DERECHO AL SECRETO DE LAS COMUNICACIONES TELEFÓNICAS. UN RETO PARA LA BUENA ADMINISTRACIÓN

JOSÉ RON ROMERO

Abogado
Profesor de Derecho Administrativo
Universidad de A Coruña

Recepción: 15 de junio de 2011
Aprobado por el Consejo de Redacción: 15 de julio de 2011

RESUMEN: El presente trabajo intenta conceptuar, bajo el prisma de la Constitución Española de 1.978, el derecho al secreto de las comunicaciones; su interceptación legal y el procedimiento o sistema utilizado para su ejecución; y reflexionar sobre algunas cuestiones que plantea esa interceptación y el SITEL para la buena Administración.

PALABRAS CLAVE: Derechos fundamentales. Libertad y dignidad de la persona. Secreto de las comunicaciones. Interceptación legal. SITEL. Gobernanza.

ABSTRACT: This paper attempts to conceptualize, through the prism of the Spanish Constitution of 1978, the right to privacy of communications, its lawful interception and the procedure or system used for execution, and reflect on some issues raised by the interception and SITEL to good Administration.

KEYWORDS: Fundamental Rights. Freedom and dignity. Secret communications. Lawful interception. SITEL. Gobernance.

SUMARIO: I. INTRODUCCIÓN. II. PANORAMA NORMATIVO-JURÍDICO. III. DERECHO AL SECRETO DE LAS COMUNICACIONES E INTERVENCIÓN TELEFÓNICA. IV. LA INTERCEPTACIÓN LEGAL Y EL SISTEMA SITEL. V. ALGUNAS CUESTIONES QUE PLANTEA LA INTERCEPTACIÓN Y EL SITEL PARA LA BUENA ADMINISTRACIÓN.

I. INTRODUCCIÓN

El derecho al secreto de las comunicaciones recibe su primera formulación en el moderno constitucionalismo con un Decreto de la Asamblea Nacional francesa de 10 de agosto de 1.790 que, en consonancia con su tiempo, utiliza la expresión "le secret des lettres".

La historia constitucionalista española, con la "impuntualidad histórica que nos caracteriza", utilizando las palabras del profesor JIMÉNEZ CAMPO[1], recoge este derecho en las Constituciones de 1.869[2], 1.876[3] y 1.931[4], hasta su formulación actual en la de 1978 (CE), donde su artículo 18, párrafo 3º, garantiza el secreto de las comunicaciones y, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial[5].

Esta defensa de la privacidad o intimidad del individuo (la "intimité" francesa, la "privacy" anglosajona o la "reservatezza" italiana), del secreto de las comunicaciones entendido como un derecho de la libertad de la persona, de la sociedad, frente al Estado, es reflejo de lo contenido en tres grandes Tratados Internacionales suscritos por España: la Declaración Universal de Derechos Humanos (1948)[6], el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950 (CEDH)[7] y el Pacto Internacional de Derechos Civiles y Políticos del año 1.966[8].

Dos consideraciones previas. Una, el artículo 10.2 de la CE impone la interpretación de las normas relativas a derechos fundamentales conforme a los tratados internacionales

1 JIMÉNEZ CAMPO, J., "La garantía constitucional del secreto de las comunicaciones", *Revista Española de Derecho Constitucional*, núm. 20, mayo-agosto 1987, pág. 35.

2 Su artículo 7 dispone que "en ningún caso podrá detenerse ni abrirse por Autoridad gubernativa la correspondencia confiada al correo, ni tampoco detenerse la telegráfica. Pero en virtud de auto de Juez competente podrá detenerse una y otra correspondencia, y también abrirse en presencia del procesado la que se dirija por el correo".

3 Este texto constitucional protege dicho derecho en dos artículos; el número 7: "No podrá detenerse ni abrirse por la autoridad gubernativa la correspondencia confiada al correo; y el 8: "Todo auto... de detención de la correspondencia, será motivado".

4 La Constitución Republicana en su artículo 32 deja "garantizada la inviolabilidad de la correspondencia en todas sus formas, a no ser que se dicte auto judicial en contrario".

5 No salió adelante la redacción "salvo resolución judicial motivada" propuesta por los grupos Minoría Catalana, Mixto y Socialista.

6 En su artículo 12 nos dice que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o 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".

7 "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia", reza su artículo 8.

8 El artículo 17.1 proclama que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia".

ratificados por España; lo cual hoy en día se hace extensivo a la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH)[9]. Y otra, que aún cuando los textos internacionales antes citados no hacen alusión alguna al concepto de "comunicaciones telefónicas", el TEDH en sus sentencias de 6 de septiembre de 1978 (caso Klass), de 2 de agosto de 1984 (caso Malone) y de 24 de abril de 1990 (casos Kruslin y Huvig) deja perfectamente establecido que este concepto forma parte del derecho a la intimidad y al secreto de las comunicaciones.

Lo que en definitiva estos textos legales tratan de conjugar, como reconoce el mismo TEDH[10], son dos aspectos que laten en la vida diaria de las sociedades democráticas.

De una parte está la persona, el individuo, que desea vivir la vida según su propia elección, conforme a sus formas, gustos y preferencias, con la mayor libertad posible, procurando evitar que alguien se inmiscuya en su proyecto vital sin su consentimiento o aprobación. No quiere que el Gobierno y la Administración le marquen la hoja de ruta en su actuación diaria. Y de ahí surge esa garantía de derechos frente a posibles injerencias, ataques, vigilancias y demás actos abrasivos de los poderes públicos.

En el otro peso de la balanza se asienta el grupo, la sociedad, lo de todos; en definitiva, el interés general, de forma que el ejercicio de la libertad individual no puede vulnerar o poner en peligro el igual derecho de los demás. Por ello surge el contrapeso de la autorización judicial.

En este contexto surgen en el siglo XX, y así continuamos en el XXI, importantes avances científicos y técnicos, especialmente en las áreas de telecomunicaciones, tratamiento de datos, técnicas informáticas y telemáticas, cuya utilización por el poder político puede suponer un peligro para el derecho de la persona o individuo al secreto de sus comunicaciones, a su libertad, y también a su intimidad. Estamos frente al Estado, a su poder ejecutivo, que con su Administración Pública, so pretexto y utilización del concepto tan manido "defensa del interés general", muchas veces no tan general, procede a realizar una importante función investigadora, obteniendo valiosísima información sobre actuaciones concretas de ciudadanos. Si dicha información se transforma en prueba judicial y sirve para proteger al grupo social el objetivo está cumplido y los brazos de la balanza compensados. Pero si se produce la vigilancia constante del "Gran Hermano", la "telepantalla" que describe ORWELL en su novela *1984*, nos meteríamos en un peligroso laberinto con un final incierto para el Estado de Derecho, una auténtica distopía[11].

9 En este sentido puede verse la STC de 26 de marzo de 1996.

10 En su Sentencia de 6 de septiembre de 1978, caso Klass, juzga inherente al sistema del Convenio una cierta forma de conciliación entre los imperativos de la defensa de la sociedad democrática y aquellos otros de la salvaguarda de los derechos individuales.

11 La distopía, por contraposición a utopía, describe una sociedad opresiva y cerrada sobre sí misma, generalmente bajo el control de un gobierno autoritario, pero que es presentada a los ciudadanos de a pie como una utopía. La distopía es el peor de los mundos, la sumisión definitiva y absoluta, el sueño de todo gobernante hecho realidad, y será tanto más efectiva cuanto mayor grado de satisfacción produzca en el ciudadano. Es lo que el autor sueco LUNDWALLl, Sam Jerrie define como "la pesadilla con aire acondicionado". La palabra distopía no está recogida en el Diccionario de la Real Academia Española, ¡qué casualidad!, pero si aparece registrada por SECO REYMUNDO, M.; ANDRÉS PUENTE, O.; y RAMOS, G., *Diccionario del Español Actual,* Aguilar, Madrid, 1999, pág. 1647. AL respecto pueden verse los artículos de NÚÑEZ LADEVEZA, L., "De la utopía clásica a la distopía actual" y "Sobre el proceso

Un caso muy significativo de regulación administrativa del secreto de las telecomunicaciones causando una profunda injerencia en la libertad e intimidad del ciudadano se produce en EE.UU como consecuencia de los atentados del 11 de septiembre de 2001 en Nueva York. A raíz de este suceso, que produjo una conmoción e impacto en la población difícil de calibrar, se aprueba con una abrumadora mayoría, la Ley Patriótica (Usa Patriot Act)[12], que en aras de combatir el terrorismo, permite que el Estado y su Administración, entre otros aspectos, incremente las facultades de los servicios de inteligencia para vigilar las comunicaciones telefónicas y de correo electrónico, así como los registros públicos y privados (médicos, financieros, libros solicitados en las bibliotecas, etc.), sin que para ello se requiera una autorización judicial previa. El Gobierno americano aduce razones de lucha contra el terrorismo, y le resulta mucho más fácil justificar el control sobre la vida de todas las personas, restringiendo sus libertades y garantías constitucionales, especialmente aquéllas referidas a la esfera de su intimidad.

La cuestión, el problema está en enmascarar, bajo el concepto de "Seguridad Nacional y Terrorismo", un asunto de "Información y Comunicación" que debería regularse como tal. Es de agradecer que Europa haya hecho un mayor esfuerzo para enmarcar este tipo de medidas dentro de sus valores de libertad.[13] Con todo, como indica RODRÍGUEZ-ARANA, la tentación intervencionista siempre está al acecho y no pocos Gobiernos y Administraciones públicas ceden ante la posibilidad de aplicar técnicas de control social que garanticen, en lugar de los derechos de los ciudadanos a realizarse libremente en la sociedad, la supervivencia política[14].

El quid es establecer, regular cuando en un Estado social y democrático de Derecho 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 libertades de los demás necesitan que se efectúe una injerencia en el derecho a la libertad de comunicaciones del individuo; definir en qué forma discurrirá esa inmersión, qué

de la utopía a la distopía", *Revista de Estudios Políticos*, números 44 (marzo-abril 1985, págs. 45 y ss.) y 52 (julio-agosto 1986, págs. 111 y ss.), respectivamente.

