este tipo de medidas de forma general o abstracta; una medida de estas características ha de ir destinada a la investigación de un concreto y determinado hecho delictivo. Por esta senda caminan tanto el Tribunal Constitucional como el Tribunal Supremo al afirmar, respectivamente, que «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 en los encargados de la investigación[,] ya que de otro modo se desvanecería la garantía formalmente consagrada en el art. 18.3 CE»[119] y, en la misma dirección, que «la autorización judicial ha de ser específica, es decir, debe atender a circunstancias concretas, y tiene que ser también razonada»[120].

Por otro lado, la excepcionalidad pone de manifiesto el carácter extraordinario de la medida. No se puede solicitar una interceptación legal de comunicaciones «porque sí» ni basándose en razones triviales, sino que es necesario alegar unas dificultades en la investigación que imposibiliten llevar a cabo la misma por los medios considerados normales. El Tribunal Supremo dejó claro que no se puede consentir el hecho de que se pidan este tipo de autorizaciones judiciales de forma sistemática y, aún menos, que éstas lleguen a concederse por la autoridad judicial[121].

Para finalizar hemos de hacer referencia a dos conceptos que también han de cumplirse para que la interceptación legal de comunicaciones no traspase esa «línea roja». Hablamos de que exista, a la hora de solicitar y aplicar dicha medida restrictiva de un derecho fundamental, tanto una finalidad legítima desde el punto de vista constitucional como una serie de indicios suficientes en los cuales apoyarse.

[119] STC 136/2006, de 8 de mayo.
[120] STS de 5 de febrero de 2014.
[121] STS de 5 de noviembre de 2013.

5.2.4. La finalidad constitucionalmente legítima: delitos susceptibles de interceptación

En lo que a la finalidad legítima desde el punto de vista constitucional se refiere, la exigencia es que la interceptación legal de comunicaciones no se establezca en virtud de una infracción penal leve. Esto se traduce en que ha de existir un delito de carácter grave, y sólo de esta manera procederá la limitación de un derecho fundamental. El Tribunal Supremo, en su sentencia de 22 de noviembre, exige «la existencia de una investigación en curso por un hecho constitutivo de infracción punible grave, en atención al bien jurídico protegido y la relevancia social del mismo».

En la misma línea, y como bien reflejan URIARTE VALIENTE y FARTO PAY, el Tribunal Supremo indica que se requiere «una gravedad acorde y proporcionada a los delitos a investigar. […] solo en relación con la investigación de delitos graves, que son los que mayor interés despiertan su persecución y castigo, será adecuado el sacrificio de la vulneración de derechos fundamentales para facilitar su descubrimiento […]. Frente a otras legislaciones que establecen un catálogo de delitos para cuya investigación está previsto este medio excepcional, la legislación española guarda un silencio que ha sido interpretado por la jurisprudencia en el sentido de exigir la investigación de hechos delictivos graves; de alguna manera, puede decirse que en un riguroso juicio de ponderación concretado a cada caso, la derogación del principio de intangibilidad de los derechos fundamentales, debe ser proporcionado a la legítima finalidad perseguida»[122].

¿Qué entendemos, hoy en día, por «delitos graves»? Según el art. 13.1 del Código Penal, serán «delitos graves» las infracciones que la Ley castiga con pena grave. En su segundo apartado define los «delitos menos graves»[123] como, valga la redundancia, aquéllos castigados por la Ley con penas menos graves. En ambos casos estaremos ante delitos de carácter grave, en virtud de lo expuesto por la primera parte del cuarto apartado del mismo artículo.

De interpretar lo dispuesto hasta el momento de forma literal, resultaría que los delitos susceptibles de interceptación de comunicaciones son, simplemente, aquéllos castigados con pena grave o pena menos grave. Sin embargo, si acudimos al artículo 588 *ter* «a» de la Ley de Enjuiciamiento Criminal, nos encontramos con que la interceptación «solo podrá ser concedida cuando la investigación tenga por objeto

[122] STS de 19 de octubre; véase URIARTE VALIENTE, L. M.; FARTO PIAY, T., *El proceso penal español: jurisprudencia sistematizada*, LA LEY, Madrid, 2007, p. 230.
[123] Artículo 13.2 de la Ley 10/1995, de 23 de noviembre, del Código Penal: «son delitos menos graves las infracciones que la Ley castiga con penas menos grave».

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».

Se hace remisión al art. 579.1 LECrim, en el cual nos encontramos con un listado de delitos en cuyo caso es posible la detención y apertura de la correspondencia escrita y telegráfica. Lo que hace el legislador español es remitir a estos casos y autorizar que, en dichas situaciones, se pueda solicitar una autorización judicial para llevar a cabo una interceptación legal de comunicaciones. Hablaríamos, concretamente, de «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».

