InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

# Interceptación de las comunicaciones electrónicas.

Concordancias y discordancias de SITEL con el artículo 18.3 CE

Cristina Zoco Zabala

Universidad Pública de Navarra
Facultad de Derecho

BARCELONA, OCTUBRE 2010

## *Abstract*

*Este trabajo tiene por objeto analizar el Capítulo II del Real Decreto 424/2005, de 15 de abril, por el que se regula el procedimiento para intervenir las comunicaciones electrónicas con el objeto de verificar si su ejecución afecta a las condiciones que delimitan el contenido esencial del art. 18.3 CE. Se concluye que dicho reglamento no afecta al art. 18.3 CE en lo relativo a la enumeración que realiza de los tipos de datos asociados a las comunicaciones electrónicas que pueden ser susceptibles de intervención legal junto con el contenido de las mismas. Sin embargo, cercena el contenido esencial del art. 18.3 CE en lo relativo a la obligación del juez a determinar, siquiera, algunos de estos datos en la orden legal de intervención. En la medida en que el secreto de las comunicaciones es un derecho formal que delimita su contenido a la posibilidad de intervenir las comunicaciones previa resolución judicial motivada, los datos asociados obtenidos como consecuencia de la intervención no quedan protegidos por el art. 18.3 CE, sino, en todo caso, por los arts. 18.1 y 18.4 CE. Ello significa que una vez que el órgano judicial ha explicitado en la resolución judicial de intervención las sospechas objetivas de la presunta comisión de un delito grave y la inexistencia de otros medios probatorios que permitan esclarecer los hechos presuntamente delictivos que se investigan, los datos obtenidos como consecuencia de la interceptación quedan protegidos por el art. 18.1 CE si dicha información es revelada a terceros, o por el art. 18.4 CE si la información se utiliza para otro fin distinto para el que fue recabada. Derivado de lo anterior, tampoco es necesario que el legislador orgánico regule qué datos asociados a las comunicaciones debe mencionar el juez, pues es preciso dejar un margen de libertad a la autoridad judicial para determinar si cree conveniente que se recaben algunos de los datos asociados que menciona el reglamento, o si precisa una apertura general de las comunicaciones electrónicas, que recabe tanto el contenido de la comunicación como los datos que se asocian a ella.*

*The objective of this work is to analyse Chapter II of Royal Decree 424/2005, dated 15th April, by which a procedure is regulated to tap electronic communications with the aim of verifying if this practice affects the conditions that limit the essential content of article 18.3 CE. It is concluded that these regulations do not affect article 18.3 CE as refers to the enumeration it includes of the types of data associated to electronic communications that can be legally intervened together with the content thereof. It does, however, mutilate the essential content of article 18.3 CE as refers to the obligation of the judge to determine at least some of such data in the legal tapping order. Inasmuch as the secret of communications is a formal right that limits its content to the possibility of intervene communications by means of a previous judicial resolution detailing the causes thereof, the associated data obtained as a consequence of such an intervention are not protected by article 18.3 CE, but in any case by articles 18.1 and 18.4 CE. This means that once the judicial organ has explicated in its judicial intervention order the objective suspicions of an alleged serious crime as well as the inexistence of other means to prove such a crime that would clarify the alleged criminal conduct that is being investigated, the data obtained as a consequence of such an interception would be protected by article 18.1 CE if that information is revealed to third parties, or by article 18.4 CE if the information is used for other purposes that are different from those for which the tapping was authorised. As a derivation of this, it is also not necessary that organic legislators regulate what data associated to the communications the judges are to mention, as it is necessary to leave a margin of action for the judicial authorities to determine if they believe it is convenient to gather certain associated data mentioned in the regulations, or if a generalised judicial opening of electronic communications is necessary that gathers both the content of the communication as well as data that are associated thereto.*

*Title:* Interception of electronic communications. Convergences and divergences of SITEL with article 18.3 CE

*Keywords: Secrecy in communications, Intimacy, Protection of personal data, Objective suspicions, Serious crimes.*

*Palabras clave:* Secreto de las comunicaciones, Intimidad, Protección de datos personales, Sospechas objetivas, Delitos graves.

## *Sumario*

**1. Introducción**
**2. Procedimiento para intervenir las comunicaciones en el 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**
**2.1. Las leyes orgánicas reguladoras del contenido esencial de la intervención de las comunicaciones**
**2.2. La obligación de explicitar en la resolución judicial algunos de los datos asociados a las comunicaciones electrónicas**
**2.3. La obligación de transmitir la información intervenida al agente facultado y la confidencialidad de la información obtenida**
**3. Conclusión**
**4. Bibliografía**

## *1. Introducción*

La creciente aplicación de las comunicaciones electrónicas originada por la revolución de las nuevas tecnologías ha trascendido a la protección de su secreto en virtud del art. 18.3 CE[1]; bien sea mediante la proscripción de la interceptación del correo electrónico, o mediante su intervención condicionada a la previa existencia de una autorización judicial constitucionalmente conforme. El artículo 33 (párrafos 1 y 2) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (BOE nº 264, de 4.1.2003) (en adelante LGT), en su redacción dada por la disposición final 1ª de la Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas (BOE nº 251, de 19.10.2007) (en adelante LCDCE), ha recordado, de modo expreso, que la delimitación del secreto de las comunicaciones electrónicas lo es conforme al art. 18.3 CE y a las leyes orgánicas que desarrollan su contenido[2].

Este recordatorio de la LCDCE alusivo a las garantías constitucionales del art. 18.3 CE y de la correspondiente ley orgánica no pasaría de ser una mera redundancia si no fuera por la polémica social e institucional que ha generado la aprobación, mediante 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 (BOE nº 102, de 20.04.2005) (en adelante RLGT), del avanzado procedimiento técnico de intervención de las comunicaciones o sistema integral de interceptación de las comunicaciones electrónicas (SITEL) que se instala en los proveedores de servicios de redes de telecomunicación (ISP). La razón estriba en la consideración de que esta norma reglamentaria reguladora de la ejecución del procedimiento de intervención de las comunicaciones cercena el contenido esencial del art. 18.3 CE que en todo caso debe ser objeto de regulación mediante ley orgánica.