12 La denominada USA PATRIOT Act (Uniting and Strengthening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism Act). Public Law 107-56, firmada por George W. Bush el 26 de octubre de 2001, se modificó posteriormente a través de la USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 y la USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006. Es muy interesante el rechazo mostrado por la American Library Association (ALA), debido a que con esta normativa se afectó de forma negativa a las bibliotecas en la medida en que aumentó la capacidad del FBI para obtener legalmente, en forma de citaciones, órdenes de registro y escuchas telefónicas, los registros de cualquier biblioteca del tipo que sea, es decir, de espiar a las personas usuarias que se consideraban peligrosas, perdiéndose por lo tanto la confianza que estas personas pudieran tener en los centros. Si el FBI recibe permiso, plantea la ALA, podrá realizar el seguimiento de determinadas personas en Internet, y si se le permite la instalación de hardware o software en los ordenadores de la biblioteca o incluso la confiscación del ordenador o hardware de almacenamiento, lo que ya significaría una pérdida absoluta de la confianza.

13 La Resolución del Consejo de la Unión Europea de 17 de enero de 1995 en su segundo párrafo ya dice: "Reiterando la necesidad de respetar, en la aplicación de las medidas de interceptación de las telecomunicaciones, el derecho al respeto de la vida privada de las personas consagrado por las leyes nacionales aplicables."

14 RODRÍGUEZ-ARANA MUÑOZ, J., *El Buen Gobierno y la Buena Administración de Instituciones Públicas*, Navarra, Aranzadi, 2006, págs..177-178.

tratamiento debe darse a la información y datos obtenidos, y qué controles han de operar en todo el procedimiento. "Sed quis custodiet ipsos custodes?", ¿quién vigilará a los propios vigilantes?, plantea el poeta romano JUVENAL en sus famosas Sátiras.

Naturalmente no se nos escapan las implicaciones que un sistema de este tipo, usado sin un control adecuado, puede tener sobre los derechos de la ciudadanía. Nos preocupa profundamente que, como en EE.UU, el terrorismo u otras circunstancias se usen para restringir los derechos de los ciudadanos, y especialmente sin su consentimiento.

No podemos olvidar – y este es uno de nuestros hilvanes- que nos movemos en el ámbito o esfera de los derechos fundamentales de la persona; que la Administración debe ejercer sus potestades en función del interés público, cumpliendo el mandato del 103 CE, de servir con objetividad los intereses generales, y actuar con sometimiento pleno a la ley y al Derecho (principio de legalidad); que, como poder público que es, está sujeta a la Constitución y al resto del Ordenamiento jurídico (art. 9.1 CE), y debe promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas (art. 9.2 CE). Todo ello en el marco fundamental del 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.

Sabemos que el Derecho Administrativo como parte del ordenamiento jurídico, que regula la Administración Pública, su organización y sus servicios, así como sus relaciones con los ciudadanos, debe encargarse de la satisfacción del interés general, esto es, del interés de la colectividad; compatibilizando interés general con interés particular, bajo garantía de los derechos individuales . Pero parece que de un tiempo a esta parte lo que se legisla muchas veces no está dirigido al bien común, produciéndose en la práctica lo que el mismo RODRÍGUEZ-ARANA denomina crisis de la generalidad de las normas, pues "la ley, como expresión de la voluntad general, es hoy un principio excepcionado por la realidad de la promulgación de no pocas normas aprobadas para resolver problemas concretos. Desafortunadamente, hoy las leyes, en términos generales, no pretenden conformar abstractamente y a largo plazo la sociedad de acuerdo con la justicia, la libertad o la igualdad."[15]

El Derecho Administrativo, sus fundamentos y principios, encuentran su verdadero sentido y significado a la luz de la Constitución, y de ahí la atinada expresión Derecho Administrativo Constitucional del profesor MEILÁN GIL en el sentido del profundo impacto que la Constitución provoca en cada una de las instituciones, categorías y conceptos que conforman el sistema administrativo de un Estado social y democrático de Derecho, que necesariamente deberán ser analizadas desde la "iluminación constitucional".[16]

El presente trabajo intenta conceptuar, bajo ese prisma constitucional, el derecho al secreto de las comunicaciones; su interceptación legal y el procedimiento o sistema utilizado para su ejecución, y reflexionar sobre algunas cuestiones que plantea esa interceptación y el SITEL para la buena Administración.

15 RODRÍGUEZ-ARANA MUÑOZ, J., *Derecho Administrativo Españo. Introducción al Derecho Administrativo Constitucional*, A Coruña, Netbiblo, 2008, tomo I, pág. 108.

16 RODRÍGUEZ ARANA, *Derecho...*, cit., pág. 3.

II. PANORAMA NORMATIVO-JURÍDICO

La Ley Orgánica (LO) 4/1988, de 25 de mayo, al dar una nueva redacción al artículo 579 de la Ley de Enjuiciamiento Criminal (LECr) supone un antes y un después en la normativa existente sobre comunicaciones[17], regulando de forma más específica la intervención de las telefónicas que hasta entonces cubría su licitud mediante el amparo y la aplicación directa del artículo 18.3 CE, tal y como entendieron los Tribunales Constitucional (TC)[18] y Supremo (TS)[19]; frente a la opinión de la doctrina mayoritaria[20] de que tal precepto por sí solo no era suficiente para conferir al juez el poder adoptar la medida de intervención telefónica.

Igualmente el TEDH en su Sentencia de 30 de julio de 1998, caso Valenzuela Contreras, condena a España por no ofrecer garantías suficientes en el momento de los hechos (1985), señalando que del conjunto de ambos artículos, 18.3 CE y 579 LECr, no se desprenden garantías legales suficientes para dar cobertura a la intervención de la línea telefónica, existiendo violación del artículo 8 del CEDH.[21]

En el mismo sentido se expresa la STC 49/1999, de 5 de abril. "Por lo tanto, en el presente caso, al haber tenido lugar la injerencia en el secreto de las comunicaciones entre diciembre de 1986 y abril de 1987, cabe concluir, como lo hizo el Tribunal Europeo de Derechos Humanos en el Caso Valenzuela antes citado, que el ordenamiento jurídico español ni definía las categorías de personas susceptibles de ser sometidas a escucha, ni fijaba límite a la duración de la medida, ni determinaba las condiciones que hubieran de

17 Antes de la reforma el artículo 579 LECr decía: "Podrá el juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa". Esta redacción continúa ahora vigente como el párrafo 1 del mismo artículo.

18 Sentencias, entre otras, 16/1982, de 28 de abril; 81/1982, de 21 de diciembre; 7/1983, de 14 de febrero; 53/1985, de 11 de abril; 129/1985, de 17 de julio, sostienen que la Constitución no es un mero catálogo de principios vinculantes y de no inmediato cumplimiento hasta que sean objeto de desarrollo por vía legal, sino que por el contrario, constituyen la norma jurídica suprema de nuestro ordenamiento, de tal forma que los derechos y libertades reconocidos en su Capítulo segundo, Título primero son directamente alegables ante los Tribunales, los cuales, junto con el resto de los poderes públicos han de cumplirlos y observarlos.

19 La Sentencia del TS de 5 de febrero de 1988, aún cuando consideraba que era necesario que una ley regulara este tipo de intervenciones, entendió que los artículos 192 bis y 497 bis del antiguo Código Penal de 1973, ambos introducidos por la LO 7/1984, de 15 de octubre, junto a la LO 9/1984, de 26 de diciembre, relativa a bandas armadas y grupos terroristas, eran suficientes para establecer unos cauces procedimentales a los que poder atenerse el juez a la hora de decretar la intercepción de las comunicaciones de un determinada persona. En la misma línea de cobertura de legitimidad puede verse la STS de 5 de octubre de 1990.

20 RODRIGUEZ RAMOS, L. , *Comentarios a la Ley de Enjuiciamiento Criminal*, Colex, 1997, 9ª edición, págs. 403 y 404; GONZALEZ GUITIÁN, L., *Comentarios a la Legislación Penal*, Edersa, 1986, tomo VII, pág. 131; LÓPEZ-FRAGOSO ALVAREZ, T., *Las intervenciones telefónicas en el proceso penal*, Colex, Madrid, 1991, pág. 166; NARVÁEZ RODRÍGUEZ, A., "Escuchas telefónicas: alcance constitucional y procesal", *Revista del Ministerio Fiscal*, núm. 1, 1995, pág. 128.

21 El Tribunal señala en el apartado 59 de la Sentencia que algunas de las condiciones que se desprenden del Convenio, necesarias para asegurar la previsibilidad de la «ley» y garantizar en consecuencia el respeto de la vida privada y de la correspondencia, no están incluidas ni en el artículo 18.3 de la Constitución ni en las disposiciones de la Ley de Enjuiciamiento Criminal; principalmente la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial, la naturaleza de las infracciones a que puedan dar lugar, la fijación de un límite de la duración de la ejecución de la medida, las condiciones de establecimiento de los atestados que consignen las conversaciones interceptadas, y, la utilización y el borrado de las grabaciones realizadas.

reunir las transcripciones de las conversaciones interceptadas, ni las relativas a la utilización de las mismas. En consecuencia, la situación del ordenamiento jurídico español, puesta de manifiesto en la concreta actuación que aquí se examina, y sufrida por los recurrentes, ha de estimarse contraria a lo dispuesto en el art. 18.3 CE". A renglón seguido evita analizar la nueva redacción del 579 LECr[22] y modula la ilegitimidad constitucional en la actuación judicial de intervención[23].

Desde 1988 el art. 579 LECr[24] contempla la intervención de las comunicaciones telefónicas del procesado; la observación de las mismas en aquellas personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirven para la realización de sus fines delictivos. Pero aún así, por la imprecisión de la norma, las marcas de inconstitucionalidad por omisión siguen presentes.