En consecuencia, ese requisito de que la pena tenga como límite máximo, al menos, tres años de prisión, no operará cuando estamos ante delitos cometidos a través de instrumentos informáticos u otra tecnología de comunicación similar, ni tampoco ante los cometidos por delincuencia organizada, incluyendo –lógicamente– al terrorismo[124].

Hemos de recordar una obviedad antes de dar por finalizado este punto: el cumplimiento del ámbito objetivo de que se trate no supone la seguridad o la confirmación de poder llevar a cabo la interceptación. El hecho de que estemos ante una presunta organización criminal no significa que la solicitud de la intervención vaya a derivar en una autorización por parte del órgano judicial; deberán cumplirse el resto de requisitos que hemos ido viendo hasta ahora.

5.2.5. Los requeridos indicios suficientes

A este requisito hace referencia el art. 588 *bis* «a» LECrim al indicar que «para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la […] intensidad de los indicios existentes».

Cabe preguntarse, antes de nada, qué entendemos por «indicio» en sentido estricto. Según el Tribunal Supremo, no hablamos de una mera sospecha. Hemos de estar ante datos objetivos que justifiquen dicha sospecha, y sólo existiendo éstos y siendo verificables, serán considerados como indicios. Estos datos habrán de ser

[124] A este respecto se incorpora, en el Anexo III, sito al término del trabajo, una relación lo más completa posible de aquellos delitos susceptibles, por su pena, de conllevar una interceptación legal.

accesibles para el juez cuando éste vaya a pronunciarse, pues así podrá conocerlos, valorarlos y tomar la decisión pertinente de forma adecuada[125].

El Tribunal Constitucional, por su parte, estableció que «[era] insuficiente la mera afirmación de la existencia de una investigación previa, sin especificar en qué consiste, ni cuál ha sido su resultado por muy provisional que éste pueda ser»[126]. Así mismo, siguiendo lo dispuesto en la STC 49/1999, de 5 de abril[127], la interceptación legal de comunicaciones sólo podrá llevarse a cabo si hay «datos fácticos o indicios que permitan suponer que alguien intenta cometer, está cometiendo o ha cometido una infracción grave o donde existan buenas razones o fuertes presunciones de que las infracciones están a punto de cometerse».

En conclusión, si bien no se pide una certeza –pues carecería de sentido–, sí ciertos datos objetivos que permitan suponer la comisión de una infracción grave, ya sea pasada, presente o futura. Sin embargo, dicho requisito no puede entorpecer la labor de investigación de forma desproporcionada. Esto significa que no se puede exigir indicios de carga probatoria similar a la que resultaría necesaria para comenzar el procesamiento del investigado. Así lo establece la STS de 15 de noviembre de 2006 al afirmar que «no es necesario que se alcance el nivel de los indicios racionales de criminalidad propios de la adopción del procesamiento».

6. OTRAS CUESTIONES DE INTERÉS

6.1. No necesidad de la autorización judicial

La autorización judicial es uno de los elementos clave de la diligencia vinculada al SITEL, considerándose requisito indispensable para poder proceder. Sin embargo, hay una circunstancia que, de tener lugar, validaría la interceptación legal de comunicaciones sin autorización judicial de por medio.

El último apartado del art. 588 *ter* «d» LECrim[128] establece que, «en caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan

[125] STS de 8 de octubre de 2013.
[126] STC 197/2009, de 28 de septiembre.
[127] El referido extracto de la STC 49/1999, de 5 de abril, no hace otra cosa que resumir dos razonamientos sitos en sendas sentencias del Tribunal Europeo de Derechos Humanos a este respecto: SSTEDH de 6 de septiembre de 1978 y de 15 de junio de 1992.
[128] Modifica ligeramente lo anteriormente expuesto por el artículo 579.4 LECrim.

razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad […]».

Este artículo continúa dándonos unos requisitos adicionales: establece un plazo máximo de veinticuatro horas para comunicarlo al juez competente, debiendo informarle de los motivos que llevaron al ejercicio de tal diligencia, así como de la ejecución de la misma y del resultado producido. La autoridad judicial dispondrá de setenta y dos horas, como máximo, para confirmar o revocar la actuación.

6.2. Destino de las informaciones tras el proceso penal

Históricamente se puede apreciar, por parte del TEDH, una posición claramente decantada por la destrucción de dichas informaciones tras el proceso penal[129]. En cambio, en el ámbito del Derecho español, el Tribunal Constitucional y el Tribunal Supremo se preocupaban tan sólo de la autenticidad de los soportes que contenían las informaciones y no de su destino final[130].

Esto cambiará con la STS 293/2011, de 14 de abril. Desde este momento, se establece que «los Tribunales, de oficio, en las causas en las que se haya procedido a la realización de intervenciones telefónicas, deberán acordar en sus sentencias la destrucción de las grabaciones originales que existan en la unidad central del sistema SITEL y de todas las copias, conservando solamente de forma segura las copias entregadas a la autoridad judicial, y verificando en ejecución de sentencia, una vez firme, que tal destrucción se ha producido».

