LA SEGURIDAD NACIONAL Y EL ACCESO A LOS DATOS DE TRÁFICO DE LAS COMUNICACIONES ELECTRÓNICAS (UN ANÁLISIS A PARTIR DE LA LEY 34/2002, DE 11 DE JULIO, DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO, LA LEY 11/2002, DE 6 DE MAYO, REGULADORA DEL CENTRO NACIONAL DE INTELIGENCIA, Y LA DIRECTIVA 2002/58/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 12 DE JULIO DE 2002) (1)

Lorenzo Marroig Pol
Comandante Auditor

SUMARIO

(1) El presente trabajo fue artículo finalista en el XVII Premio LA LEY 2002, de artículos doctrinales.

I. CONSIDERACIONES PRELIMINARES

Entre las distintas cuestiones que, en la actualidad, suscitan un más vivo debate se encuentra el establecimiento de las condiciones de almacenamiento y de cesión a terceros de los denominados «datos del tráfico de las comunicaciones electrónicas», en tanto en cuanto constituyen una categoría especial de los datos personales en las conexiones entre el emisor y el receptor de una comunicación electrónica.

El problema de los datos de tráfico de las comunicaciones electrónicas es que estos datos se sitúan más allá del tiempo real en que ha tenido lugar la comunicación, en el almacenamiento en soporte permanente para una posterior utilización (acceso) legítima por parte de los operadores o de terceros. Este almacenamiento y posterior acceso son legítimos para finalidades específicas que previamente hayan sido determinadas en la norma, salvo las excepciones que legalmente pudieran establecerse (2), y siempre que no se vacíe el contenido del derecho, con aplicación de un marco de garantías (3).

El objeto del presente trabajo se centrará en el examen del acceso a los datos de tráfico de las comunicaciones electrónicas por parte del servicio de inteligencia español, el Centro Nacional de Inteligencia, conforme la Ley 11/2002, de 6 de mayo, reguladora de este Centro (4), en necesaria conexión con el «derecho fundamental a la protección de datos personales», teniendo en cuenta que, precisamente, el sector de las comunicaciones electrónicas, como ha venido destacando la doctrina científica, es uno de los ámbitos en el que la protección de datos de carácter personal «cobra

---

(2) Por ejemplo, las excepciones al principio general contenidas en el Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo del Título III de esta Ley, en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones, en línea con la Directiva 97/66/CE, lo son a efectos de facturación y pagos de las interconexiones, así como la promoción comercial de los propios servicios de telecomunicaciones, y están acompañadas de un marco de garantías, en la que se identifican las finalidades específicas a las que podrán estar destinados los tratamientos (facturación y pago de interconexiones o la promoción comercial de los servicios propios), así como el establecimiento de límites temporales y condiciones (artículos 65).

(3) En concreto, estando en vigor la Directiva 97/66/CE, de 15 de diciembre de 1997, la cuestión del almacenamiento o conservación de los datos del tráfico fue objeto de estudio en la Recomendación 3/99, sobre conservación de los datos del tráfico por los proveedores de servicio de Internet a efectos de cumplimiento de la legislación, de 7 de septiembre de 1999, del Grupo 29 de la Directiva 95/46/CE, de 24 de noviembre de 1995.

(4) B.O.E. núm. núm. 109, de 7 de mayo de 2002.

especial relieve» (5), al ser decisivo para el ejercicio de las libertades y derechos fundamentales.

Para ello, las previsiones contenidas en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, deberán ponerse en relación con las importantes novedades legislativas que han sido introducidas por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (6), en relación con la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (7), al objeto de comprobar, en este caso, si existe una excepción legal al consentimiento previo del interesado para proceder a la cesión de los datos personales, amparada en el artículo 11.2, letra a), de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (8), en el que se dispone que este consentimiento no es preciso «cuando la cesión está autorizada en una Ley».