El Tribunal Supremo ha contestado de forma negativa a las reiteradas demandas que cuestionaron SITEL. La primera de ellas, planteada por la asociación de internautas, sostuvo que dicho procedimiento vulneraba las condiciones que delimitan la intervención de las comunicaciones por cuanto entendió que corresponde a la ley orgánica delimitadora de la intervención de las comunicaciones y no al RLGT regular la obligación del juez de explicitar en la resolución de intervención el tipo de datos asociados a la comunicación que se pretende intervenir[3]. El Alto Tribunal ha expresado que dicho procedimiento supone la puesta en marcha

---

[1] El artículo 18.3 CE garantiza, de modo especial, el secreto de las comunicaciones postales, telegráficas y telefónicas, por lo que no supone un *numerus clausus*. De tal manera, los modernos medios de comunicación que habitualmente aprovechan las líneas telefónicas, tales como la terminal de un ordenador, también son susceptibles de protección por el artículo 18.3 CE. Véase Ricardo MARTÍN MORALES (1995, p. 45).

[2] Artículo 579 de la Ley de Enjuiciamiento Criminal (en adelante LECrim) en su redacción dada por la Ley Orgánica 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal (BOE nº 126, de 26.05.1988). Párrafo 2º del Artículo único de la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia (BOE nº 109, de 07.05.2002).

[3] STS, 3ª, 5.02.2008 (MP: Manuel Campos Sánchez-Bordona); STS, 1ª, 23.03.2009 (MP: Joaquín Delgado Varela); 1ª,

de un derecho fundamental cuyo contenido esencial está delimitado previamente en la ley orgánica reguladora del artículo 18.3 CE, y en la jurisprudencia del Tribunal Supremo y del Tribunal Constitucional. De tal manera, que las garantías del art. 18.3 CE –los criterios que motivan la intervención de las comunicaciones- no se encuentran desarrolladas en el RLGT, sino en la ley orgánica reguladora de los requisitos de la autorización judicial para intervenir cualesquier tipo de comunicaciones (art. 579 LECrim). Y si bien reconoce la existencia de lagunas legales en relación con dichas condiciones de interceptación, no cree necesaria una mayor previsibilidad legislativa, pues ésta se entiende suplida por la doctrina del Tribunal Supremo y el Tribunal Constitucional, conforme a lo que establece la reciente jurisprudencia del Tribunal Europeo de Derecho Humanos (en adelante TEDH)[1].

Verdaderamente, poco se sabe de la regulación reglamentaria de este procedimiento de intervención de las comunicaciones, y de si las condiciones de intervención que impone conculcan el contenido esencial del art. 18.3 CE en lo relativo a la posibilidad de intervenir las comunicaciones.

SITEL constituye una aplicación informática muy avanzada que permite interceptar no sólo la conversación sino también el paquete de datos que acompaña a la misma, y que se denomina "información asociada a la comunicación". Así pues, la localización geográfica del interlocutor o el tipo de contrato de los interlocutores[2]. Sin embargo, de ello no se deduce que el órgano judicial tenga que explicitar qué datos asociados a la comunicación tienen que intervenirse. La razón estriba en que una vez que la resolución judicial ha explicitado las razones que le llevan a intervenir las comunicaciones –las sospechas objetivas de la presunta comisión de un delito grave, o la necesidad de evitar un peligro que afecte a los intereses nacionales-, el proceso posterior –la información asociada que se recaba como consecuencia de la apertura de las comunicaciones-, ya no queda protegida por el art. 18.3 CE.

El art. 18.3 CE se fundamenta en la explicitación de las razones que inducen al juez a intervenir las comunicaciones. Tiene un significado formal en la medida en que protege el proceso previo a la interceptación de las comunicaciones, con independencia del contenido de la comunicación y de que la misma haya llegado a producirse. De ello se deduce que el RLGT no afecta al contenido esencial del art. 18.3 CE por explicitar los tipos de datos asociados a la comunicación electrónica

---

5.11.2009 (MP: Luciano Varela Castro); 1ª, 5.11.2009 (MP: Luciano Varela Castro).

[1] Auto del TEDH, de 25 de septiembre de 2006 (Abdulkadir Coban c. España).

[2] El correo electrónico supone un tipo de comunicación especial, por cuanto contiene muchos otros datos asociados al contenido de la información, tales como la denominada "identidad" o etiqueta técnica que representa el origen o el destino de cualquier tráfico de comunicaciones electrónicas (art. 84.i RLGT), perteneciente a las otras partes involucradas en la comunicación electrónica (art. 88.1 a y b RLGT), o las identidades de los servicios básicos y suplementarios utilizados por el sujeto objeto de la medida de interceptación (art. 88.1 RLGT, c y d).

que pueden ser recabados tras la intervención, cuanto por la obligación que impone al órgano judicial de incluir, cómo mínimo, alguno de ellos, en la orden judicial de interceptación. Y si bien corresponde a la ley orgánica reguladora del art. 18.3 CE desarrollar los requisitos de la resolución judicial de intervención, de ello no se deriva, necesariamente, que el legislador tenga que enumerar, siquiera, los tipos de datos asociados y adjuntos a la comunicación, y menos, que obligue al juez a especificar en su auto cuáles de estos datos tienen que ser susceptibles de intervención.

Las actuaciones consistentes en la revelación de estos datos a terceros por el agente facultado, o la utilización de dichos datos para un fin diferente al de la intervención de las comunicaciones –la investigación de la presunta comisión de delitos graves- ya no quedan protegidas por el art. 18.3 CE sino por los derechos a la intimidad y a la protección de datos, respectivamente (apartados 1 y 4 del art. 18 CE).