La STEDH, de 18 de febrero de 2003, asunto Prado Bugallo, en relación a unas injerencias producidas en el año 1990, de nuevo condena a España por violación del artículo 8 del CEDH. Reconoce los avances efectuados en el campo del secreto de las comunicaciones respecto al caso Valenzuela Contreras, calificando de "progreso innegable" las garantías introducidas por la Ley de 1988, pero entiende igualmente que las mismas "no responden a todas las condiciones exigidas por la jurisprudencia del Tribunal, especialmente en las sentencias Kruslin contra Francia y Huvig contra Francia, para evitar abusos.

Las SSTEDH en los casos Kruslin y Huvig, 24 de abril de 1990; Haldford, 25 de junio de 1997 y Koop, 25 de marzo de 1998, razonan que la legislación española actual carece de la "calidad" requerida por la exigencia de previsibilidad, de tal forma que la Ley debe utilizar términos lo suficientemente claros para indicar a todos en qué circunstancias y bajo qué condiciones habilita a los poderes públicos para adoptar las medidas de intervención.

En la misma línea se pronunció el TC en la sentencia 184/2003, de 23 de octubre, aunque matizando que el problema no se resuelve mediante la vía de la cuestión de inconstitucionalidad, pues una declaración en tal sentido aún provocaría un perjuicio mayor al no poder ser aplicada por los Tribunales, creando un completo vacío de legislación respecto

22 Dice la misma STC: "ha de precisarse que, obviamente, no nos corresponde ahora analizar si, en virtud de la reforma llevada a cabo por la Ley 4/1988, de 25 de mayo, en el art. 579 de la L.E.Crim. se han cumplimentado, desde la perspectiva de las exigencias de certeza dimanantes del principio de legalidad, las condiciones a que acaba de hacerse mención".

23 Fundamento jurídico 5, in fine,: "Si, pese a la inexistencia de una ley que satisficiera las genéricas exigencias constitucionales de seguridad jurídica, los órganos judiciales, a los que el art. 18.3 de la Constitución se remite, hubieran actuado en el marco de la investigación de una infracción grave, para la que de modo patente hubiera sido necesaria, adecuada y proporcionada la intervención telefónica y la hubiesen acordado respecto de personas presuntamente implicadas en el mismo, respetando, además, las exigencias constitucionales dimanantes del principio de proporcionalidad, no cabría entender que el Juez hubiese vulnerado, por la sola ausencia de dicha ley, el derecho al secreto de las comunicaciones telefónicas".

24 Art. 579.2. 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. 3.- De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.

a la intervención de las comunicaciones telefónicas hasta que el legislador procediese a regular la materia con una ley clara y precisa. En conclusión, hasta que llegue ese momento, son los tribunales los que deben unificar y consolidar su doctrina en materia de intervenciones telefónicas y suplir las insuficiencias legales precisando los requisitos que la Constitución exige para la legitimidad de las intervenciones telefónicas.

El propio TS manifiesta en su Sentencia de 7 de noviembre de 1997, que estas insuficiencias han sido paliadas en gran parte por la propia jurisprudencia del TS manifestada en Sentencia de 21 de febrero de 1991 y en el Auto, pronunciado en el llamado caso Naseiro, de 18 de junio de 1992[25], que según el fiscal RIVES SEVA "pareció poner punto final a la polémica, al hacer una completa regulación, siquiera fuese por vía jurisprudencial, de las escuchas telefónicas, con lo que a partir de ese momento se podía pensar que todo, o casi todo, estaba ya dicho"[26]

El planteamiento de creación del Derecho por parte de los tribunales lo rechazamos. Nuestra Constitución ya proclama en su Preámbulo la voluntad de consolidar un Estado de Derecho que asegure el imperio de la ley como expresión de la voluntad popular y no quiere, en boca de GARCÍA DE ENTERRÍA, "un orden jurídico gobernado por la jurisprudencia de un grupo de altos jueces, los que componen el Tribunal Supremo", de forma que "investir de potestad creadora del Derecho objetivo, vinculante para todos, a una decena de jueces, resulta más bien preocupante"[27].

La pasividad del legislador español[28] para dotar a las intervenciones telefónicas de la cobertura legal suficiente, tomando como referencias los términos y condiciones expresados por la jurisprudencia del TEDH, TC y TS, contrasta con la actividad que se produce en el seno de la Unión Europea, mediante el denominado "Grupo de TREVI"[29] que en diciembre de 1991 decide llevar a cabo un estudio sobre los nuevos sistemas de telecomunicaciones

25 Este Auto, que marca un punto de inflexión en tema de interceptación de comunicaciones, consideró que la falta de motivación efectiva, la ausencia de control y de periodicidad del control, la disociación entre autorización e investigación, la entrega de copias, la no constatación de la proporcionalidad y la indeterminación de la medida y sus límites son vulneraciones que determinan la nulidad de la prueba de intervención telefónica.

26 RIVES SEVA, A.P., *La intervención de las comunicaciones en el proceso penal*, Bosch, 2010, págs. 17 y 18.

27 GARCIA DE ENTERRÍA, E., "¿Cambio radical del sistema jurídico español?", *Diario ABC*, 6 de julio de 2002, pág. 3.

28 El Boletín Oficial de las Cortes Generales, Congreso de los Diputados, en su número 240-1, de fecha 23 de abril de 2010, publica una Proposición de Ley Orgánica de reforma de la Ley de Enjuiciamiento Criminal en materia de interceptación de las comunicaciones, presentada por el Grupo Parlamentario Popular del Congreso. El Pleno del Congreso, en su sesión de 8 de junio de 2010, debatió la toma de consideración de la citada Proposición, siendo rechazada con 179 votos, frente a 159 a favor y cuatro abstenciones.

29 El Consejo Europeo de Roma de diciembre de 1975 acordó formalizar reuniones periódicas de los Ministros de Interior (y/o de Justicia) de los Estados miembros, naciendo el llamado Grupo de TREVI (denominación que coge de la famosa Fontana). Su finalidad era intercambiar de manera informal experiencias, información y conocimientos técnicos, así como construir redes para facilitar estos intercambios entre los Estados miembros. Encargado inicialmente de la colaboración en materia de terrorismo y seguridad interior, más tarde también trata temas relativos a la inmigración ilegal o clandestina y a la delincuencia organizada. El Grupo TREVI responde, para TAMAMES, a las siglas de "Terrorismo, Revolución y Violencia" y de acuerdo con BENNEFOI, a las de "Terrorismo, Radicalismo, Extremismo y Violencia Internacional". A este respecto puede verse TAMAMES GÓMEZ, R. y LÓPEZ FERNÁNDEZ, M., *La Unión Europea*, Alianza Editorial, Madrid, 1999, pág. 173 y BENNEFOI, S.: "Europe et Securité Intérieure", *Encyclopédie Delmas pour la vie des affaires,* Paris, 1995, págs. 21 a 28.

y su interceptación[30], que cristaliza en la Resolución del Consejo de 17 de enero de 1995 sobre la interceptación legal de las comunicaciones. Esta norma, publicada casi dos años más tarde en el Diario Oficial (núm. C 329 de 4 de noviembre de 1996), expone los requisitos de las autoridades competentes para la realización de la interceptación legal de las telecomunicaciones, los cuales se entenderán sin perjuicio del derecho nacional y deberán interpretarse de acuerdo con las disposiciones nacionales aplicables.

El Parlamento Europeo, después de que su propio Comité de Derechos Humanos votara días antes a favor de su retirada, aprueba el 7 de mayo de 1999 la Resolución ENFOPOL (Enforcement Police - Policía de Refuerzo), que contiene una serie de requisitos técnicos que han de seguir las operadoras de telefonía y proveedores de acceso a internet para adecuar sus sistemas, ante eventuales demandas de "pinchazos" por parte de la policía. Teóricamente, los "pinchazos" sólo podrán hacerse bajo autorización judicial, aunque el documento aprobado no lo aclara, siendo más un texto técnico que legal.

Al mismo tiempo, dentro del marco de cooperación judicial en materia penal que establece el Tratado de la Unión Europea, para su mejora, con la finalidad esencial, según URIARTE VALIENTE, de proporcionar a los ciudadanos el mayor grado de seguridad dentro de un espacio de libertad, seguridad y justicia, y con el propósito de mejorar la cooperación judicial en materia penal entre los Estados miembros de la Unión, surgió el Convenio de Asistencia Judicial en Materia Penal entre los Estados miembros de la Unión Europea, hecho en Bruselas, el 29 de mayo de 2000 (BOE 15 octubre 2003)[31], siendo éste el primer instrumento de cooperación internacional en materia penal adoptado tras la entrada en vigor del Tratado de la Unión Europea. Se dedica el Título III, artículos 17 a 22, a regular la solicitud de ayuda mutua entre los Estados miembros para la intervención y transmisión de telecomunicaciones.

En España la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, vigente hasta el 5 de noviembre del 2003, establece en su artículo 49, Secreto de las comunicaciones, que los operadores que presten servicios de telecomunicaciones al público o exploten redes de telecomunicaciones accesibles al públicos deberán garantizar el secreto de las comunicaciones, de conformidad con los artículos 18.3 y 55.2 CE y el artículo 579 LECR[32].

Para desarrollar el citado artículo 49 y poner en práctica la interceptación legal de las comunicaciones, con la base de la Resolución del Consejo Europeo del año 1995, el entonces

30 Según una decisión de los Ministros del Grupo TREVI deberían estudiarse los efectos que la evolución jurídica, técnica y comercial tiene en el sector de las telecomunicaciones con respecto a las distintas posibilidades de interceptación, así como las medidas que deberían adoptarse para hacer frente a los problemas que surgen.

31 Para un comentario general puede verse con el mismo título que el Convenio el artículo de URIARTE VALIENTE, L.M., "El Convenio de asistencia judicial en materia penal entre los Estados Miembros de la Unión Europea, hecho en Bruselas, el 29 de mayo de 2000 (BOE 15 octubre 2003)", *Centro de Estudios Jurídicos*, Ministerio de Justicia, 2004, págs. 3199 y ss.

32 Este deber genérico se reproduce en la Orden de 22 de septiembre de 1998 (vigente hasta el 30 de abril de 2005) por la que se establece el régimen aplicable a las licencias individuales para servicios y redes de telecomunicaciones y las condiciones que deben cumplirse por sus titulares.