En efecto, el desarrollo de las tecnologías de la información y las comunicaciones, basado en la convergencia de los sectores de telecomunicaciones, medios de comunicación, tecnologías de la información y del audiovisual, que, hasta hace poco, tenían infraestructura y equipos propios e integraban mercados independientes, está dando paso a un modelo social denominado «sociedad de la información» (9), y, a su vez, determinando la necesidad de establecer un nuevo marco normativo regulador

---

(5) MARTÍN-RETORTILLO BAQUER, L., «Consideraciones comunes a los artículos 49, 50 y 51 de la Ley General de Telecomunicaciones», VV.AA., Comentarios a la Ley General de Telecomunicaciones (Ley 11/1998, de 24 de abril), Editorial Civitas, S.A., Madrid, 1999, p. 428.

(6) B.O.E. núm. 166, de 12 de julio de 2002.

(7) D.O.C.E. L 201/37, de 31 de julio de 2002.

(8) B.O.E. núm. 298, de 14 de diciembre de 1999.

(9) En este sentido, como ha sido reiteradamente puesto de manifiesto, al igual que sucedió con la «revolución industrial» que caracterizó los siglos XIX y XX, la actual «revolución tecnológica digital», con la que finalizó el siglo pasado y se ha iniciado el siglo XXI, también ha generado profundos cambios y transformaciones sociales, dando lugar a un nuevo modelo social, el de la «sociedad de la información», en el que las empresas y personas establecen relaciones, producen y ofertan servicios, con el único freno que impone la velocidad de comunicación y la capacidad de integración o conexión cultural, al tiempo que se produce un almacenamiento y tratamiento de ingentes cantidades de datos transaccionales e informacionales. Por todos, vid., CORRIPIO GIL-DELGADO, M.R., Y MARROIG POL, L., El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones, Premio Agencia de Protección de Datos, V Edición, 2001, Madrid, pp. 55 y ss.

de la infraestructura de las comunicaciones electrónicas y los servicios asociados (10,11).

La convergencia tecnológica que se ha producido en el campo de las «comunicaciones electrónicas» ha hecho que las medidas que los Estados están adoptando en aras a la «Seguridad Nacional» frente al terrorismo cuestionen las garantías que, hasta ahora, se han venido tradicionalmente reconociendo al secreto de las comunicaciones y a la protección de los datos de carácter personal (12), hasta el punto que, siendo conscientes de la gravedad de un fenómeno que Europa conoce desde hace tiempo, desde el momento en que la protección de datos se está intentando presentar «como un obstáculo a la lucha eficaz contra el terrorismo», haya sido ineludible recordar, como se hace en el Dictamen 10/2001, de 14 de diciem-

---

(10) Los servicios de la sociedad de la información engloban, «además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador» (Exposición de Motivos II, Ley 34/2002, de 11 de julio).

(11) Fundamentalmente, desde la Recomendación núm. R (99) 5, del Comité de Ministros del Consejo de Europa, sobre la protección de la vida privada en Internet, adoptada el 23 de febrero de 1999 (que puede consultarse en en http://www.coe.fr/dataprotection/elignes.htm), la Unión Europea ha constatado la necesidad de proceder a la regulación de los tratamientos de datos personales en Internet, complementando otras Recomendaciones, entre las que se encuentra la Recomendación núm. (95) 4, sobre la protección de datos personales en el sector de los servicios de telecomunicaciones, referidos sobre todo a los servicios telefónicos, la evolución técnica ha originado la necesidad, bien de separar la regulación de estas nuevas tecnologías de las que se han considerado tradicionalmente «telecomunicaciones» (teléfono, telégrafo y radiocomunicaciones), bien, como se ha hecho, sin perjuicio de considerar la incorporación peculiaridades derivadas de la naturaleza de las redes y de los distintos servicios a través de las mismas se prestan, su consideración bajo un término omnicomprensivo, el de «comunicaciones electrónicas», con el que se abarca el «mercado de las telecomunicaciones», el «mercado de las comunicaciones de difusión» y el «mercado de las tecnologías de la información».