Actualmente contamos con el art. 588 *bis* «k» LECrim. Dicho artículo determina que «una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida», conservándose una copia bajo custodia del Letrado de la Administración de Justicia. Transcurridos cinco años, se acordará la destrucción de esa copia conservada.[131]

[129] Véase la STEDH de 30 de julio de 1998, y el precedente relativo a la STEDH de 24 de abril de 1990.
[130] En realidad sí que hubo algún pronunciamiento al respecto, pero sin valía en la práctica. Véase el Auto del Tribunal Supremo de 18 de junio de 1992.
[131] Para más información sobre el destino de las informaciones tras el proceso penal, véase RODRÍGUEZ LAINZ, J. L., «Sobre el destino de las grabaciones de conversaciones objeto de una intervención legal de comunicaciones, una vez finalizado el proceso en que se acordaron», *Diario La Ley*, LA LEY, 2012, n.º 7.982, pp. 2 y 3.

6.3. Las aplicaciones de telefonía móvil: cifrado de la información

Como ya hemos mencionado, el SITEL nos permite interceptar comunicaciones telefónicas propiamente dichas, conversaciones vía SMS e, incluso, geolocalizar un aparato. Ahora bien, nuestra generación está siendo testigo de la aparición de nuevas y revolucionaras vías de comunicación; desde el ya nada moderno –aunque en absoluto en desuso– correo electrónico, hasta las aplicaciones móviles más novedosas, utilizadas segundo a segundo y de forma masiva en todo el mundo[132].

Si nosotros, hoy en día, nos comunicamos con nuestro teléfono no sólo por las vías tradicionales, sino por incontables aplicaciones de telefonía móvil o gracias al acceso mismo a Internet (foros, chats…), ¿no harán algo similar los delincuentes? Además, ellos serán conscientes, al igual que nosotros, de que muchas de estas vías de comunicación traen consigo un sistema de cifrado, con lo que ello implica.

En el caso de *WhatsApp*, la aplicación de estas características con más uso en España, está el denominado «cifrado de extremo a extremo». Todo aquello que un usuario de *WhatsApp* envíe a otro, ya sea texto, fotografías, vídeos o mensajes de voz, será encriptado y tan sólo se descifrará al llegar a su destinatario[133]. Además, cabe mencionar que el operador de telecomunicaciones que da este servicio no es, ni mucho menos, el operador clásico. Entonces, ¿cómo se harán las Fuerzas y Cuerpos de Seguridad del Estado con la información necesaria en caso de precisarla?

Realmente el proceso será similar, al menos en lo que a su esencia se refiere. Así queda claro en el apartado primero del art. 588 *ter* «e», donde se establece que «todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información […], están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones».

Pero esto tan sólo es la teoría. Podemos encontrarnos con problemas con los que antes no contábamos: puede ser que queramos intervenir información que esté sita en

[132] En nuestro país *WhatsApp* es la gran vencedora. De media, cada español dedica más de una hora al día a comunicarse por medio de la misma, frente a la media hora de la media mundial.

[133] *WhatsApp* no guarda sus claves de cifrado en un servidor central, como suele ser normal, sino que dichas claves se almacenan en el dispositivo de cada usuario. Esto es combinado con *TextSecure*, que se encarga de que para cada mensaje haya una nueva clave de cifrado. El resultado es que los piratas informáticos, acostumbrados a atacar los servidores centrales donde reposan las referidas claves, se ven con las manos atadas.

otro país, por lo que hemos de adecuarnos a su Derecho propio. Así mismo, el operador de telecomunicaciones de que se trate ha de cooperar, desencriptando la información y cediéndonosla o haciéndonos saber cómo descifrarla… y esto en ocasiones no es tan sencillo. Podemos apreciar dicha dificultad en la famosa confrontación entre *Apple* y el FBI, en relación con la Masacre de San Bernardino[134]. Aunque no es un caso que se pueda extrapolar completamente al tema que nos ocupa, sirve para dar buena cuenta de las negativas que emanan de estas empresas.

En consecuencia, nos encontramos con que, sobre el papel, las Fuerzas y Cuerpos de Seguridad tendrían la capacidad de acceder a las conversaciones que se lleven a cabo por medio de estas aplicaciones de telefonía móvil, pero en la práctica esto puede no suceder. Más allá de casos icónicos como el de la Masacre de San Bernardino, desde la Unión Europea se está intentando dar pasos en pos de facilitar el acceso a dichas informaciones, sobre todo en asuntos de terrorismo. Hemos de mencionar, por otro lado, que nuestras Fuerzas y Cuerpos de Seguridad del Estado también cuentan con herramientas de desencriptación, aunque suelen mostrarse inútiles ante determinados sistemas de cifrado. Es, por tanto, lícito y legítimo; pero está plagado de dificultades. Y es que, de nuevo, el Derecho camina por detrás de la realidad social y sus necesidades.[135]

7. CONCLUSIONES

En la medida en que el trabajo que nos ocupa trata de dar una visión global y objetiva del SITEL, casi didáctica, parece oportuno el evitar realizar juicios de valor en demasía. Sin embargo, fuera de esa subjetividad, podríamos afirmar que nos encontramos, con sus más y sus menos, ante un sistema que ha resultado ser útil en las tareas para las que fue concebido. Un sistema que, más allá de su efectividad técnica y pese a la perenne controversia, respeta los principios relativos al proceso penal.