En este trabajo se analiza la regulación jurídica del proceso de intervención de las comunicaciones para verificar su posible incidencia en el contenido esencial del art. 18.3 CE. Se concluye que la ejecución mediante reglamento del proceso de intervención de las comunicaciones electrónicas no afecta art. 18.3 CE, en lo que se refiere a la enumeración de los tipos de datos asociados a las comunicaciones electrónicas que pueden ser susceptibles de intervención junto con el contenido de las mismas. Pues el art. 18.3 CE tiene un significado formal, en la medida en que protege el proceso de la comunicación con independencia del contenido de la misma o de los tipos de datos asociados que sea posible interceptar. Incluso al margen de que la comunicación no exista, porque la persona intervenida no se haya conectado nunca a Internet. Sin embargo, el RLGT cercena el contenido esencial del art. 18.3 CE en lo relativo a obligación del juez a determinar, siquiera, algunos de estos datos en la orden legal de intervención. La razón estriba, en que, en todo caso, corresponde a la ley orgánica y no al reglamento la regulación de las condiciones de intervención legal de las comunicaciones. Ahora bien, ni siquiera es necesario que el legislador orgánico especifique cuántos datos asociados a las comunicaciones tiene que mencionar el auto judicial, pues el fundamento de la intervención de las comunicaciones -las sospechas objetivas de la presunta comisión de delitos graves, o la prevención de la comisión de delitos graves contra los intereses nacionales-, legitiman al juez para determinar libremente qué datos asociados es preciso recabar, en función de los hechos que son objeto de investigación.

## *2. Procedimiento para intervenir las comunicaciones en el 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*

El análisis acerca de la posible incidencia del procedimiento para intervenir las comunicaciones en el contenido esencial del art. 18.3 CE se centra en tres aspectos. En primer lugar, la alusión del

reglamento a la necesidad de que el procedimiento para la ejecución de la intervención de las comunicaciones respete los criterios que delimitan el contenido esencial del art. 18.3 CE en las correspondientes leyes orgánicas. El segundo aspecto se centra en la incidencia del reglamento en las condiciones de la autorización judicial que delimitan el contenido esencial del art. 18.3 CE en lo relativo a la obligación del órgano judicial de mencionar, siquiera, alguno de los datos asociados a la comunicación electrónica. Finalmente, se analiza la obligación que tienen las operadoras de facilitar al agente facultado la información relativa a la interceptación, así como la confidencialidad que éste debe guardar sobre la información que, en todo caso, debe se utilizada para el fin para el que se recaba.

### 2.1. Las leyes orgánicas reguladoras del contenido esencial de la intervención de las comunicaciones

El art. 83 RLGT comienza aludiendo a la necesidad de que los operadores que presten o estén condiciones de prestar servicios de comunicaciones electrónicas respeten las leyes orgánicas que desarrollan el contenido esencial del art. 18.3 CE: art. 579 LCRim y art. único de la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia (BOE nº 109, 7.5.2002).

Estas disposiciones normativas delimitan el contenido esencial del art. 18.3 CE, es decir, desarrollan los criterios de intervención judicial de las comunicaciones telefónicas, postales y telegráficas, proyectando estas condiciones al correo electrónico por considerarse un medio asimilable al teléfono[1].

El art. 579 LECrim condiciona la autorización judicial a la motivación de la existencia de indicios o sospechas objetivas de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. Estos indicios han sido definidos por el Tribunal Constitucional como algo más que meras conjeturas o sospechas subjetivas del juez, si bien algo menos que los indicios racionales que se exigen para el procesamiento en el artículo 384 LECrim[2].

---

[1] La doctrina ha afirmado que resulta censurable que el art. 579 LECrim no haya abordado la regulación de la intervención del correo electrónico con el objetivo de facilitar la investigación de los delitos graves, especialmente de aquellos relacionados con las nuevas tecnologías, pues, de esta forma, se cierra la posibilidad de eventuales recursos de amparo por vulneración de los derechos fundamentales. Véase Antonio Pablo RIVES SEVA (2010, p. 97).

[2] STC, 1ª, 7.4.2010 (MP: Mª Emilia Casas Baamonde); SSTC 1ª, 21.12.2009 (MP: Mª Emilia Casas Baamonde); STC, 1ª, 21.12.2009 (MP: Mª Emilia Casas Baamonde); STC, 1ª, 20.9.2009 (MP: Javier Delgado Barrio); STC, 1ª, 16.6.2009 (MP: Pablo Pérez Tremps); STC, 2ª, 30.1.2006 (MP: Guillermo Giménez Sánchez; STC, 1ª, 8.5.2006 (MP: Javier Delgado Barrio); STC 1ª, 11.9.2006, (MP: Javier Delgado Barrio); STC, 1ª, 3.7.2006 (MP: Javier Delgado Barrio); STC, 2ª, 20.6.2005 (MP: Vicente Conde Martín de Hijas).STC, 2ª, 11.11.2002 (MP: Eugeni Gay Montalvo); STC, 2ª, 9.10.2002 (MP: Vicente Conde Martín de Hijas); STC, 2ª, 11.12.2000 (MP: Vicente Conde Martín de Hijas); STC, Pleno, 5.4.1999 (MP: Tomas S. Vives Anton); STC 1ª, 14.13.1994, (MP: Fernando García-Mon y González de

La previsión legal de los criterios para intervenir las comunicaciones en los supuestos generales se ha caracterizado por su parquedad. El artículo 579 LECrim regulador de las condiciones de la resolución judicial que permite la intervención de la comunicación ha sido, a juicio de la doctrina, poco explícito por cuanto se expresan unas referencias mínimas a los supuestos y forma de proceder[1]. Dicha parquedad ha sido completada por la jurisprudencia del Tribunal Constitucional al precisar que la resolución judicial en la que se acuerda la medida de intervención telefónica o su prórroga debe expresar o exteriorizar las razones fácticas y jurídicas que apoyan la necesidad de la intervención, esto es, cuáles son los indicios que existen acerca de la presunta comisión de un hecho delictivo grave por una determinada persona, así como la determinación del número o números de teléfono de las personas cuyas conversaciones han de ser intervenidas; la resolución judicial también debe determinar el tiempo de duración de la intervención, quiénes deben llevarla a cabo y cómo, y los periodos en los que deba darse cuenta al juez para controlar su ejecución[2]. Finalmente, el Tribunal Constitucional establece la necesidad de exteriorizar en la resolución los datos o hechos objetivos que puedan considerarse indicios de la existencia del delito y la conexión de la persona o personas investigadas con el mismo.