(12) CORRIPIO GIL-DELGADO, M.R., Y MARROIG POL, L., El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones, Premio Agencia de Protección de Datos, V Edición, 2001, Madrid, p. 18, sobre las consideraciones de HEREDERO HIGUERAS, M., «Informática y Libertad: la respuesta de los juristas a un problema de nuestro tiempo», Documentación Administrativa, núm. 171, Junio/Septiembre 1976, pp. 127-128, y MARTÍN RETORTILLO, L., Análisis del artículo 50 de la Ley 11/1998, de 24 de abril, Comentarios a la Ley General de Telecomunicaciones, Civitas, Madrid, 1999, p. 437, entienden que es el ámbito de las telecomunicaciones (hoy, «comunicaciones electrónicas») donde se acentúan los «tres órdenes de problemas» (tecnológicos, deontológicos y jurídicos), que aparecieron con el fenómeno informático.

bre de 2001, relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo, del Grupo 29 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de noviembre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (13), el deber de respeto de «determinados principios que constituyen el fundamento de nuestras sociedades democráticas», así como que, si bien los distintos textos comunitarios y nacionales sobre protección de datos personales tienen como «objetivo proteger derechos fundamentales del ciudadano», no es menos cierto que también «contemplan las excepciones necesarias para la lucha contra la delincuencia dentro de los límites autorizados por el Convenio Europeo sobre Derechos Humanos». En consecuencia, «las medidas contra el terrorismo no deben reducir los niveles de protección de los derechos fundamentales que caracterizan a las sociedades democráticas», desde el momento que «uno de los elementos clave de la lucha contra el terrorismo» ha de ser la preservación de «los valores fundamentales que constituyen el fundamento de nuestras sociedades democráticas» que intentan destruirse por quienes «abogan por el recurso a la violencia» (14).

Esta polémica en orden al acceso a los datos personales se ha acentuado (15) como consecuencia del artículo 15.1 de la Directiva 2002/58/CE,

---

(13) D.O.C.E. L 281, de 23 de noviembre de 1995.

(14) Dictamen 10/2001, de 14 de diciembre de 2001, relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo, del Grupo 29 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada...

(15) En efecto, el acceso a datos personales en los campos de Internet y las tecnologías de la información es una cuestión de acalorada polémica, debido a las medidas legislativas que se han ido adoptando en el llamado «territorio digital», tanto en Estados Unidos como en el seno de la Unión Europea y de los países que forman parte de ella, y en la que se enfrentan posturas diametralmente antitéticas. Protección de datos personales vs. Investigación criminal. Vid., Ciberpaís, núm. 235, El País, 5 de septiembre de 2002. Y que, incluso, ha trascendido entre los propios diputados europeos, como pone de manifiesto la intervención de Marco Cappato, del Partido Radical italiano, en la XXIII Converencia internacional de los Autoridades de Protección de Datos, celebrada en París, 24-26 de septiembre de 2001, cuya síntesis puede consultarse en, que llamada la atención respecto a que los datos de tráfico son datos «externos» de la comunicación que son a menudo tratados de la misma forma que el contenido de la comunicación misma, como, por ejemplo, en la jurisprudencia italiana, en la Corte Supremo de Casación, en 1998, que entendió que los datos de tráfico no son utilizables como pureba en un proceso sin autorización de la autoridad judicial. Señalando que la conservación de estos datos —que es una fase del tratamiento— por parte del Estado y el prestador de los servicios, ha sido asimilado a un registro del contenido de la conversación, considerándose como una interceptación de la comunicación. Una tesis similar ha venido siendo mantenida tradicionalmente por la jurisprudencia española, aunque, como veremos, se ha abierto recientemente una nueva doctrina.

del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (16), que introduce una ordenación que no aparece en la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre, que deroga (17), que refuerza las limitaciones a los derechos reconocidos en el artículo 13.1 de la Directiva general de protección de datos personales (Directiva 95/46/CE, de 24 de noviembre de 1995), permitiendo a los Estados miembros de la Unión Europa que puedan adoptar medidas legales limitativas del alcance de los derechos y obligaciones de los artículos 5 (confidencialidad), 6 (datos del tráfico), 8 (tratamiento de las líneas de origen y conectada) y 9 (datos de localización distintos de los de tráfico), siempre y «cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada de un sistema de comunicaciones electrónicas» (18,19).