Hablamos de controversia pues cabría apreciar cierto margen de mejora en cuanto a su regulación. A lo largo de la realización de este trabajo nos hemos cerciorado de la inusitada cantidad de jurisprudencia a la que hemos tenido que acudir, en muchas ocasiones no para reafirmar lo dicho o aclarar conceptos, sino para llenar de significado y

[134] El FBI quería que *Apple* crease una puerta trasera para acceder al contenido del teléfono móvil de los atacantes de San Bernardino, Syed Rizwan Farook y Tasfeen Malik. El tiroteo, acaecido el 2 de diciembre de 2015 en San Bernardino, California, causó catorce muertos y veintiún heridos.

[135] Para más información, véase RODRÍGUEZ LAINZ, J. L., *El secreto de las telecomunicaciones y su interceptación legal*, SEPIN, Madrid, 2016.

contenido cuestiones hasta el momento huérfanas de sentido. Este fenómeno, en un sistema como el nuestro –que dista mucho de tener las notas típicas de los ordenamientos jurídicos anglosajones–, suele responder a una regulación deficiente o, simplemente, con un escaso desarollo. Pareciera que nos situásemos, sobre todo en un primer momento, ante una regulación marco, dejando a los tribunales la concreción de la norma.

Sea como fuere, a mi juicio y aun teniendo en cuenta semejantes inconvenientes, el SITEL goza de unas garantías que, a nivel general y en el marco de la interceptación legal de comunicaciones, se traducen en el respeto a los derechos de los investigados. Si bien podríamos mostrarnos más contrariados en el contexto del art. 579 LECrim antes de la LO 13/2005, de 5 de octubre, y aún más con anterioridad a la LO 4/1988, de 25 de mayo, hemos de aceptar la actual regulación como garante de los derechos en conflicto, si bien no decaer en la llamada al legislador para que regule, de forma más detallada, un tema como el que nos ocupa.

A lo largo de este trabajo hemos analizado cuestiones de muy distinta naturaleza, resultando estéril el recopilar aquí, sin nexo alguno, algunas de las conclusiones particulares que hemos ido alcanzando. Siendo así, nos remitimos a lo ya dicho respecto a las cuestiones más controvertidas como, por ejemplo, el cumplimiento del requisito de ser regulado por Ley Orgánica, o las garantías de autenticidad de la información sita en el CD o DVD de que se trate.

En mi opinión, y con el fin de poner el punto y final a este TFG, decir que estamos ante un sistema que funciona de forma más que adecuada. Es mejorable, sin duda, pues llegar a la perfección en un ámbito como el que nos ocupa, con derechos en conflicto, se estima a todas luces utópico.

La limitación o la cesión en el campo de los derechos en pos de la seguridad es algo que ha estado, está y estará siempre envuelto en argumentaciones contradictorias; lo hemos visto recientemente en Francia con el Estado de excepción y los posteriores movimientos del Presidente de la República para normalizar alguna de las medidas propias de ese estatus especial. Surge, en este contexto, la imperiosa necesidad de conjugar derechos y seguridad; y de igual forma emana cuando hablamos de intervenir comunicaciones.

En este sentido, el SITEL ofrece las garantías necesarias para que esta conciliación efectivamente se produzca, delimitando claramente cuándo se puede acudir a la interceptación legal de comunicaciones y en qué términos hemos de hacerlo.

BIBLIOGRAFÍA

Doctrina

BARRADO CASADO, M. A., «La captación de datos e intervención de las comunicaciones. Una visión técnico policial», *Interceptación de las comunicaciones y nuevas tecnologías*, Cuadernos Digitales de Formación, Consejo del Poder Judicial, Madrid, 2010, n.º 43.

BELDA PÉREZ-PEDRERO, E. *El derecho al secreto de las comunicaciones*. Dialnet: La Rioja.

BRAGE CAMAZANO, J., *Los límites a los derechos fundamentales*, Editorial Dykinson, Madrid, 2004.

CASANOVA MARTÍ, R., *Problemática de las intervenciones telefónicas en el proceso penal: una propuesta normativa*, PICO I JUNOY, J. (dir.), Publicacions URV, Tarragona, 2014.

CASANOVA MARTÍ, R., *Las intervenciones telefónicas en el proceso penal*, J.M. Bosch Editor, Barcelona, 2014.