Estos indicios deben ser más que meras conjeturas, pero algo menos que los indicios racionales que se exigen para el procesamiento. El Tribunal Constitucional ha establecido que la relación entre la persona y el delito investigado se expresa a través de la sospecha objetiva. Pero las sospechas, en cuanto meras conjeturas, pertenecen al ámbito de las opiniones subjetivas, por lo que precisan ser apoyadas en datos objetivos para ser justificativas de la interceptación de las comunicaciones. De tal manera, se exige que sean accesibles a terceros, sin los que no serían susceptibles de control. También deben proporcionar una base real de la que pueda inferirse que se ha cometido o se va a cometer el delito sin que puedan consistir en valoraciones acerca de la persona[3]. Estos requisitos de la sospecha deben ser indispensables, dado que si el secreto pudiera alzarse sobre la base de meras hipótesis subjetivas, el derecho al secreto de las comunicaciones quedaría vacío de contenido, desde una perspectiva constitucional.

Así mismo, el art. único de la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia (BOE nº 109, 7.5.2002) condiciona la

---

Regueral); STC 1ª, 17.11.1982 (MP: Rafael Gómez-Ferrer Morant); STC, 2ª, 13.8.1981 (MP: Luis Díez Picazo y Ponce de León).

[1] Ascensión ELVIRA PERALES (2007, p. 23)

[2] STC, 1ª, 5.11.2007 (MP: Pablo Pérez Tremps); STC, 2ª, 8.5.2006 (MP: Elisa Pérez Vera); STC, 1ª, 24.10.2005 (MP: Javier Delgado Barrios); STC, 2ª, 20.6.2005 (MP: Vicente Conde Martín de Hijas); STC, Pleno, 23.10.2003 (MP: Mª Emilia Casas Baamonde); STC, 2ª, 11.12.2000 (MP: Vicente Conde Martín de Hijas); STC, Pleno, 5.4.1999 (MP: Tomas S. Vives Anton).

[3] STC, 1ª, 11.9.2006 (MP: Javier Delgado Barrio); STC, 2ª, 29.1.2001 (MP: Julio Diego González Campos); STC, 2ª, 11.11.2000 (MP: Vicente Conde Martín de Hijas); STC, 2ª, 27.9.1999 (MP: Carles Viver Py-Sunyer); STC, 1ª, 27.9.1999 (MP: Pablo García Manzano); STC, Pleno, 5.4.1999 (MP: Tomas S. Vives Anton).

autorización del magistrado del Tribunal Supremo a que la solicitud motivada de la interceptación del Secretario de Estado Director del Centro Nacional de Inteligencia esté basada en la prevención o erradicación de cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de Derecho y sus instituciones (art. 4b) de la Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia (BOE nº 109, 7.5.2002)).

La interceptación de las comunicaciones que realiza el Centro Nacional de Inteligencia se subordina a las condiciones establecidas en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del Control Judicial Previo del Centro Nacional de Inteligencia. En ella se regula el control judicial previo de entradas domiciliarias o de intervención de las comunicaciones. La exposición de motivos de dicha ley ha recordado que la delimitación del derecho fundamental a la inviolabilidad del domicilio, o al secreto de las comunicaciones, exige, en virtud del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que esté prevista en la ley y que 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

El reglamento ha explicitado la necesidad de respetar el contenido esencial del art. 18.3 CE regulado en las leyes y en la jurisprudencia. Eso significa que la falta de previsión legislativa de los criterios que son necesarios para garantizar la seguridad jurídica de la intervención, no puede ser suplida por el reglamento, pues ello afecta al contenido esencial del art. 18.3 CE.

La función del reglamento no es otra que la ejecución del procedimiento de intervención. Ello significa que puede completar o desarrollar el contenido de la ley pero no puede sustituir las condiciones establecidas en ella, o añadir nuevos criterios que afecten al contenido esencial del art. 18.3 CE. El RLGT ha aclarado el significado de algunos de los criterios que autorizan la intervención legal, pero también ha añadido algunas condiciones a la intervención judicial de las comunicaciones afectando al contenido esencial del art. 18.3 CE, como se verá más adelante.

### 2.2. La obligación de explicitar en la resolución judicial algunos de los datos asociados a las comunicaciones electrónicas

El RLGT ha comenzado desentrañado el sentido de alguno de los criterios judiciales de intervención al señalar que la alusión del juez a la intervención de las comunicaciones electrónicas se entiende inclusiva de cualquier modalidad relativa a este tipo de comunicación (vídeo, audio, de intercambio de mensajes, de ficheros o de transmisión de facsímil (art. 87.2 RLGT)), al tiempo que excluyente de cualquier otro tipo de comunicación que no se mencione expresamente en la orden de intervención judicial (art. 87.1 RLGT).

La polémica social e institucional del desarrollo reglamentario del proceso de intervención

judicial de las comunicaciones se ha originado por la enumeración de los tipos de datos asociados a la comunicación electrónica que pueden ser objeto de intervención judicial. Se ha entendido que dicha regulación vulnera el secreto de las comunicaciones, y el derecho a la intimidad de los sujetos intervenidos.