Ministerio de Ciencia y Tecnología en el año 2001[33] redacta un borrador de proyecto de "Real Decreto por el que se establecen los procedimientos y las medidas técnicas para la interceptación legal de las comunicaciones electrónicas, exigibles a los operadores que presten servicios o exploten redes de comunicaciones electrónicas disponibles al público"; que como tal no llegó a entrar en vigor.

La Ley 32/2003, de 3 de noviembre, también denominada General de Telecomunicaciones, sustituye a la del año 1998, y el nuevo artículo 33, Secreto de las comunicaciones, es una reproducción casi literal del derogado artículo 49.

Con 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 (BOE de 29 de abril), se incorpora a nuestro ordenamiento jurídico mediante el capítulo II, Título V, artículos 83-101, el procedimiento para las interceptaciones legales de las comunicaciones; capítulo sobre el cual se interpone, por parte de la Asociación de Internautas, con fecha 29 de junio de 2005, recurso contencioso-administrativo, que da lugar al pronunciamiento del TS en la Sentencia de 5 de febrero de 2008, con un voto particular de indudable valor jurídico.

Durante la sustanciación del recurso, la Disposición final primera de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, procede a modificar el artículo 33 de la Ley 32/2003 introduciendo una buena parte del contenido del controvertido capítulo II del RD 424/2005.

Mediante la Orden PRE/1575/2006, de 19 de mayo, se crea la Comisión Interministerial para la elaboración del informe previo a la aprobación de las órdenes ministeriales que se dicten de conformidad con lo establecido en la disposición transitoria sexta del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, en materia de interceptación legal de las comunicaciones electrónicas.

Por último el Ministerio de Industria, Turismo y Comercio con la Orden ITC/110/2009, de 28 de enero, determina los requisitos y las especificaciones técnicas que resultan necesarios para el desarrollo del capítulo II del título V del reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

En resumen. La buena política legislativa, con orden y método, brilla por su ausencia. El procedimiento establecido para la interceptación de las comunicaciones, en lo que afecta al poder judicial y a la Administración Pública, es tortuoso, poco transparente y, a veces, constituye un verdadero galimatías jurídico.

Tal y como declaró la jurisprudencia del TEDH (casos Malone y Klass), que luego recoge la STC 184/2003, de 23 de octubre, el art. 8.1 CEDH al referirse a que la injerencia "esté prevista en la Ley" está exigiendo que la medida de intervención telefónica se fundamente en el "Derecho interno", esto es, que exista una Ley en sentido formal y amplio que prevea

33 Este Ministerio forma parte del Gobierno de la VII Legislatura que, bajo la presidencia de Don José María Aznar, conformó el Partido Popular al ganar las elecciones del año 2000 con mayoría absoluta.

la posibilidad de dicha medida y que la norma que la prevea sea asequible al ciudadano para que adecue su conducta –calidad de la Ley–; en definitiva, que las normas sean precisas, claras y detalladas.

Es necesario como recuerda el propio Parlamento Europeo, en su Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELÓN)[34], que la estructuración de la protección contra la actividad de los servicios de inteligencia se haga en los propios los ordenamientos jurídicos nacionales, pues en este campo son únicamente los Parlamentos nacionales quien tienen la doble función clásica de legislar, en conformidad con el citado art. 8 del CEDH, creando mecanismos de control eficaces y adecuados sobre las competencias de las autoridades de supervisión; y de controlar al Ejecutivo (y, por consiguiente, también a los servicios de inteligencia).

III. DERECHO AL SECRETO DE LAS COMUNICACIONES E INTERVENCIÓN TELEFÓNICA

El hecho de que en la Constitución de 1978 el derecho al secreto de las comunicaciones se encuadre en su Título Primero, Capítulo II, Sección 1ª (Derechos fundamentales y libertades públicas), no puede considerarse como algo casual y exento de consecuencias jurídicas, pues con tal ubicación son de aplicación las garantías contempladas en los artículos 53, 55 y 81.1 CE. Vincula a todos los poderes públicos; se puede regular sólo por ley respetando su contenido esencial; se le concede recurso preferente sumario ante los Tribunales ordinarios con posibilidad de acudir en amparo ante el Tribunal Constitucional; y su suspensión, individual, con intervención judicial y adecuado control parlamentario, así como su desarrollo requieren Ley orgánica.

El legislador constituyente considera el derecho al secreto de las comunicaciones como una plasmación singular de la dignidad de la persona y el libre desarrollo de la personalidad, incluyéndolo en el catálogo de los derechos fundamentales que, según el art. 10.1 CE, constituyen el fundamento del orden político y la paz social, sin que pueda prevalecer una pre o extrajurídica razón de Estado, como la seguridad nacional (STS 367/2001, de 22 de marzo).

Aún cuando aparece acompañado de derechos referidos a la protección de la intimidad personal y familiar (honor, intimidad, propia imagen, inviolabilidad del domicilio) el derecho de las comunicaciones tiene, según ELVIRA PERALES, "una entidad propia que trasciende esa protección, ya que las comunicaciones deberán resultar protegidas con independencia de su contenido, esto es, ya se trate de comunicaciones de carácter íntimo o de otro género, e incluso aunque no se entre a conocer el contenido de la comunicación"[35].

34 A raíz de este Informe de 11 de julio de 2001 de la Comisión Temporal sobre el sistema de interceptación ECHELON (Ponente: Gerhard Schmid) surge la Resolución del Parlamento Europeo de 5 de septiembre de 2001 sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON).

35 ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, Iustel Portal Derecho, 2007, págs. 15 y 16.

El fundamento del carácter autónomo y separado del reconocimiento de este derecho fundamental y de su específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación (STC 123/2002, de 20 de mayo).

Frente a la "intimidad" del artículo 18.1 CE, como concepto de carácter material, la Constitución configura el concepto "secreto de las comunicaciones" bajo un prisma formal[36]. No se dispensa el secreto en virtud del contenido de la comunicación, sino que toda comunicación es secreta aunque sólo algunas, como es obvio, serán íntimas, de manera que sólo desligando la existencia del derecho de la cuestión sustantiva del contenido de lo comunicado puede evitarse el caer en la inaceptable aleatoriedad en su reconocimiento a que llevaría la confusión entre este derecho y el que protege la intimidad de las personas (JIMENEZ CAMPO)[37].

Para la STC 114/1984, de 29 de noviembre, el concepto "secreto de la comunicación" ampara el contenido de la comunicación y la identidad subjetiva de los interlocutores, no siendo posible disponer de dichos datos sin el consentimiento de su titular. El bien constitucionalmente protegido es así -a través de la imposición a todos del "secreto"- la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje -con conocimiento o no del mismo- o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo). Y comparte la Sentencia del TEDH de 2 de agosto de 1984 -caso Malone-, que reconoce expresamente la posibilidad de que el art. 8 de la CEDH pueda resultar violado por el empleo de un artificio técnico que, como el llamado *comptage*, permite registrar cuáles han sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma.

El Constitucional también pone de manifiesto que el conocimiento por terceros, de los números telefónicos marcados desde un determinado aparato, no es una cuestión intrascendente, porque afecta al derecho de la intimidad, y en concreto a la privacidad de las comunicaciones telefónicas.

La norma del 18.3 CE se dirige inequívocamente a garantizar su impenetrabilidad por terceros, públicos o privados (el derecho posee eficacia *erga omnes*), ajenos a la comunicación misma. La Administración, como poder público, vinculada a este derecho, deberá cumplir con su obligación de "no hacer", sea cual sea el contenido de la comunicación; obligación que persistirá mientras una resolución judicial no disponga lo contrario. Y el ciudadano, con su derecho público subjetivo de defensa frente a la Administración, debe tener los

36 STC 114/1984, de 29 de noviembre, fundamento jurídico séptimo :"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 el contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado". En el mismo sentido SSTC 34/1996, de 11 de marzo; 123/2002, de 20 de mayo y 56/2003, de 24 de marzo.

37 Cit., pág. 41.

cauces legales adecuados para impedir cualquier actuar público que socave su libertad real, contraviniendo el marco constitucional. Con personas libres se construyen sociedades libres. Y con sociedades libres se logra el progreso de la humanidad.

Aún cuando el constituyente optó por no recoger en la redacción del 18.3 CE el término motivación para la resolución judicial, la misma es exigible pues, como bien dice la STC 62/1982, de 15 de octubre, toda resolución que limite o restrinja el ejercicio de un derecho fundamental ha de estar motivada, de tal forma que la razón determinante de la decisión pueda ser conocida por el afectado. Hay que hacer posible su control posterior en aras del respeto del derecho defensa del sujeto pasivo de la medida, por lo que la resolución ha de exteriorizar las razones fácticas y jurídicas que apoyan la necesidad de la intervención (STC 167/2002, de 18 de septiembre).

Con todo, mal que nos pese, se admite, como hace la STC 13/1985, de 31 de enero, la posibilidad de que alguna resolución judicial base su carencia de motivación en que tuvo que adoptarse con urgencia.

Este respeto a la legalidad constitucional implica para el TS (SS de 18 de julio de 2000 y 13 de marzo de 2009) que la autorización judicial de intervención telefónica se formalice en una resolución motivada, exigida expresamente por los artículos 18.3 y 120.3 CE, de tal forma que podrá recibir esa calificación cuando no quebrante los principios que justifican el sacrificio del derecho del ciudadano: proporcionalidad (delitos de notoria gravedad); especialidad de la materia a investigar (no cabe para actividades delictivas genéricas); sospechas fundadas[38] (exclusión de la mera arbitrariedad); necesidad (que no se puedan utilizar otros medios menos gravosos) y justificación de la autorización (que el intervenido pueda comprender las razones por las que se exige el sacrificio).

El secreto de las comunicaciones telefónicas tiene también una vertiente externa que la constituyen datos tales como los destinatarios, números de los destinatarios de las llamadas o su duración, momento en que se realiza, requiriéndose autorización judicial para el acceso a los mismos, aunque su contravención la considera el propio TC en su Sentencia 123/2002, de 20 de mayo, como una injerencia en el citado derecho fundamental de menor intensidad que las escuchas telefónicas, de cara a la ponderación de su proporcionalidad.