CASTILLEJO MANZANARES, «R. Medios de Investigación en la lucha contra la criminalidad organizada. SITEL», *Revista General de Derecho procesal*, Iustel, 2012, n.º 27.

COTINO HUESO, L., *Derecho constitucional II: derechos fundamentales*, PUV, Universitat de València, 2007.

ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, Iustel Publicaciones, Madrid, 2007.

ENGAÑA CEA, J. L., *Derecho constitucional chileno: Tomo II*, Ediciones UC, Santiago, 2012.

FERNÁNDEZ FERNÁNDEZ, F., «El sistema policial de interceptación de las comunicaciones: SITEL», *La interceptación de las comunicaciones telefónicas y telemáticas*, CEJ, 2016.

GIMENO SENDRA, J. V., *Derecho procesal penal*, Civitas, Navarra, 2012.

GONZÁLEZ MONJE, A., *Cooperación jurídica internacional en materia penal e intervención de comunicaciones como técnica especial de investigación*, Comares, Granada, 2017.

LÓPEZ BARJA DE QUIROGA, J., *Tratado de Derecho Procesal Penal, Tomo I*, Aranzadi, Navarra, 2012.

LÓPEZ-FRAGOSO ÁLVAREZ, T., *Las intervenciones telefónicas en el proceso penal*, COLEX, Madrid, 1991.

MARCHENA GÓMEZ, M., «Proceso penal: nuevos problemas, viejas soluciones», *La Ley Penal*, LA LEY, 2015, n.º 100.

MARTÍNEZ FERRIZ, J. L. J., «La operatividad de SITEL: su discutida legalidad dentro de un Estado de derecho que actúa bajo el imperio de la ley», *Diario La Ley*, LA LEY, 2010, n.º 7.434.

PERELLÓ DOMÉNECH, I., «El principio de proporcionalidad y la jurisprudencia constitucional», Jueces para la democracia. Información y debate, Unigraf, Móstoles, 1997, n.º 28.

PUY MUÑOZ, F., Los derechos del constitucionalismo histórico español, Servicio de Publicacións e Intercambio Científico, Universidade de Santiago de Compostela, 2002.

RICO LINAGE, R., Constituciones históricas, Publicaciones de la Universidad de Sevilla, Sevilla, 1999.

RODRÍGUEZ LAINZ, J. L., «SITEL: nuevas tendencias, nuevos retos», *Diario La Ley*, LA LEY, 2013, n.º 8.082.

RODRÍGUEZ LAINZ, J. L., «Sobre el destino de las grabaciones de conversaciones objeto de una intervención legal de comunicaciones, una vez finalizado el proceso en que se acordaron», *Diario La Ley*, LA LEY, 2012, n.º 7.982.

RODRÍGUEZ LAINZ, J. L., *El secreto de las telecomunicaciones y su interceptación legal*, SEPIN, Madrid, 2016.

TEJERINA RODRÍGUEZ, O., *Seguridad del Estado y privacidad*, Reus Editorial, Madrid, 2014.

URIARTE VALIENTE, L. M.; FARTO PIAY, T., *El proceso penal español: jurisprudencia sistematizada*, LA LEY, Madrid, 2007.

Legislación

Decreto de la Asamblea Nacional Francesa de 10 de agosto de 1970.

Constitución Española de 1869.

Constitución Española de 1876.

Fuero de los Españoles de 1945.

Constitución Española de 1978.

Convenio Europeo de Derechos Humanos.

Declaración Universal de los Derechos Humanos.

Pacto Internacional de Derechos Civiles y Políticos.

Declaración de Derechos del Hombre y el Ciudadano

Real Decreto de 14 de septiembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal

Ley Orgánica 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal.

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Informe de la Secretaría Técnica de la Fiscalía General del Estado, de 5 de octubre de 2005, titulado «Consideraciones sobre el sistema SITEL de interceptación de comunicaciones».

Resolución COM 96/C 329/01 del Consejo de la Unión Europea, de 17 de enero de 1995, sobre la interceptación legal de las telecomunicaciones.

Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Conclusiones de la inspección del SITEL por la Agencia Española de Protección de Datos, con fecha de 19 de enero de 2010.

Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

Jurisprudencia

España. Tribunal Constitucional (Sala Segunda). Sentencia n.º 114/1984, de 19 de noviembre.

España. Tribunal Constitucional (Sala Segunda). Sentencia n.º 115/2003, de 9 de mayo.

España. Tribunal Constitucional (Sala Segunda). Sentencia n.º 170/2003, de 7 de octubre.

España. Tribunal Constitucional (Sala Primera). Sentencia n.º 2/1982, de 29 de enero.

España. Tribunal Constitucional (Sala Segunda). Sentencia n.º 81/1983, de 10 de octubre.

España. Tribunal Constitucional (Pleno). Sentencia n.º 154/2002, de 18 de julio.