---

(16) Con independencia de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, otros exponentes de la preocupación de la Unión Europea por todos los asuntos atinentes a las «comunicaciones electrónicas» son: la Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso); la Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización); la Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco); y la Directiva 2002/22/CE, del Parlamento Europeo y del Consejo, relativa al servicio universal y los derechos de usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva de servicio universal).

(17) En efecto, la Directiva 2002/58/CE deroga la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (D.O.C.E. L 24, de 30 de enero de 1998).

(18) Debemos entender, por lo tanto, que esta disposición refuerza las limitaciones de la Directiva general de protección de datos (Directiva 95/46/CE), en particular su artículo 13.1, que permiten a los Estados miembros de la Unión Europea para adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6 (principio de calidad de los datos), en el artículo 10 (deber de información de los datos recabados del propio interesado), en el apartado 1 del artículo 11 (deber de información cuando los datos no han sido recabados del propio interesado), y en los artículos 12 (derecho de acceso) y 21 (publicidad de los tratamientos) cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones

Precisamente, en nuestro ordenamiento jurídico, en correspondencia con los trabajos que se venían realizando en el seno de las instituciones de la Unión Europea, plasmados en el citado artículo 15 de la Directiva 2002/58/CE, de 12 de julio de 2002, en el artículo 12.1 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se establece la obligación para los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos, de retener por un periodo máximo de doce meses, los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio en la sociedad de la información (20), que ha de ser siempre con el fin de proteger otros derechos fundamentales, garantizar la persecución y represión de los delitos, y la defensa nacional y la seguridad pública (21). En otras palabras, el legislador español, al elabo-

---

reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas.

(19) Estas nuevas excepciones al deber de eliminación de los datos de las conexiones electrónicas en redes abiertas deberán ser incorporadas a los distintos ordenamientos de los Estados de la Unión Europea antes del 31 de octubre de 2003, conforme lo dispuesto en el artículo 17 de la Directiva 2002/58/CE.

(20) Quedan, no obstante, excluidos otros servicios de telecomunicaciones, como la telefonía y otros ajenos al referido ámbito de la Ley. Por tal motivo, la excepción contenida en el artículo 12 de la Ley 34/2002, de 11 de julio, no da cobertura ni puede aplicarse a los datos de las conexiones telefónicas ya efectuadas, existiendo únicamente la posibilidad legal de retener los datos relativos a la identificación del número de llamada en el caso de las maliciosas o molestas. Para estos supuestos, los procedimientos que pueden utilizarse vienen en el artículo 75.2 del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones, sobre protección suspensión de las garantías del secreto de las comunicaciones.

(21) En este sentido, la Ley 34/2002, de 11 de julio, ha venido alterar las previsiones contenidas en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones (B.O.E. núm. 99, de 25 de abril; corrección de erratas en B.O.E. núm. 162, de 8 de julio), y, en concreto, el Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo del Título III de esta Ley, en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones, que, en su artículo 65.1, recogía, como principio general, la obligación para los operadores de telecomunicaciones «de destruir los datos de carácter personal sobre el tráfico relacionados con los usuarios y los abonados que han sido tratados y almacenado para establecer una comunicación, en cuanto termine la misma», dando, así, cumplimiento al principio de cali-

rar la excepción, inexcusablemente debe configurarla como una limitación a un derecho fundamental, con lo que ello entraña, según el artículo 53.1 de la Constitución Española.

II. LA DIVISORIA ENTRE EL TRADICIONAL «DERECHO FUNDAMENTAL AL SECRETO DE LAS COMUNICACIONES» Y EL NUEVO «DERECHO FUNDAMENTAL A LA PROTECCIÓN DE LOS DATOS PERSONALES»

Desde este marco normativo, en que el que, con todo, se hace patente la fuerza expansiva del derecho fundamental a la intimidad, que va dotando a los diferentes apartados del artículo 18 de la Constitución Española «de una cierta autonomía respecto del derecho a la íntimo» (22), y, consiguientemente, de una cierta heterogeneidad en el estatus constitucional y en el régimen de desarrollo (23), los datos del tráfico de las comunicaciones electrónicas se han venido incluyendo tanto en el ámbito del «derecho fundamental al secreto de las comunicaciones» como en el del «derecho fundamental a la protección de los datos personales» (artículos 18.3 y 18.4 de la Constitución).