El TC con una doctrina, ya muy consolidada, entiende que el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE protege implícitamente la libertad de comunicaciones y además de modo expreso su secreto; cualquiera que sea la técnica de transmisión utilizada en el proceso comunicativo; con independencia del contenido del mensaje transmitido o intentado transmitir (conversaciones, informaciones, datos, imágenes, votos, etc...); de si el mismo pertenece o no al ámbito de lo personal, lo íntimo o lo reservado; y frente a cualquier forma de interceptación o captación del proceso de comunicación por terceros ajenos, sean sujetos públicos o privados. (STC 281/2006, de 9 de octubre).

38 La STC 167/2002 de 18 de septiembre dice la resolución judicial también debe exteriorizar "los datos o hechos objetivos que puedan considerarse indicios de la existencia del delito y la conexión de la persona o personas investigadas en el mismo, indicios que son algo más que simples sospechas, pero también algo menos que los indicios racionales de que se exigen para el procesamiento. Esto es sospechas fundadas en alguna clase de dato objetivo".

IV. LA INTERCEPTACION LEGAL Y EL SISTEMA SITEL

La Ley 32/2003 se refiere en su artículo 33 a la interceptación de comunicaciones de forma genérica sin referirse a un sistema en concreto, aún cuando, que sepamos, el que está en funcionamiento interno en España y resulta más familiar es el denominado SITEL que veremos a continuación.

El insuficiente armazón jurídico en vigor, conformado por la citada Ley ordinaria, el RD 424/2005 y la Orden ITC/110/2009, de 28 de enero, sería o debería ser puesto en práctica y tenido muy en cuenta en la operativa de cualquier sistema o red de interceptación aplicable en España en virtud de norma o Tratado internacional, o que afectase a ciudadanos españoles, siempre contando con la previa autorización judicial. No importa que la herramienta, el sistema o la red tenga carácter o ámbito particular, como ocurre con el CARNIVORE[39], o alcance mundial como el ECHELON[40], ni tampoco que estemos ante los planes de interceptación ENFOPOL de la Unión Europea o elaborando proyectos técnicos como el OSEMINTI[41].

39 Carnivore (en español, carnívoro), rebautizado como DCS1000, es el nombre de un software usado en EE.UU por el FBI que se instala en los proveedores de acceso a Internet y rastrea todo lo que un usuario hace durante su conexión a Internet, siendo necesaria la autorización judicial, al menos antes de la Ley Patriótica (Usa Patriot Act). A través de esta herramienta se espía información de internet tal como correos electrónicos, páginas visitadas y archivos transferidos.

40 El pleno del Parlamento Europeo aprobó el 5 de septiembre de 2001 una resolución que constata, basándose en las informaciones recogidas por la comisión temporal creada al efecto, la existencia de una red de interceptación mundial de las comunicaciones, resultado de una cooperación entre los EE.UU., el Reino Unido, Canadá, Australia y Nueva Zelanda, que se utiliza para interceptar comunicaciones privadas y económicas, y no con fines militares. El Parlamento, favorable a la generalización de estas técnicas de cifrado, preconiza la elaboración, a escala comunitaria, de medidas de promoción, desarrollo y fabricación de materiales y programas informáticos de cifrado europeos. Invita también a los Estados miembros a adoptar medidas para reforzar las garantías legales relativas a la protección de la vida privada, para todos los ciudadanos europeos, en particular, por mediación de una plataforma europea competente en este ámbito. Y recomienda incluir en el Tratado CE una cláusula que prohíba el espionaje económico. Posteriormente aprueba otra resolución de 7 de noviembre de 2002 en donde lamenta que, más de un año después de que concluyera su investigación sobre el sistema mundial de interceptación "Echelon", ni el Consejo ni la Comisión hayan adoptado las medidas convenientes para aplicar sus recomendaciones. Considera que, aunque la Comisión y el Consejo han tomado iniciativas para garantizar la seguridad de las comunicaciones electrónicas, serían útiles otras medidas para proteger a los ciudadanos y a las empresas contra el uso abusivo e ilegal de la interceptación de las comunicaciones, para introducir y utilizar sistemas y técnicas que permitan proteger la vida privada y la confidencialidad de las comunicaciones, así como para luchar contra el espionaje industrial. El Parlamento pide también que se entablen negociaciones con vistas a lograr acuerdos internacionales, en particular con EE.UU, para que puedan firmarse acuerdos relativos a la protección de los ciudadanos y de las empresas europeas contra tales prácticas. Además, reitera su petición a los Estados miembros de la Unión Europea de que aumenten su cooperación en materia de intercambios de información con el objetivo de aumentar la eficacia en el ámbito de la política común de seguridad y de defensa y en la lucha contra el terrorismo y contra la delincuencia organizada.

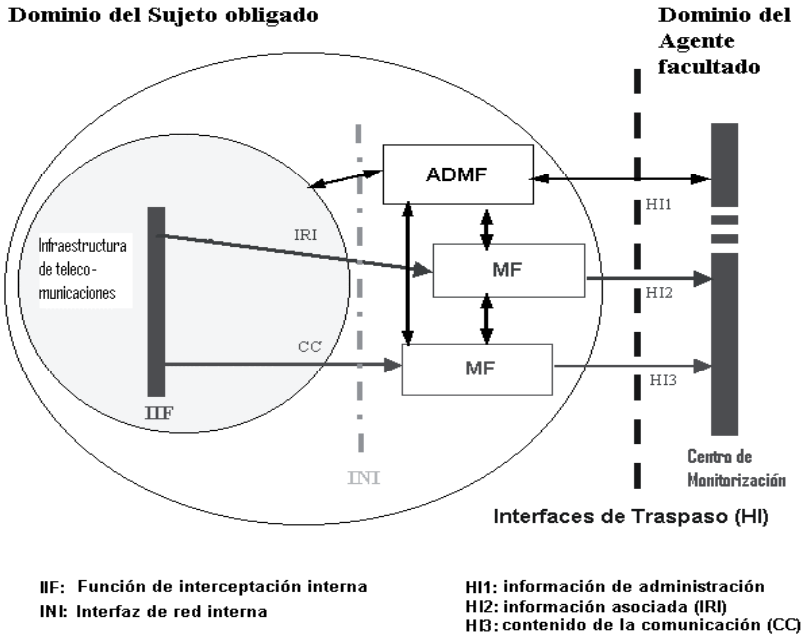
41 El Consejo de Ministros de 29 de diciembre de 2006 autorizó la suscripción del acuerdo técnico B-0034-IAP04 ERG "Infraestructura de Inteligencia Semántica Operacional (OSEMINTI)". Este proyecto, en el que participan Francia, como nación líder, Italia, y España, con una duración estimada de veinticuatro meses, permitirá a la larga diseñar sistemas de información inteligentes que posibiliten que un ordenador identifique, por ejemplo, grabaciones de audio con frases de significado concreto, como la pretensión de llevar a cabo un acto terrorista. Actualmente, sólo realizan tales identificaciones personas especializadas. Asimismo, podrán diseñarse sistemas de reconocimiento de texto que los interpreten y resalten la información que busquemos. Este proyecto permite acceder a un conocimiento tecnológico avanzado a través de una baja inversión por parte del Ministerio de Defensa, que es en este caso, aproximadamente, un 30 por ciento de su coste total. El gasto es de 928.000 euros distribuidos en tres anualidades (2007 a 2009, am-

Dejando al margen, en la medida de lo posible, la noticia periodística y las refriegas políticas interesadas, con el fin de que el lector pueda valorar nuestros comentarios y obtener sus propias conclusiones, es necesario conceptuar el marco técnico-jurídico de la interceptación legal y de su abanderado SITEL.

Además de la autoridad judicial y del sujeto interceptado existen dos figuras claves en este procedimiento: el agente facultado y los sujetos obligados.

El agente facultado es la policía judicial o personal del CNI habilitado por una autoridad judicial para materializar una interceptación legal.[42] Y los sujetos obligados son los operadores que prestan o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público o de establecer o explotar redes públicas de comunicaciones electrónicas en España.

La siguiente figura[43] muestra una configuración de referencia con una representación lógica de las entidades involucradas en la interceptación legal, en donde se pueden observar los dominios existentes y las funciones que incorpora cada uno de ellos, así como la forma de comunicación o contacto entre ambos.



IIF: Función de interceptación interna
INI: Interfaz de red interna

HI1: información de administración
HI2: información asociada (IRI)
HI3: contenido de la comunicación (CC)

bos inclusive). Estos datos han sido obtenidos en la URL: http://www.lamoncloa.gob.es/consejodeministros/referencias/_2006/refc20061229.htm

42 Este significado de agente facultado es la que recoge el RD 424/2005 en su artículo 8, destinado en su totalidad a definiciones, en el apartado e) y no se encuentra incorporado al artículo 33 de la Ley 32/2003. El que corresponde a sujeto obligado, además de contenerse en el artículo 85.1 del citado RD, es fácilmente deducible a partir del artículo 33, párrafos 1 y 2.

43 Vid. Anexo I de la citada Orden ITC/110/2009, de 28 de enero.

El binomio Sujeto obligado - Agente facultado da lugar a dos dominios independientes, pero con una superficie de contacto, una conexión o frontera común, denomina interfaces de traspaso (HI).

Los conceptos básicos[44] a barajar en el dominio del Sujeto obligado son:

IIF (Internal Interceptión Function): Punto de la red o de un elemento de red donde se obtienen el contenido de la comunicación (CC) y/o la información relativa a la interceptación (IRI).

ADMF (Administration Function): Función que controla el sistema de interceptación legal del sujeto obligado, en donde se recibe la órden de interceptación legal y genera las instrucciones para que el sistema la ejecute. Esta función impide el control del sistema de interceptación legal del sujeto obligado por los agentes facultados.