La especialidad de este tipo de comunicaciones electrónicas, que deriva de la complejidad de estas nuevas tecnologías, hace que junto al contenido de las mismas el órgano judicial pueda recabar todo un paquete de datos que acompaña a la misma y que puede ser de gran ayuda para esclarecer hechos presuntamente delictivos o prevenir atentados. Ello ha sido tenido en cuenta en el reglamento al explicitar los tipos de datos asociados a las comunicaciones electrónicas que por ser de utilidad para la investigación, pueden ser solicitados por el juez. Así, por ejemplo, la dirección de correo electrónico, el número de identificación del terminal, o los servicios básicos y complementarios utilizados por la persona intervenida (art. 88 RLGT). En este sentido, el reglamento insta a los operadores a facilitar al agente facultado (policía judicial, o personal del Centro Nacional de Inteligencia habilitado por una autoridad judicial para materializar una intervención legal (art. 84 e) RLGT)) los datos asociados que se mencionan expresamente en la orden de interceptación legal (art. 88.1 RLGT) salvo que, por las características del servicio, dichos datos no estén a su disposición. El reglamento también alude a la posibilidad de que mediante disposición reglamentaria, puedan mencionarse, *a posteriori*, otros datos asociados susceptibles de ser facilitados por los operadores.

En contra de la idea de que la mención reglamentaria de los datos asociados a las comunicaciones electrónicas vulnera el art. 18.3 CE, se debe argumentar que el secreto de las comunicaciones tiene un significado formal que trasciende tanto a la confidencialidad de la comunicación, como a la posibilidad de intervenir las comunicaciones por resolución judicial motivada. Ello significa que el art. 18.3 CE garantiza el proceso previo de la intervención de la comunicación con independencia de la naturaleza íntima o no de su contenido, es decir, al margen de lo comunicado. Concluido el proceso en que la comunicación consiste, desaparece también la protección constitucional[1]. En este sentido, el destino de los datos obtenidos como consecuencia de la orden legal de intervención no queda protegido por el art. 18.3 CE sino por el derecho a la intimidad o a la protección de datos. El art. 18.3 CE protege el proceso previo a la intervención de las comunicaciones siempre que ésta vaya precedida de una resolución judicial constitucionalmente conforme mas no garantiza la protección de la intimidad de estos datos, en el sentido de prohibir la revelación a terceros de las comunicaciones interceptadas, ni tampoco la protección de datos personales, en el sentido de vedar la utilización de los mismos para otros fines que no sean el esclarecimiento de los hechos presuntamente delictivos[2].

---

[1] Javier JIMÉNEZ CAMPO (1987, p. 44).

[2] Por el contrario, la doctrina ha expresado que la protección constitucional del secreto de las comunicaciones supone el instrumento jurídico para garantizar el derecho a la intimidad. Veánse: Ricardo MARTÍN MORALES (1995, p. 44) y Blanca RODRÍGUEZ RUIZ (1998, pp. 1 y 133). El secreto de las comunicaciones constituye un aspecto de la intimidad, aunque con perfiles propios por la relevancia del medio empleado (véase, Francisco BALAGUER CALLEJÓN [1995 p. 13]), cual es la comunicación, pero entendiendo que el objeto de protección es la intimidad, o

La mención reglamentaria de los tipos de datos asociados resulta muy operativa para comprender el alcance de este tipo de comunicaciones. En este sentido, no es necesario que estos datos tengan que regularse mediante ley orgánica, pues no forman parte del contenido esencial del art. 18.3 CE. Así lo ha entendido el Tribunal Supremo quien ha reconocido que los datos asociados que se mencionan en los apartados 2 y 3 del art. 88 RLGT además de haber sido reproducidos en los apartados 6º y 7º del art. 33 LGT, no afectan al contenido material de las comunicaciones, sino que son datos instrumentales de información asociada que –siendo relevantes para el fin de la interceptación- no tienen por qué ser incluidos por el legislador ordinario quien tiene libertad de configuración normativa. Por tanto, corresponde a los jueces que autorizan la intervención determinar, en su caso, la procedencia o improcedencia de excluir los referidos datos identificativos en el marco de las actuaciones que conozcan, de acuerdo con los principios de necesidad y de proporcionalidad[1]. Sin embargo, El RLGT ha ido más allá incidiendo en las condiciones que tiene que expresar la autorización judicial para intervenir las comunicaciones, al exigir que el juez incluya, al menos, uno de los siguientes datos asociados en la orden de intervención para que las operadoras los puedan facilitar: la identificación del abonado o usuario, la situación geográfica donde se encuentre el punto de terminación de red al que el operador da servicio, el identificador de punto de terminación de red (dirección) o de terminal al que el proveedor de servicios de comunicaciones electrónicas da servicio, el código de identificación en el caso de que el usuario sea el que active el terminal para la comunicación, y cualquier otra identidad definida conforme al art. 84 i) RLGT que corresponda al sujeto especificado en la orden de intervención judicial (art. 90 RLGT).

En reciente jurisprudencia, el Tribunal Supremo ha reconocido que la interceptación de los datos identificativos de un titular o de un terminal no deben ser encuadrados dentro del secreto de las comunicaciones sino en el marco del derecho a la intimidad personal, o también en el de la protección que se realiza a través de la ley de protección de datos de carácter personal[2]. Así

---

de forma más genérica, la vida privada (véase, Lucrecio REBOLLO DELGADO [2005, p. 316]). También se ha establecido que el secreto de las comunicaciones, si bien no es un derecho equivalente al de la intimidad, constituye una garantía formal cuyo objeto es la protección del derecho a la intimidad cuyo significado es material (véase, Francisco BALAGUER CALLEJÓN [1995, p. 13]). La jurisprudencia del Tribunal Constitucional ha evolucionado desde entender que el art. 18.3 CE tiene un significado formal a considerar que el secreto de las comunicaciones también tiene un significado sustancial, en la medida en que debe dirigir su objeto a la protección de nuevos ámbitos de protección. Pues si bien, en un primer momento, ha entendido que el secreto de las comunicaciones se predica del proceso que permite la comunicación (STC , 2ª, 29.11.1984 [MP: Luís Díez-Picazo y Ponce de León]) en garantía de la impenetrabilidad de la comunicación para terceros, con posterioridad ha aducido avances tecnológicos de las telecomunicaciones producidos especialmente en el campo de la informática para modificar su criterio y entender necesaria una revisión del concepto de comunicación y de su objeto de protección que garantice otros derechos: intimidad y protección de datos[2]. Así es como termina reconociendo que el art. 18.3 se predica no sólo de la comunicación sino también de lo comunicado (STC, 1ª, 3.4.2002 [MP: Fernando Garrido Falla]).