España. Tribunal Constitucional (Pleno). Sentencia n.º 49/1999, de 5 de abril.

España. Tribunal Constitucional (Sala Segunda). Sentencia n.º 126/2000, de 16 de mayo.

España. Tribunal Constitucional (Sala Primera). Sentencia n.º 11/2006, de 16 de enero.

España. Tribunal Constitucional (Pleno). Sentencia n.º 154/2002, de 18 de julio.

España. Tribunal Constitucional (Sala Segunda). Sentencia n.º 136/2006, de 8 de mayo.

España. Tribunal Constitucional (Sala Primera). Sentencia n.º 197/2009, de 28 de septiembre.

España. Tribunal Constitucional (Pleno). Sentencia n.º 4/1999, de 5 de abril.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 503/2013, de 19 de junio.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 250/2009, de 13 de marzo.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 661/2013, de 15 de julio.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 1.078/2009, de 5 de noviembre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 1.114/2009, de 12 de noviembre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 554/2011, de 7 de junio.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 9.770/1991, de 19 de abril.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 423/2012, de 20 de enero.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 6.654/2012, de 2 de octubre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 5.634/2012, de 13 de julio.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 1.215/2009, de 30 de diciembre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 722/2012, de 2 de octubre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 4.331/2010, de 6 de julio.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 8.417/2009, de 30 de diciembre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 4.270/2013, de 9 de julio.

España. Tribunal Supremo (Sala de lo Contencioso). Sentencia n.º 390/2008, de 5 de febrero.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 3.397/2013, de 15 de mayo.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 84/2014, de 5 de febrero.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 823/2013, de 5 de noviembre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 871/2013, de 22 de noviembre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 1.012/2006, de 19 de octubre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 720/2013, de 8 de octubre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 1.129/2006, de 15 de noviembre.

España. Tribunal Supremo (Sala de lo Penal). Sentencia n.º 293/2011, de 14 de abril.

España. Tribunal Supremo (Sala de lo Penal). Auto de 18 de junio de 1992.

Tribunal Europeo de Derechos Humanos. Caso Klass y otros contra Alemania. Sentencia de 6 de septiembre de 1978.

Tribunal Europeo de Derechos Humanos. Caso Lüdi contra Suiza. Sentencia de 15 de junio de 1986.

Tribunal Europeo de Derechos Humanos. Caso Huvig y Kruslin contra Francia. Sentencia de 24 de abril de 1990.

Tribunal Europeo de Derechos Humanos. Caso Valenzuela Contreras contra España. Sentencia de 30 de julio de 1998.

Recursos electrónicos

Boletín Oficial del Estado: https://www.boe.es/

Centro de Estudios Jurídicos: http://www.cej-mjusticia.es/

Congreso de los Diputados: http://www.congreso.es/

Dialnet: https://dialnet.unirioja.es/

EUR-Lex: https://eur-lex.europa.eu/

Iustel: https://www.iustel.com/

Noticias Jurídicas: http://noticias.juridicas.com/

Présidence de la République: http://www.elysee.fr/

Tribunal Europeo de los Derechos Humanos: https://www.echr.coe.int/

vLex: https://vlex.es/

ANEXO I

«1. Los sujetos obligados deberán facilitar al agente facultado […] los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad […] del sujeto objeto de la medida de la interceptación.
b) Identidad […] de las otras partes involucradas en la comunicación electrónica.
c) Servicios básicos utilizados.
d) Servicios suplementarios utilizados.
e) Dirección de la comunicación.
f) Indicación de respuesta.
g) Causa de finalización.
h) Marcas temporales.
i) Información de localización.
j) Información intercambiada a través del canal de control o señalización.

2. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado […] los siguientes datos:

a) Identificación de la persona física o jurídica.
b) Domicilio en el que el proveedor realiza las notificaciones.

   Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).
d) Número de identificación del terminal.
e) Número de cuenta asignada por el proveedor de servicios Internet.
f) Dirección de correo electrónico.

3. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.»[136]

[136] Artículo 88 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

ANEXO II

«Por parte de quien asuma en el centro de recepción las funciones de responsable del fichero y de seguridad:

1. Certificación de la fecha de la generación de la carpeta, con identificación de la clave numérica asignada.
2. Identificación del agente o agentes facultados que han tenido acceso al fichero.
3. Identificación de los accesos realizados por los agentes facultados.
4. Fechas en que se hayan producido descargas de archivos de comunicaciones y datos, con relación nominal de cada uno de los archivos descargados, o al menos fechas de las sesiones de interceptación; con certificación de si tales eventos generaron la emisión de la correspondiente firma electrónica tanto por parte del centro de recepción como por parte del agente facultado.
5. Certificación de que no se ha producido acceso alguno que haya podido afectar a la integridad o contenido de los archivos asociados al fichero.
6. Relación nominal de todos los registros, tipo archivos de datos o de comunicaciones, que se hayan almacenado en la correspondiente carpeta.
7. Certificación relativa a la superación del último informe de auditoría sobre el funcionamiento del sistema realizado por el centro de recepción.