MF (Mediation Function): Mecanismo que transforma la información que se obtiene en la función IIF y la transfiere hasta la interfaz de traspaso (HI). O sea, que el contenido de la comunicación (CC) y de la información relativa a la interceptación (IRI) pasan de su formato en la interfaz de la red interna (INI) al formato normalizado de la interfaz de traspaso (HI).

La comunicación del dominio del Sujeto obligado con el dominio del Agente facultado se produce a través de tres interfaces de traspaso:

Interfaz de traspaso 1 (HI1): Interfaz bidireccional para el intercambio de información de administración, que incluye desde las órdenes de interceptación hasta la resolución de incidencias técnicas.

Interfaz de traspaso 2 (HI2): Para la entrega de la información asociada con la interceptación (IRI) al centro de recepción de las interceptaciones.

Interfaz de traspaso 3 (HI3): Para la entrega del contenido de la comunicación (CC) al centro de recepción de las interceptaciones

En el dominio del Agente facultado está el centro de monitorización. Aquí tiene su campo de juego el SITEL.

Bajo el acrónimo SITEL el Ministerio de Interior se refiere al sistema informático integrado de interceptación legal de telecomunicaciones de ámbito nacional y utilización conjunta por las Direcciones Generales de Policía y Guardia Civil, con dos centros de monitorización y sus redes asociadas y terminales remotos.[45]

No se incluye, por tanto, dentro del SITEL aquellas interceptaciones que realice el Centro Nacional de Inteligencia (CNI)[46], dentro del marco de sus funciones, con el fin de

44 En la misma Orden ITC/110/2009 existe un apéndice dedicado a definiciones.

45 Información obtenida de la nota de prensa del Ministerio de Interior en relación a sus presupuestos del año 2002, publicada en la página oficial del Ministerio en la red, cuyo enlace es: http://www.mir.es/DGRIS/Notas_Prensa/Ministerio_Interior/2001/np101101.htm

46 En la Ley 11/2002, de 6 de mayo, reguladora del CNI, éste, que sustituye al antiguo Centro Superior de Información de la Defensa (CESID), se configura, a diferencia de la anterior regulación en la que el Servicio de Inteligencia era un simple órgano, en una Dirección General dentro de la estructura general del Ministerio de Defensa, como un organismo público con autonomía funcional y personalidad jurídica propia y plena capacidad de obrar. Sus funciones, pese a adscribirse orgánicamente al Ministerio de Defensa, transcienden las necesidades o intereses estrictos de la Defensa Nacional y de las Fuerzas Armadas, lo que explica que se prevea en la Ley la eventual modificación de la adscripción orgánica a dicho Ministerio, autorizándose a tal efecto al Presidente de Gobierno.

obtener información y realizar los correspondientes análisis para el Presidente del Gobierno y los Ministros; que necesitan, si afectan a los derechos recogidos en los artículos 18.2 y 3 CE. de la autorización previa judicial[47].

SITEL se decide adquirir en el año 2001 por parte del Ministerio de Interior[48] y se adjudica a la empresa danesa ETI A/S, estableciéndose como momento final para la ejecución o cumplimiento del contrato el 30 de noviembre de 2003, tras la concesión de dos prórrogas[49] sobre el plazo inicial que expiraba el 31 de marzo del mismo año. Su puesta en funcionamiento se produce en el año 2004, aún cuando sobre esta fecha existe diversa controversia política, debido a la impopularidad de que goza SITEL.

El TS, a través de su Sentencia de 13 de marzo de 2009, que luego recoge la de 5 de noviembre de 2009, explica los grandes rasgos de SITEL. Es una implementación cuya titularidad ostenta el Ministerio del Interior. Su desarrollo responde a la necesidad de articular un mecanismo moderno, automatizado, simplificador y garantista para la figura o concepto jurídico de la intervención de las comunicaciones. El sistema se articula en tres principios de actuación:

1. Centralización: El servidor y administrador del sistema se encuentra en la sede central de la Dirección General de la Guardia Civil, distribuyendo la información aportada por las operadoras de comunicaciones a los distintos usuarios implicados.
2. Seguridad: El sistema establece numerosos filtros de seguridad y responsabilidad, apoyados en el principio anterior. Existen 2 ámbitos de seguridad:

   2.1 Nivel central: Existe un ordenador central del sistema para cada sede reseñada, dotado del máximo nivel de seguridad, con unos operarios de mantenimiento específicos, donde se dirige la información a los puntos de acceso periféricos de forma estanca. La misión de este ámbito central es almacenar la información y distribuir la información.

   2.2 Nivel periférico: El sistema cuenta con ordenadores únicos para este empleo en los grupos periféricos de enlace en las Unidades encargadas de la investigación y responsables de la intervención de la comunicación, dotados de sistema de conexión con sede central propio y seguro. Se establece codificación de acceso por usuario autorizado y clave personal, garantizando la conexión al contenido de información autorizado para ese usuario, siendo necesario que

47 Así el artículo 12 de la Ley reguladora del CNI y el artículo único de su complementaria Ley Orgánica 2/2002, también de 6 de mayo, reguladora del Control Judicial Previo del CNI señalan que el Secretario de Estado Director del CNI deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro.

48 Siendo su titular Don Mariano Rajoy Brey y subsecretaria Doña María Dolores de Cospedal; y por un importe de adjudicación de 9.825.975 euros.

49 Muy importante es que en la solicitud de aplazamiento se afirma que "la participación de los operadores de telecomunicaciones en el Proyecto SITEL, concretamente los operadores de telefonía móvil TME, Amena y Vodafone y el operador de telefonía fija Telefónica España, es indispensable para la ejecución del proyecto".

sea componente de la Unidad de investigación encargada y responsable de la intervención.

3. Automatización: El sistema responde a la necesidad de modernizar el funcionamiento de las intervenciones de las comunicaciones, dotándole de mayor nivel de garantía y seguridad, reduciendo costes y espacio de almacenamiento, así como adaptarse al uso de nuevos dispositivos de almacenamiento.

El sistema, en la actualidad, aporta la siguiente información relativa a la intervención telefónica:

1. Fecha, hora y duración de las llamadas.
2. identificador de IMEI y nº de móvil afectado por la intervención.
3. Distribución de llamadas por día.
4. Tipo de información contenida (SMS, carpeta audio, etc.)

En referencia al contenido de la intervención de la comunicación, y ámbito de información aportada por el sistema, se verifica los siguientes puntos:

1. Repetidor activado y mapa de situación del mismo.
2. Número de teléfono que efectúa y emite la llamada o contenido de la información.
3. Contenido de las carpetas de audio (llamadas) y de los mensajes de texto (SMS).

El sistema de trabajo que se lleva a cabo con SITEL también lo describen las citadas SSTS. Solicitada la intervención de la comunicación y autorizada esta por la Autoridad Judicial el empleo del Programa SITEL, la operadora afectada inicia el envío de información al Servidor Central donde se almacena a disposición de la Unidad encargada y solicitante de la investigación de los hechos, responsable de la intervención de la comunicación. El acceso por parte del personal de esta Unidad se realiza mediante código identificador de usuario y clave personal. Realizada la supervisión del contenido, se actúa igual que en el modo tradicional, confeccionando las diligencias de informe correspondientes para la Autoridad Judicial. La evidencia legal del contenido de la intervención es aportada por el Servidor Central, responsable del volcado de todos los datos a formato DVD para entrega a la Autoridad Judicial pertinente, constituyéndose como la única versión original. De este modo el espacio de almacenamiento se reduce considerablemente, facilitando su entrega por la Unidad de investigación a la Autoridad Judicial competente, verificándose que en sede central no queda vestigio de la información.

V. ALGUNAS CUESTIONES QUE PLANTEA LA INTERCEPTACIÓN Y EL SITEL PARA LA BUENA ADMINISTRACION

Algún procesalista como DE LA OLIVA[50] mantiene, a propósito de la STS de 5 de noviembre de 2009, que lo cuestionable de SITEL es su posible manejo ordinario o cotidiano sin autorización judicial, así como el almacenamiento y uso de la información que sea obtenida

50 http://andresdelaoliva.blogspot.com/search/label/SITEL

en esas condiciones; la peligrosidad general de un sistema que, como tal, es manejado por el Ejecutivo.

La tecnología no puede calificarse como buena, mala, mejor o peor, desde una perspectiva moral. Son los actos humanos los que son evaluables moralmente y la cuestión que nos hemos de plantear con los sofisticados sistemas de interceptación de las comunicaciones telefónicas, como el SITEL, fes qué se puede hacer con ellos, cómo se hace y para qué se hace.

Primera cuestión. ¿Tiene la policía judicial como agente facultado integrado en la Administración Pública, a su vez poder ejecutivo del Estado, margen de maniobra suficiente y discrecional para llevar a cabo "escuchas telefónicas" al margen de la autorización judicial? La respuesta es casi negativa. Y decimos casi porque necesitaría de la colaboración del sujeto obligado, en el sentido de que éste pusiera en marcha el sistema de interceptación sin haber recibido la orden judicial, con autoviolación de la función ADMF, que es la que impide el control del sistema de interceptación legal del sujeto obligado por parte de los agentes facultados. El SITEL por si mismo no intercepta sino que requiere de la decisión del sujeto obligado en su sistema. Por decirlo gráficamente, quien baja el interruptor para poder escuchar es la operadora, no la policía judicial ni el Juez autorizante.

El verdadero problema que plantea SITEL es jurídico, no técnico: se trata de que la normativa reguladora concentre sus esfuerzos de control en las entidades involucradas; primero, en el dominio del sujeto obligado con el fin de asegurar que sólo se interceptan las conversaciones de aquellos teléfonos que el juez ha autorizado; y segundo, en el dominio del agente facultado, comprobando que SITEL recibe únicamente información asociada con interceptación (IRI) y contenido de comunicación (CC), conforme a resolución judicial.

Para ello es necesario que cualquier intervención en un punto de red o en un elemento de la red genere un mensaje informativo a la unidad judicial de control de las comunicaciones creada al efecto, quedando al mismo tiempo rastro informático suficiente, indeleble y evidente para el auditor del sistema o infraestructura de telecomunicaciones del sujeto obligado. Técnicamente no resulta complejo cruzar los mensajes informativos de números interceptados con autorizaciones judiciales, ver que la coincidencia es plena, sin excepción alguna.