[1] STS, 3ª, 5.2.2008 (MP: Manuel Campos Sánchez-Bordona).

[2] STS 2ª, 18.3.2010 (MP: José Ramón Soriano Soriano).

mismo, ha diferenciado entre datos conectados a la comunicación y datos autónomos verificados con ocasión de la apertura de las comunicaciones. De tal manera, distingue entre los datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto de lo comunicado conforme al art. 18.3 CE, y los datos o circunstancias personales referentes a la intimidad de una persona que son autónomos o desconectados de cualquier comunicación, protegidos por el derecho a la protección de los datos personales[1].

La apertura de estos datos asociados a las comunicaciones electrónicas permite recabar información que puede ser muy útil para el caso que se está investigando. Así, por ejemplo, la apertura de las comunicaciones electrónicas permite conocer desde dónde se envía un correo electrónico, el domicilio en el que el proveedor realiza las notificaciones, o, los servicios básicos y suplementarios que utiliza la persona intervenida (art. 88.1 RLGT). En este sentido, es laudable que el reglamento explicite sus distintas modalidades pues ello puede ayudar al esclarecimiento de los hechos presuntamente delictivos. Sin embargo, de ello no se sigue que el juez esté obligado a mencionar algunos de estos datos en la orden de interceptación, pues la delimitación de los criterios para intervenir las comunicaciones, en cuanto forma parte del contenido esencial del art. 18.3 CE corresponde a la ley orgánica y no al reglamento. Incluso, tampoco es necesario que la ley orgánica prevea qué tipo de datos asociados tiene que mencionar el juez en la orden judicial de interceptación, pues, la variedad de supuestos que analiza, escapa al control de la ley. El órgano judicial tiene que tener libertad para decidir no sólo qué tipo de comunicaciones interviene, sino también cuáles de entre los datos adjuntos o asociados a esas comunicaciones electrónicas es preciso intervenir. Es más, el desconocimiento de la información habida tras la interceptación y la necesidad de pruebas son razones suficientes para que el juez no tenga, siquiera, que hacer diferenciación entre unos datos asociados –los incluidos en la orden legal-, y otros –los que no precisa interceptar-. Una vez que el órgano judicial ha expresado las razones constitucionalmente conformes por las que es preciso intervenir las comunicaciones electrónicas, el contenido de las mismas y los datos asociados no quedan protegidos por el art. 18.3 CE., sino en todo caso, por el derecho a la intimidad y a la protección de datos.

El derecho fundamental protege todo el proceso que permite la comunicación, mientras que el art. 18.1 CE ampara la reserva que incumbe a quienes hayan interceptado la comunicación cuando su contenido[2] tenga carácter íntimo o reservado[3]. Ello significa que el art. 18.1 CE protege frente a la intromisión en la vida íntima y privada de las personas mediante el emplazamiento de aparatos de audio y vídeo, o frente a la revelación por terceros de datos que forman parte de ese reducto íntimo de la persona (párrafos 1º, 2º, 3º y 4º del artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia

[1] STS 2ª, 18.3.2010 (MP: José Ramón Soriano Soriano).

[2] "La comunicación es a efectos constitucionales el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos": STC, 1ª, 9.10.2006 (MP: Emilia Casas Baamonde).

[3] Inmaculada MARÍN ALONSO (2005, p.141.)

imagen).

La reafirmación sobre la naturaleza formal del art. 18. 3 CE es determinante para entender que no existe, siquiera, una obligación de enumerar mediante ley orgánica los datos asociados a las comunicaciones electrónicas que deben ser explicitados por el juez en la orden legal de intervención; pues en la medida en que dicha información se recaba como consecuencia de la orden judicial de interceptación, ya no queda protegida por el art. 18.3 CE. Una vez que el juez ha argüido las razones constitucionalmente conformes por las que es preciso intervenir, la información que se obtiene no tiene por qué limitarse al contenido de lo comunicado, salvo que el órgano judicial explicite qué datos asociados, de entre los que menciona el RLGT, deben ser intervenidos, o determine de forma explícita que no sea necesario recabarlos.

### 2.3. La obligación de transmitir la información intervenida al agente facultado y la confidencialidad de la información obtenida

El RLGT ha determinado quiénes están legitimados para recabar la información facilitada por las operadoras así como la obligación de éstos de guardar confidencialidad sobre el contenido de la misma. El proceso de ejecución comienza con la recepción de la orden de interceptación por parte de las operadoras (sujetos obligados, en virtud del art. 86 RLGT). Una vez recibida dicha orden tienen que transmitir la información a los centros de recepción de las interceptaciones, por medio de interfaces (art. 95 RLGT) que son las localizaciones físicas o lógicas dentro de las instalaciones de los operadores en las que se proporcionan las comunicaciones electrónicas interceptadas y la información relativa a la interceptación (art. 84 b) RLGT).