Por parte del agente facultado, una certificación que se extienda a los siguientes aspectos:

1. Ídem respecto de los puntos 1 a 5.
2. Que todos los archivos correspondientes a contenidos y datos asociados han sido descargados del centro de recepción, contando con la correspondiente firma electrónica que lo respalde.
3. Que la información que se adjunta en el CD se corresponde íntegramente con la descargada del centro de recepción, sin que se haya producido modificación o alteración alguna.
4. Que dicha información, mientras ha sido objeto de descarga y conservación por el agente facultado, hasta el momento mismo de la facilitación del CD a la autoridad judicial, ha estado custodiada en un entorno seguro; sin que conste igualmente ninguna clase de acceso inconsentido, manipulación o eliminación de archivos.»[137]

[137] RODRÍGUEZ LAINZ, J. L., «SITEL: nuevas…», *Diario…*, op., cit., pp. 12 y 13.

ANEXO III

Adjunto en este anexo, de la forma más exhaustivamente posible aunque sin el ánimo de determinar unos *numerus clausus* o una lista tasada, aquellos delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión. Hemos de recordar que dicho requisito, a priori esencial para llevar a cabo la diligencia que nos ocupa, decaerá cuando estemos ante delitos cometidos a través de instrumentos informáticos u otra tecnología de comunicación similar, así como ante los cometidos por delincuencia organizada o con fines terroristas.

Con el fin de no anexar una lista de mayúsculas dimensiones, en la gran mayoría de los casos habrá que comprobar los subtipos penales de que se traten. Por ejemplo, en los casos de aborto (arts. 144 – 146 CP) tan sólo hemos de quedarnos con los arts. 144 y 145, pues los arts. 145 *bis* y 146 no poseen el requisito de estar penados con, al menos, tres años de prisión. Este ejercicio de precisión habrá que hacerlo con muchos de los tipos penales de la lista, si bien en algunas ocasiones se especificará el subtipo concreto por ser el único al que podría afectar esta diligencia, como por ejemplo en lo relativo a las lesiones al feto (sólo resultándonos apropiado el art. 157 CP y no así el artículo que le sigue) o a la omisión del deber de socorro (en cuyo caso tan sólo podría ser objeto de esta diligencia el caso del art. 195.3 CP y no el resto del precepto). Precisado lo anterior, los delitos que, por su gravedad, podrían ser objeto de esta diligencia de investigación, son los siguientes:

- del homicidio y sus formas (arts. 138 y ss.); incluyendo, además del asesinato, la inducción al suicidio del art. 143 CP
- del aborto (arts. 144 y 145 CP); como hemos dicho, excluyendo los casos de los arts. 145 *bis* y 146 por no llegar a ese techo máximo de, al menos, tres años de prisión
- de las lesiones (arts. 147 y ss. CP); incluyendo el tráfico ilegal de órganos humanos del art. 156 *bis* CP
- de las lesiones al feto (art. 157 CP)
- relativos a la manipulación genética (arts. 159 y ss. CP)
- de las detenciones ilegales y secuestros (arts. 163 y ss. CP)
- de las amenazas (arts. 169 y ss. CP)
- de las coacciones (art. 172 y ss.)

- de las torturas y otros delitos contra la integridad moral (arts. 173 y ss. CP); destacando la violencia doméstica del art. 173.2 CP y la tortura en sentido estricto del art. 174 CP
- de la trata de seres humanos (art. 177 *bis* CP)
- de las agresiones sexuales (arts. 178 y ss. CP)
- de los abusos sexuales (arts. 181 y ss. CP)
- de la prostitución, explotación sexual y corrupción de menores (arts. 187 y ss. CP)
- de la omisión del deber de socorro (art. 195.3 CP); tan sólo cuando el accidente es causado, por imprudencia, por el mismo que omite el deber de socorro
- del descubrimiento y revelación de secretos (arts. 197 y ss. CP)
- del allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público (art. 203.3 CP)
- de la suposición de parto y de la alteración de la paternidad, estado o condición del menor (arts. 220 y ss. CP)
- contra los derechos y deberes familiares (arts. 225 *bis* y 229 en sus apartados 2.º y 3.º CP); la sustracción de menores se encontraría subsumida en el art. 225 *bis* CP.
- de los hurtos (art. 235 CP); tan sólo en su vertiente agravada
- de los robos (arts. 237 y ss. CP)
- de la extorsión (art. 243 CP)
- de las defraudaciones (arts. 248 y ss. y 253CP); incluyendo las estafas y la apropiación indebida
- de la frustración de la ejecución (arts. 257 y ss. CP)
- de las insolvencias punibles (arts. 259 y ss. CP)
- de la alteración de precios en concursos y subastas públicas (art. 262 CP)
- de los daños (arts. 263 y ss. CP); destacando los daños del art. 263.2 y los daños de carácter informático de los arts. 264 y ss. CP
- relativos a la propiedad intelectual e industrial, al mercado y a los consumidores (arts. 270 y ss. CP); incluyendo también los delitos de corrupción en los negocios de los arts. 286 *bis* y ss. CP
- de los delitos societarios (arts. 290 y ss. CP)
- de la receptación y el blanqueo de capitales (arts. 298.2 y 301 y ss. CP)
- de la financiación ilegal de los partidos políticos (art. 304 *bis* y ss. CP)
- contra la Hacienda Pública y la Seguridad Social (arts. 305 y ss. CP)
- contra los derechos de los trabajadores (arts. 311 y ss. CP)