Toda la información (IRI) y contenido (CC) entregado al centro de recepción de las interceptaciones de SITEL a través de los interfaces de traspaso HI1, HI2 y HI3 se efectuaría, como envío simultáneo, a la unidad judicial de control de las comunicaciones.

Segunda cuestión. Las informaciones, la de administración y la asociada con la interceptación, y el propio contenido de la comunicación se van enviando desde el dominio del sujeto obligado al SITEL, o sea, al centro de monitorización, que la distribuye con su red asociada y terminales remotos. Las SSTS de 13 de marzo y 5 de noviembre de 2009 son categóricas al expresar que entregada la información por parte de la Unidad de investigación a la Autoridad Judicial competente, se verifica que en sede central no queda vestigio de la información.

La realidad no es tan simple como la plantea el TS. Primero, que la información no está sólo en el centro de monitorización, sino también en el terminal en donde el miembro de la policía judicial o unidad de investigación ha realizado las audiciones personales e individualizadas para confeccionar las diligencias de su informe. Y segundo ¿quién verifica que no queda vestigio de la información? ¿La propia Administración a través del responsable de la Unidad de investigación? ¿El Juez, el Secretario judicial, un funcionario de la Administración de Justicia? ¿Algún otro órgano de la Administración ajena a la investigación? Todas estos interrogantes no están previstos en la Ley y si bien es cierto que existe, en general, un alto grado de confianza en la forma de proceder de las Fuerzas y Cuerpos de Seguridad[51]; una convicción interna de que los archivos de información en cada interceptación son borrados una vez se efectúa la entrega a la Autoridad Judicial; no lo es menos que un Estado de Derecho como garante de derechos fundamentales como la libertad (artículo 1 CE) tiene que apoyarse y moverse, no por hipotéticas convicciones de sus ciudadanos, sino por procedimientos reglados en normas jurídicas. La confianza (aspecto subjetivo) no excluye el control (jurídico).

Diremos, utilizando la argumentación del voto particular formulado en la STS de 30 de diciembre de 2009[52], que no se trata de buscar respuestas que consistan en actos de fe, ni de hacer un juicio sobre la credibilidad que nos inspira la labor de las Fuerzas y Cuerpos de Seguridad del Estado sino enfocar el problema bajo un prisma genuinamente jurídico.

Al poder judicial le interesa la integridad de las conversaciones o datos que se aportan a un proceso. Es a la Administración Pública, al servicio de los intereses generales, y al Poder Legislativo, representante del pueblo y garante de ese servicio, a quien le tiene que preocupar y mucho el determinar el sistema a seguir para conservar (o no conservar) y controlar las conversaciones telefónicas legalmente intervenidas y grabadas, decidir qué hacer (el fondo) y cómo hacer (la forma) con ese archivo de escuchas integrado en el SITEL.

Tercera cuestión. Respecto a la autorización judicial hay un aspecto que conviene apuntar. En ocasiones los datos o referencias que contiene la autorización informan únicamente del número de teléfono a intervenir y la compañía a la que pertenece, pero en otras ocasiones constan, además de los datos personales, referencias concretas al presunto delito que se está investigando (muchas veces bajo secreto de sumario) o bien acerca de los hechos sobre los que hay indicios de responsabilidad criminal y que necesitan de la máxima discreción. De tal forma que el Departamento de Seguridad del sujeto obligado a practicar la intervención acaba teniendo una información en su poder innecesaria y ajena al fin que se pretende, que utilizará o no de la forma debida.

El sujeto obligado se mueve por fines muy divergentes a los del agente autorizado. Los operadores que prestan servicios de comunicaciones electrónicas son entidades mercantiles multinacionales, que están organizadas, configuradas y estructuradas para la obtención del máximo lucro posible. Y para la consecución de una cuenta de resultados jugosa existen

51 El artículo 104 CE establece que las Fuerzas y Cuerpos de seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.

52 Este voto lo formula el Magistrado Don Manuel Marchena Gómez y se adhiere Don José Manuel Maza Martín.

presiones internas y externas, a veces sofocantes, así como intereses desmedidos de sus cuerpos directivos, motivados mediante sistemas salariales basados en el objetivo puramente matemático de cumplir u obtener una o varias cifras. Las recientes noticias sobre los procedimientos y métodos de trabajo en alguna empresa del sector, y los irreparables daños que los mismos han ocasionado nos producen cuando menos inquietud al trasladarnos al campo del secreto de las comunicaciones. A ello se une lo comentado de la posibilidad de intervenir en un punto de la red y obtener información asociada y contenido de una comunicación.

No podemos olvidar las certeras palabras de GONZALEZ PÉREZ, cuando nos enseña que en la Administración, que está para servir a los intereses generales, quizás, "tengan más importancia que las medidas adoptadas en orden a las conductas de los que acceden a la función pública durante el ejercicio de la actividad, las que se prevén en orden a las conductas posteriores. En otras razones, porque el acceso a cargos bien remunerados en las grandes empresas suele ser la recompensa de los servicios prestados durante el desempeño del cargo o función pública".[53]

Cuarta cuestión. El software y el hardware existente en los dominios del sujeto obligado y del agente facultado, que posibilitan la interceptación, requieren en buena lógica de un servicio de mantenimiento que Administración y operadores de telefonía suelen externalizar en compañías especializadas. Es necesario regular un procedimiento de tal forma que las inevitables incidencias técnicas se solucionen con total respeto al secreto de las comunicaciones interceptadas, ya finalizadas o en tramitación, con plena garantía de que el tercero externo, que acude a mantener o corregir, no tenga acceso a las mismas ni a copiar los datos acumulados.

Los archivos relativos al contenido de la comunicación intervenida se almacenan, al menos temporalmente, con lo que existe un problema de seguridad ante robos o fugas de información, que puede agravarse cuando la función de mantenimiento ha sido adjudicada a una empresa externa[54].

No se puede separar el problema de las escuchas del de los bancos de datos, puesto que las escuchas tienen como consecuencia el registro y archivo de las informaciones obtenidas (Opinión concordante del Juez Señor Pettiti en STEDH de 2 de agosto de 1984, caso Malone).

En agosto de 2007 Gran Bretaña lanzó una alerta máxima de seguridad tras el robo de una base de datos que contenía escuchas telefónicas de la policía por casos de terrorismo

53 GONZÁLEZ PÉREZ, J., *La ética en la Administración pública*, Civitas, 2000, segunda edición, pág. 100.

54 Un campo que las operadoras telefónicas, sobre todo de móviles, suelen externalizar es el relativo a las reclamaciones sobre facturas, de tal forma que, como apunta la Fiscalía en su Consulta 1/1999, de 22 de enero, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones, "por razones de facturación el usuario de servicios de telecomunicación autoriza contractualmente al operador a registrar y conservar aquellos datos –número de llamadas efectuadas en cada período de facturación, número de los abonados con los que se ha puesto en conexión, duración de la llamada, fecha y hora y otros- que resultan indispensables para determinar el precio justo del servicio prestado y para fundar una reclamación en caso de discrepancia o abuso y cuyo registro deviene necesario en el desenvolvimiento de la relación negocial en los términos del art. 1258 del Código Civil".

y crimen organizado. El robo se había producido en la sede de la firma informática Forensic Telecommunication Services Ltd (FTS) en Sevenoaks, condado de Kent. Ello generó una polémica acerca de si un Gobierno debe contratar este tipo de servicios de investigación y custodia de datos, a empresas privadas.

El debate no alcanzó a España. El Boletín Oficial del Estado de 25 de octubre de 2007 publica una Resolución de la División de Coordinación Económica y Técnica de la Dirección General de la Policía y de la Guardia Civil, que adjudica a la empresa Fujitsu España Services S.A[55] un contrato para la ejecución del servicio de mantenimiento y soporte plurianual, preventivo y correctivo, del sistema de entorno de alta disponibilidad y plataforma de almacenamiento/archivado/back up del Sistema de Interceptación Legal de las Telecomunicaciones (SITEL), del Cuerpo Nacional de Policía, ubicado en el Complejo Policial de Canillas.

Este tipo de servicios de out-tasking o de outsourcing deben ser proscritos por la normativa sobre interceptación de telecomunicaciones, siendo necesario configurar un sistema que haga recaer en un órgano - podría ser el Centro Criptológico Nacional (CCN)[56] o similar- la seguridad de los sistemas de interceptación e información, tanto de los que se encuentran a disposición del agente autorizado, como es el SITEL, como los que utilizan los sujetos obligados (operadoras) para realizar las interceptaciones autorizadas. Se trata de garantizar la confidencialidad, la disponibilidad y la integridad de la información que manejan y de los propios sistemas, pues resulta fundamental en éstos, particularmente en los dedicados a la administración electrónica, conocer la autenticidad del usuario y la trazabilidad del uso del servicio y del acceso a los datos. Sólo conociendo quién accede a los datos y cuándo, se puede prestar correctamente el servicio y perseguir los fallos que puedan producirse (accidentales o deliberados).[57]

El CCN[58], previa variación de su dirección y adscripción orgánica, u organismo al estilo, llevaría a cabo la evaluación y certificación de la seguridad de las tecnologías y sistemas de

55 Aún cuando en la resolución se dice que esta empresa tiene nacionalidad española, lo que formalmente es cierto, de sobra es conocido que pertenece a Fujitsu Limited, la multinacional japonesa con sede en Tokio, de gran importancia en el sector de las tecnologías de la información y como proveedor global de servicios de tecnología, que cuenta con casi 175.000 empleados y clientes en 70 países del mundo.

56 El Real Decreto 421/2004, de 12 de marzo, regula el CCN, organismo adscrito al CNI que tiene como ámbito de actuación la seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que según la normativa requieren protección, y que incluyen medios de cifra.