El RLGT obliga a que las comunicaciones facilitadas por las operadoras sean entregadas exclusivamente al agente facultado, es decir, al policía judicial, o al personal del Centro Nacional de Inteligencia habilitado por una autoridad judicial para materializar dicha interceptación legal (art. 84 e) RLGT). Con ello, se trata de impedir la manipulación de los mecanismos de intervención y de garantizar la autenticidad, confidencialidad e integridad de la información obtenida con la interceptación (art. 97 RLGT). También alude al plazo de ejecución de la orden de interceptación legal, entendiendo que es el juez quien tiene que fijarlo expresamente en la orden de interceptación legal. De tal manera que cuando no se regule de modo explícito, la orden se ejecute antes de las 12 horas del día laborable siguiente al que el sujeto obligado reciba la orden de interceptación legal (art. 99 RLGT).

*A priori*, podría pensarse que la obligación de entregar la información al agente facultado cercena el contenido esencial del art. 18.3 CE en la medida en que el órgano judicial puede solicitar mediante auto judicial que la información le sea entregada directamente por la operadora sin necesidad de que el agente facultado intervenga en su tramitación. Avalarían este argumento razones técnicas, como el hecho de que antes la función del agente facultado era imprescindible, en la medida en que las llamadas telefónicas se efectuaban de forma manual, y se hacían, de una en una, mediante la desviación de la llamada a un número que

facilitaba la policía, mientras que, ahora, SITEL es un sistema automatizado. Ello significa que una vez introducidos los parámetros de la interceptación, no se precisa intervención humana para realizarla y trasmitirla en tiempo real a un centro de interceptación[1]. Sin embargo, el significado formal del art. 18.3 CE se esgrime, una vez, en defensa de la intervención del agente facultado. Pues el art. 18.3 CE protege el proceso previo de la intervención, más no el proceso posterior de ejecución de la intervención. Es decir, que una vez que el órgano judicial ha explicitado las razones constitucionalmente conformes de la intervención, la recepción o no de estos datos por el agente facultado, no queda protegida por el art. 18.3 CE. Los arts. 33.8 LGT y 89.3 RLGT han desarrollado la función del agente facultado al determinar la posibilidad de éste de recabar con carácter previo a la ejecución de la orden de interceptación legal la información relativa a los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas. Parece que la redacción no ha sido muy afortunada, pues podría entenderse que la cesión de los datos previa a la intervención vulnera el art. 18.3 CE, a no ser que se entienda que la información facilitada lo es en un momento previo a la ejecución de la intervención, pero posterior a la autorización judicial motivada de la necesidad de intervenir[2].

El RLGT alude a la garantía del derecho a la intimidad de las personas intervenidas, frente a la posible revelación de datos a terceros por el policía judicial o por las operadoras (arts. 92 y 93 RLGT). Sin embargo, no se refiere a la protección de datos personales (art. 18.4 CE), garantía a la que se alude el art. 34 LGT refiriéndose únicamente a los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público. Sería preciso que la ley regulara este recordatorio relativo a la protección de los datos personales no sólo para las operadoras, sino también para el agente facultado, destinatario indispensable de la información, a la luz de la ley y del reglamento.

En lo relativo al derecho a la intimidad, se ha dicho ya, el artículo 18.3 CE es un derecho autónomo pues sólo protege frente a la interceptación o el conocimiento antijurídico de las

---

[1] "Con la explosión tecnográfica de la telefonía móvil, y, más en concreto, de las comunicaciones mediante tarjeta de prepago, y la revolución tecnológica favorecida por la expansión de la red internet, lo que hasta ese momento eran componentes inmanentes y de relativamente fácil acceso a las fuerzas policiales, pasaron a ser factores relativos, por no decir extraordinariamente volátiles, cuyo acceso suele ser extraordinariamente complejo y tortuoso. La facilidad con que se da de alta un teléfono móvil con tarjeta de prepago o se registra una cuenta de correo electrónico, blog o página web, no tiene más límites que la capacidad económica del usuario y, en el supuesto de las comunicaciones a través del a Red de Redes, la diligencia del aperturante de guardar en un papel o en su memoria, los nombres de usuario y clave de acceso", véase José Luís RODRÍGUEZ LANZ (2009, pp. 1-2).

[2] Así lo ha expresado la doctrina, entendiendo que la polémica surgida se originó precisamente por pensar que la cesión de datos de carácter personal lo era con carácter previo a la interceptación (véase, Juan José GONZÁLEZ LÓPEZ, [2008, p. 37]).

comunicaciones ajenas, con independencia de que, con posterioridad se difunda el contenido de la comunicación interceptada[1]. El art. 18.3 CE queda vulnerado por la mera interceptación sin autorización judicial, o porque dicha resolución del juez no esté motivada, aunque el contenido de la comunicación no sea íntimo, al margen de que no se difunda la comunicación íntima intervenida inmotivadamente a terceros, o, incluso, aunque no exista dicha comunicación porque no ha llegado a producirse. Por tanto, los datos obtenidos como consecuencia de la interceptación no está protegidos el art. 18.3 CE sino por el derecho a la intimidad en el sentido de que al agente facultado le está vedado revelar estos datos a terceros.

La intervención de las comunicaciones también es un derecho independiente de la protección de los datos personales. El art. 18.4 CE determina el derecho a controlar el uso de los datos insertos en un programa informático[2] y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención[3]. El art. 18.4 CE "otorga a su titular una posición jurídica de contenido positivo que se conforma sobre un haz de facultades destinadas a controlar el uso de información personal, tanto en su momento inicial de la recogida de datos como en las fases posteriores del tratamiento"[4]. Se define por el Tribunal Supremo como el derecho de toda persona física a la reserva y control de los datos que le conciernen en los distintos ámbitos de la vida, de tal manera que pueda decidir siempre cómo, cuando, y en qué medida esa información puede ser recogida, almacenada, tratada y, en todo caso, transferida a terceros (STS, 3ª, 14.2.2006).