- del tráfico de mano de obra e inmigración ilegal (arts. 312 y 313 CP)
- contra los derechos de los ciudadanos extranjeros (apartado 3.º del art. 318 *bis* CP)
- contra la ordenación del territorio y el urbanismo (arts. 319 y 320 CP)
- contra el patrimonio histórico (arts. 321 y ss. CP)
- contra los recursos naturales y el medio ambiente (art. 325 y ss. CP)
- del riesgo catastrófico (arts. 341 y ss. CP)
- de los incendios (arts. 351 y ss. CP)
- contra la salud pública (arts. 359 y ss. CP)
- contra la seguridad vial (art. 381.1 CP); nos referiríamos, concretamente, a la conducción temeraria
- de la falsificación de moneda y efectos timbrados (arts. 386 y ss. CP)
- de las falsedades documentales (arts. 390 y ss. CP)
- de la usurpación del estado civil (art. 401 CP)
- de la usurpación de funciones públicas y del intrusismo (art. 402 CP)
- del abandono de destino y de la omisión del deber de perseguir delitos (art. 407 CP)
- de la infidelidad en la custodia de documentos y de la violación de secretos (art. 413, 417 y 418 CP); nos referimos, respecto a la violación de secretos, a aquéllos que puedan causar grave daño para la causa pública
- del cohecho (arts. 419 y ss. CP)
- de la malversación (arts. 432 y 433 *bis* en su apartado 3.º CP)
- de los fraudes y exacciones ilegales (art. 436 CP)
- de la prevaricación (art. 446 CP)
- del encubrimiento (art. 451 CP)
- del falso testimonio contra reo en causa criminal (art. 458.2 CP); nos incumbirá cuando se trate de un falso testimonio en contra del reo en causa criminal por delito
- de la obstrucción a la Justicia y la deslealtad profesional (art. 464 CP)
- del quebrantamiento de condena (art. 469 CP); de nuevo, requerimos un tipo cualificado, pues exige violencia o intimidación
- de los delitos contra la Administración de Justicia de la Corte Penal Internacional (art. 471 *bis* CP)
- de la rebelión (arts. 472 y ss. CP)
- contra la Corona (arts. 485 y ss. CP)
- contra las instituciones del Estado y la división de poderes (arts. 492 y ss. CP); incluyendo lo relativo a la usurpación de atribuciones del art. 506 CP

- de los delitos relativos al ejercicio de los derechos fundamentales y libertades públicas (arts. 510 y ss. CP); incluimos lo relativo a la sección primera, «de los delitos cometidos con ocasión del ejercicio de los derechos fundamentales y de las libertades públicas garantizados por la Constitución» (odio y discriminación, reuniones y manifestaciones ilícitas, etcétera)
- de la sedición (arts. 544 y ss. CP)
- de los atentados contra la autoridad, sus agentes y los funcionarios públicos, y de la resistencia y la desobediencia (arts. 550 y ss. CP)
- de los desórdenes públicos (arts. 557 y ss. CP)
- de la tenencia, tráfico y depósito de armas, municiones o explosivos (arts. 563 y ss. CP)
- del terrorismo (arts. 573 *bis* y ss. CP)
- de la traición (arts. 581 y ss. CP)
- contra la paz e independencia del Estado (arts. 589 y ss. CP)
- del descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional (arts. 598 y ss. CP)
- contra el Derecho de gentes (arts. 605 y 606 CP)
- del genocidio (art. 607 CP)
- de la lesa humanidad (art. 607 *bis* CP)
- contra las personas y bienes protegidos en caso de conflicto armado (arts. 608 y ss. CP)
- de la piratería (arts. 616 *ter* y ss. CP)
- del contrabando (art. 3 de la Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando)
- relativos a la navegación aérea (Ley 209/1964, de 24 de diciembre, por la que se establece la Ley Penal y Procesal en materia de navegación aérea)

Por tanto, más allá de los delitos señalados, no cabrá adoptar la diligencia que nos ocupa a no ser que hayan sido perpetrados por una organización criminal o grupo terrorista.