---

dad de los datos que obliga a cancelarlos una vez dejen de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados o bien hacerlos anónimos (según prevé el artículo 4.5, párrafos 1.º y 2.º, respectivamente, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).

(22) LUCAS DURÁN, M., El acceso a los datos en poder de la Administración Tributaria, Editorial Aranzadi, S.A., Pamplona, 1997, p. 137, y, en el mismo sentido, tras analizar las distintas posturas doctrinales, CORRIPIO GIL-DELGADO, M.R., Y MARROIG POL, L., El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones, Premio Agencia de Protección de Datos, V Edición, 2001, Madrid, pp. 75 y ss.

(23) Pese a la visión unitaria e integradora que ha pretendido dársele al artículo 18 de la Constitución (Vid., MARTÍN-RETORTILLO BAQUER, L., «Consideraciones comunes a los artículos 49, 50 y 51 de la Ley General de Telecomunicaciones», VV.AA., Comentarios a la Ley General de Telecomunicaciones (Ley 11/1998, de 24 de abril), Editorial Civitas, S.A., Madrid, 1999, pp. 425 y ss), el desarrollo normativo, doctrinal y jurisprudencial de los distintos apartados del artículo 18 de la Constitución, permite distinguir:

— Por un lado, están los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen del artículo 18.1 de la Constitución, que, adoptando una clásica posición defensiva frente a todo género de injerencias o intromisiones ilegítimas por parte de terceros (STC 292/2000, de 30 de noviembre, fundamentos de derecho 5.º, 6.º y 7.º), gozan de una protección civil al amparo de la Ley Orgánica 1/1982, de 5 de mayo (B.O.E. núm. 115, de 14 de mayo), sin perjuicio de la protección penal que alguno de los derechos pueda tener, como el caso del derecho al honor, en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (B.O.E. núm. 281, de 24 de noviembre de 1995).

El examen que nos hemos propuesto de la cesión de los datos de tráfico de las comunicaciones electrónicas debe partir, en nuestra opinión y como razonaremos, de la premisa de un imprescindible replanteamiento de las conexiones e interrelaciones existentes entre, por una parte, el arraigado «derecho fundamental al secreto de las comunicaciones» del artículo 18.3 de la Constitución, y, por otra parte, el «derecho fundamental a la protección de datos personales» del artículo 18.4 de la Constitución, retomando la cuestión de la frontera de uno y otro derecho fundamental, a la luz de los recientes pronunciamientos legales y jurisprudenciales, al objeto de fijar el régimen jurídico al que deben adscribirse los datos de tráfico, y, a partir de ahí, establecer cuál es el adecuado marco de garantías que hacen lícitos el acceso y utilización de los mismos.

La evolución normativa comunitaria y nacional seguida en la materia de protección de datos de carácter personal, que ha permitido su configuración como derecho fundamental, el «derecho fundamental a la protección de los datos personales», en la STC 292/2000, de 30 de noviembre, nos permite dar un alcance nuevo de lo que constituye el ámbito protegido de las comunicaciones, separando el proceso comunicativo como tal, desde su inicio hasta su fenecimiento, cualquiera que sea el sistema empleado, así como el contenido del mensaje, «en el caso de que éste se materialice en algún objeto físico» como dice la STC 114/1984, de 29 de noviembre (fundamento jurídico 7.º), amparados en el «derecho fundamental al secreto de las comunicaciones» del artículo 18.3 de la Constitución, que se declaran indemnes frente a cualquier interferencia no autorizada judicialmente», como subraya la STC 70/2002, de 3 de abril (funda-