La utilización de los datos personales interceptados en virtud del art. 18.3 CE para la investigación de la presunta comisión de delitos graves se regula en el art. 11.2.d), al precisar que no será necesaria la autorización de cesión de los datos por parte de su titular cuando la comunicación tenga por destinatarios, entre otros, a jueces y tribunales. El derecho a la protección de datos personales en un derecho independiente del art. 18.3 CE, lo que significa que la utilización de los datos personales para otro fin que no sea el de la investigación de los hechos presuntamente delictivos no vulnera el contenido esencial del art. 18.3 CE sino el art. 18.4 CE.

## *3. Conclusión*

1 STC, 2ª, 29.11.1984 (MP: Luis Díez-Picazo y Ponce de León). En este sentido, véanse: Juan Mª BILBAO UBILLOS (1997, p. 807–808); Javier JIMÉNEZ CAMPO (1987, p. 41) y Ricardo MARTÍN MORALES (1995, p. 39-44).

2 STC, Pleno, 13.5.1991 (MP: Eugenio Díaz Eimil); STC 1ª, 18.8.1993, (MP: Fernando García Mon y González-Regueral); STC 1ª, 9.5.1994 (MP: Miguel Rodríguez-Piñero y Bravo-Ferrer); STC, Pleno, 30.11.2000 (MP: Julio Diego González Campos).

3 Ana Isabel HERRÁN ORTIZ (2002, p. 109).

4 Isabel Cecilia DEL CASTILLO VÁZQUEZ (2007, p. 199).

En líneas generales, la regulación reglamentaria del procedimiento de interceptación de las comunicaciones no afecta a las condiciones de la resolución judicial de interceptación que delimitan el contenido esencial del art. 18.3 CE porque desarrolla el proceso de ejecución de la intervención de las comunicaciones, una vez que el órgano judicial aduce sospechas objetivas de la presunta comisión de un delito grave, o razones que previenen frente a la posible comisión de delitos que afectan a la integridad territorial del Estado o a los intereses nacionales.

La virtualidad del RLGT reside en la explicitación de los tipos de datos asociados a las comunicaciones electrónicas que pueden ser objeto de intervención. La posibilidad de que estos datos puedan ser intervenidos junto con el contenido de las comunicaciones no afecta al contenido esencial del art. 18.3 CE, en la medida en que la intervención de las comunicaciones tiene un significado formal que protege el proceso de la comunicación previo a la interceptación, con independencia del contenido íntimo o no de la comunicación; de que ésta no llegue a producirse, o de que su contenido, irrelevante para el fin de la intervención, adjunte, sin embargo, datos asociados que constituyan pruebas esclarecedoras de los hechos presuntamente delictivos. Por tanto, dichos datos no quedan protegidos por el art. 18.3 CE, sino por el art. 18.1 CE, en el sentido de vedar que los datos sean revelados a terceros ajenos a las personas autorizadas en el procedimiento, o por el art. 18.4 CE en el sentido de prohibir que los datos sean utilizados para otro fin diferente para el que son recabados. Sin embargo, el RLGT incide en las condiciones de la autorización judicial de intervención de las comunicaciones en la medida en que obliga al órgano judicial a explicitar, como mínimo, alguno de los datos asociados que figuran de modo expreso en el art. 90 RLGT. Que el reglamento explicite los distintos tipos de datos asociados que pueden ayudar a la investigación del caso no significa que el juez tenga que estar obligado a mencionar algunos de estos datos en la orden de interceptación. El fundamento del art. 18.3 CE –los criterios legales que delimitan la intervención judicial de las comunicaciones- determina la falta de obligación del legislador orgánico de incluir, siquiera, qué tipo de datos asociados tienen que mencionar el juez en la orden legal de intervención. De tal manera, que el juez tenga libertad para mencionar o no los datos asociados que precisa intervenir en función de los hechos que precise investigar.

La alusión a la posibilidad del agente facultado de recabar datos personales con carácter previo a la ejecución de la intervención judicial, garantiza el art. 18.3 CE si se entiende que dicha facilitación de datos es previa al procedimiento de ejecución pero posterior a la orden legal de intervención. No obstante, sería conveniente una reforma que deje muy claros estos términos.

## *4. Bibliografía*

Francisco BALAGUER CALLEJÓN (1995), Prólogo a la obra de Ricardo MARTÍN MORALES, *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid.

Juan Mª BILBAO UBILLOS (1997), *La eficacia de los derechos fundamentales frente a particulares,* Centro de Estudios Políticos y Constitucionales, Madrid, 1997.

Isabel Cecilia DEL CASTILLO VÁZQUEZ (2007), *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, Thomson-Civitas, Cizur Menor.

Ascensión ELVIRA PERALES (2007), *Derecho al secreto de las comunicaciones*, Iustel, Madrid.

Juan José GONZÁLEZ LÓPEZ, (2008), "Comentarios a la Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones", *Revista General de Derecho Procesal*, n. 16, p. 37.

Ana Isabel HERRÁN ORTIZ (2002), *El derecho a la intimidad en al nueva ley orgánica de protección de datos personales*, Dykinson, Madrid, p. 109

Javier JIMÉNEZ CAMPO (1987) "La garantía constitucional del secreto de las comunicaciones", *REDC*, 20/1987, p. 44.

Inmaculada MARÍN ALONSO (2005), *El poder de control empresarial sobre el uso del correo electrónico en la empresa*, Tirant lo Blanch, Valencia.

Ricardo MARTÍN MORALES (1995), *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid.

Lucrecio REBOLLO DELGADO (2005), *El derecho fundamental a la intimidad*, Dykinson, Madrid.

Antonio Pablo RIVES SEVA (2010), *Intervención de las comunicaciones en el proceso penal*, Bosch, Barcelona.

José Luis RODRÍGUEZ LANZ (2009), "Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas", *Diario La Ley*, nº 7086, pp. 1-2.

Blanca RODRÍGUEZ RUIZ (1998), *El secreto de las comunicaciones: tecnología e intimidad*, McGraw Hill, Madrid.