57 En este sentido Exposición de Motivos del citado RD 421/2004.

58 EL CCN es el responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, debiendo garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. Entre sus funciones están, entre otras, las siguientes: -Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración; -Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones; -Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura; -Constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de Información, de aplicación a productos y sistemas en su ámbito; - Elaborar el Catálogo de Productos con Cer-

información que se utilizan en el campo de las telecomunicaciones para garantizar que el secreto de las comunicaciones es un derecho constitucional que se cumple a rajatabla y que únicamente sufre excepción bajo autorización judicial. Sería el encargado de realizar las citadas inspecciones y auditorías de seguridad de los dominios del sujeto obligado y del agente facultado a interceptar, certificando que la línea recta de la comunicación únicamente se rompe y deviene en quebrada por mandato judicial.

Quinta cuestión. El concepto de agente facultado, pieza fundamental en la interceptación, no se incorpora al art. 33 de la Ley 32/2003, sino que permanece en el art. 84. del RD 424/2005, de tal forma que el Gobierno, sin control parlamentario, puede modificar su definición como y cuando considere oportuno y consecuentemente ampliar o restringir el ámbito de aplicación de la Ley. No resulta de recibo que la interpretación y definición de una buena parte de ese art. 33. Secreto de las comunicaciones, quede a expensas de un reglamento. Por poner un ejemplo, ¿Qué ocurriría si el Ejecutivo decide mañana modificar la norma reglamentaria y ampliar el concepto de agente facultado a determinado personal cualificado de empresas externas dedicadas al campo de la seguridad e investigación? ¿Podrían cumplimentar las órdenes judiciales de interceptación?

En el primer borrador de proyecto del RD, el personal del CNI no era calificado de "agente facultado" y por tanto no podía ser habilitado por la autoridad judicial para materializar una interceptación legal. La simple variación de una definición, en este caso la de "agente facultado", incide de forma indirecta en la regulación de la interceptación legal de las comunicaciones, operando una modificación sustancial de la misma. Con la nueva delimitación reglamentaria basta con formar parte del cuadro de personal del CNI (información clasificada con el grado de secreto o mayor nivel) para poder ser agente facultado y recibir la información relativa a la interceptación legal y todo un conjunto de datos y características de la comunicación, algunos de ellos al margen de la orden judicial.

Sexta cuestión. Es necesario encorsetar legalmente, con un contenido concreto, el concepto de "policía judicial", por cuanto el texto constitucional no establece un modelo de policía judicial sino que tan sólo señala dos únicas exigencias al legislador: una, la necesidad de crear y regular la policía judicial y, dos, que la misma tenga una dependencia funcional de Jueces, Tribunales y Ministerio Fiscal. La Constitución enuncia la tarea que incumbe a la policía judicial, pero no atribuye la función a ningún órgano, ni efectúa la distribución material y geográfica de la competencia. En rigor, tampoco predetermina si ha de constituirse como cuerpo específico o como mera función ejercitable por los Cuerpos de Seguridad, ni si su régimen de dependencia de Jueces y Fiscales debe ser orgánico o funcional, por lo que deja en manos del legislador un extenso margen de libre configuración.

Razones imperiosas de seguridad jurídica obligan a definir con claridad a qué modelo de policía judicial, genérica o específica, se refiere el artículo 84 del RD 424/2005, aún cuando para muchos de nosotros resulte obvio que el concepto de policía judicial moderno, basado

tificación Criptológica que incluye los productos capaces de proteger la información clasificada Nacional cuando es transmitida expresando, para cada equipo, el nivel de protección alcanzable.

en los principios de unidad de dirección, permanencia, estabilidad y especialización, con dependencia funcional de los Jueces, Tribunales y del Ministerio Fiscal, es el que mejor encaja con las previsiones de los artículos 18.3 y 126 de la CE.

Séptima cuestión. La Sala de lo Contencioso-Administrativo del TS en su célebre Sentencia de 5 de febrero de 2008 argumenta que la reserva de ley orgánica no tiene porque extenderse a todas y cada una de las cuestiones accesorias o instrumentales relacionadas con las interceptaciones telefónicas; que la ley ordinaria puede regular y especificar los aspectos propiamente técnicos, operativos o instrumentales de la intercepción siempre que al hacerlo no invada el ámbito del derecho fundamental protegido por la reserva de ley orgánica

Esta Sentencia entiende que las leyes orgánicas han de regular cuándo y bajo qué condiciones son legítimas las interceptaciones de las comunicaciones, y que así ya lo hacen la Ley orgánica 2/2002 sobre control judicial previo al CNI y el 579 de la LECr con las garantías necesarias para legitimar la injerencia, y siendo consciente de las insuficiencias jurídicas que conlleva el 579 a la luz de la jurisprudencia del TEDH, expresa citando la del caso Prado Bugallo de que dichas "insuficiencias han sido paliadas en gran parte por la jurisprudencia, principalmente la del Tribunal Supremo"

Y partiendo de estas consideraciones analiza diversos preceptos del RD 424/2005, de los que buena parte se incorporan al art. 33 de la Ley 32/2003, estimando que no se invade el ámbito reservado a la ley orgánica.

En el voto particular formulado por el magistrado Don Oscar González González, se entiende que debió plantearse al Tribunal Constitucional cuestión de inconstitucionalidad de los apartados 6º y 7º del art. 33 de la Ley 32/2003, como previa al dictado de la sentencia.

El razonamiento del magistrado se basa en que la ley ordinaria no es suficiente para imponer a los operadores la obligación de facilitar al agente facultado toda una serie de información y de datos, descritos en tales apartados[59], que afectan al secreto de las comunicaciones e inciden en el derecho a la intimidad personal (art. 18.1 CE) y cuyo suministro pudiera no estar previsto o incluido en la orden judicial de interceptación, por lo que requeriría de una ley orgánica. A su entender se trata de datos muy personales, que rebasan la mera instrumentalidad; son datos que están dentro del contenido esencial del derecho proclamado por el art. 18.3 de la CE y que para su intervención exigen Ley Orgánica, según su art. 81.1.

En nuestra opinión la posición jurídica de este voto particular es perfectamente aplicable al apartado 8º del mismo art. 33 por cuanto, con carácter previo a la ejecución de

59 El contenido de los artículos 88.2 y 3 del RD 424/2005 se incorporan a los apartados 6 y 7, respectivamente, del artículo 33 de la Ley 32/2003 en su nueva redacción. La información y datos a que se refieren son: identificación de la persona física o jurídica; domicilio en el que el proveedor realiza las notificaciones; número de titular de servicio; número de identificación del terminal; número de cuenta asignada por el proveedor de servicios Internet; dirección de correo electrónico; 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; y si se trata de servicios móviles una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

la orden de interceptación legal, obliga a las operadoras de servicios de comunicaciones a facilitar al agente facultado información sobre 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, (que siempre obran[60]), los correspondientes nombres de los abonados con sus números de DNI, tarjeta de residencia o pasaporte, si son personas físicas; o la denominación y CIF si se trata de personas jurídicas. La redacción dada a este apartado 8º no obliga a que esta información y datos se contemple o incluya en la orden de intervención judicial que se va a ejecutar, por lo que también requeriría ley orgánica.

El campo de interceptación de las comunicaciones es de suma importancia y relieve en la vida de la persona, en sus derechos y libertades, y una deficiente o insegura regulación jurídica conlleva múltiples peligros para su dignidad y libre desarrollo de su personalidad. Por ello es fundamental que este tipo de materias no estén sometidas a los vaivenes políticos del Gobierno de turno ni a mayorías parlamentarias débiles o coyunturales, sino que exista un consenso sustancial y un espíritu de perdurabilidad, que únicamente se puede conseguir mediante la ley orgánica, con esa exigencia del quórum reforzado que evita maniobras unilaterales del grupo en el poder.

Octava cuestión. Es urgente regular el estatuto básico de derechos de las terceras personas ajenas de las que, sin ser sujetos pasivos de la medida de interceptación de la comunicación, se obtienen datos e información triviales para el proceso judicial o la investigación (la denominada problemática de los hallazgos casuales), con interferencia o injerencia en su libertad de comunicación e incluso en su derecho a la intimidad personal (art. 18.1 CE). El TC ha expresado en varias ocasiones[61] que el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores o de los corresponsales.

Conclusión. No basta con una resolución judicial motivada autorizando la injerencia. Es necesario que todo el procedimiento esté bajo control judicial, con el fin de que el Estado de Derecho mantenga una buena asepsia e higiene. Y se logrará, en gran medida, cuando el sistema de interceptación, llámese SITEL o como se quiera, opere bajo mando y dependencia judicial, a través de una Unidad con personal científico de los Cuerpos y Fuerzas de Seguridad (Guardia Civil-Policía Nacional), independiente de la Administración Pública (poder ejecutivo), con obligación inexcusable de que el inicio de la intervención,

60 El único espacio sin identificación era el de las tarjetas de telefonía móvil de prepago. En virtud de la Disposición Adicional Única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, las tarjetas de prepago se identificarán mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal. Respecto a las tarjetas adquiridas con anterioridad a la entrada en vigor de esta Ley, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las citadas obligaciones de inscripción.

61 SSTC 114/1984, de 29 de noviembre; 123/2002, de 20 de mayo y 56/2003, de 24 de marzo, haciéndose eco de la STEDH de 2 de agosto de 1984, caso Malone.

la entrega de la información asociada y del contenido de la comunicación y su posterior borrado, se realice por la senda sede judicial-sujeto obligado, sin intermediarios ni estaciones de trasvase. La regulación jurídica de la interceptación tiene que garantizar la línea recta de la comunicación; que la operadora no pueda, sin ser detectada, intervenir en un punto de red y obtener información asociada y contenido de una comunicación; y que en la "escucha legal" exista únicamente envío de contenido sin posibilidad de conocimiento o apropiación del mismo por terceros ajenos. Y la participación real de toda la ciudadanía en esa regulación obliga a acudir a fórmulas legislativas como la ley orgánica que, al requerir un alto grado de consenso, siembran una mayor paz social.

¿O es que acaso no es esto lo que en buena lid queremos y debemos interpretar a la luz de los artículos 9.2, 10.1 y 18.3 de nuestra Constitución bajo el flexo de la jurisprudencia del TEDH y de buena parte de las Sentencias del Constitucional?