---

— De otro lado, encontramos los derechos fundamentales a la inviolabilidad del domicilio y al secreto de las comunicaciones, contemplados, respectivamente, en el artículo 18.2 y 3 de la Constitución Española, que gozan de protección reforzada. Conforme el artículo 55.2 de la Constitución, las restricciones a estos derechos sólo podrán ser de forma individual y con la necesaria intervención judicial. En el supuesto del domicilio se exige resolución judicial para la entrada o registro, salvo consentimiento del titular o en caso de flagrante delito (artículos 545, 550 y 553 de la L.E.Crim.); y, para las comunicaciones, se establece también la necesaria resolución judicial para cualquier medida de control (artículo 579 de la L.E.Crim.) (Vid., para más detalle sobre esta cuestión, ARAGONESES MARTÍNEZ, S., Diligencias de averiguación y comprobación restrictivas de derechos fundamentales, en VV.AA., Derecho Procesal Penal, Colección Ceura, Editorial Centro de Estudios Ramón Areces, S.A., Madrid, 1996, pp. 368 y ss).

— Y, finalmente, está el «derecho fundamental a la protección de datos personales», que encuentra su fundamento en el artículo 18.4 de la Constitución y cuyo régimen jurídico se encuentra contenido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que resulta preciso deslindar del clásico «derecho fundamental a la intimidad», en cuanto desempeña el titular de los datos un papel más activo en la medida que garantiza un poder de control sobre los datos personales, sobre el uso y destino, impidiendo el tráfico ilícito y lesivo para la dignidad y derecho del afectado.

mento jurídico 9.º), de los datos de emisor y receptor de la comunicación una vez finalizada aquélla, aun reconociendo la íntima o estrecha conexión o vinculación existente con la comunicación realizada, que, toda vez que, tratándose de datos de carácter personal y en la medida que no suponen una «interferencia en un proceso de comunicación», deben recibir protección constitucional, no en el marco del tradicional «derecho fundamental al secreto de las comunicaciones», sino, por el contrario, en «las normas que tutelan la intimidad u otros derechos» (24).

Esta necesidad de proceder a una revisión del planteamiento tradicional que, hasta ahora, se ha adoptado respecto de los datos personales de emisor y el receptor de las comunicaciones en su relación con el proceso y el contenido comunicativo, se basará:

1. Por un lado, en las consideraciones del voto particular del juez L-E. Pettiti contenidas en la referida Sentencia del Tribunal Europeo de Derechos Humanos, Malone vs. Reino Unido de la Gran Bretaña e Irlanda del Norte, de 27 de octubre de 1983, que resalta la necesidad de establecer una distinción legislativa entre escuchas administrativas y escuchas permitidas por la Autoridad Judicial, estas últimas, adoptadas en el curso de un procedimiento penal (25), que, a su vez, hace posible establecer una diferencia-

---

(24) Sin perjuicio de significar, como dice la mencionada STC 70/2002, de 3 de abril (fundamento jurídico 9.º), «ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendiendo del concepto de comunicación y del objeto de protección del derecho fundamental, que extiendan la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del artículo 18.3 Constitución Española», en línea con lo que ya mantuvo la doctrina científica. En este sentido, MAZA MARTÍN, J.M., «Algunos apuntes a propósito de las autorizaciones judiciales para la intervención de comunicaciones a través de redes informáticas», Base de datos La Ley, 1996-1, señala, desde un punto de vista procesal, que, sin perjuicio de la disparidad tecnológica que pudiera existir entre los distintos medios de comunicación empleados, las previsiones legales y, sobre todo jurisprudenciales de la «intervención teléfonica», permiten, en el caso de las comunicaciones efectuadas a través de redes informática, en su proceder y garantías, «sino de manera absoluta, sí bastante aproximada», la oportuna «asimilación de esta clase de comunicaciones a cualquiera de las reguladas expresamente por la Ley (telefónica y postal), a fin de poder poner en práctica los mecanismos de la analogía oportunos para dispensarle el tratamiento más acorde con el cumplimiento de las garantías en protección del referido «derecho al secreto»», y RUIZ MIGUEL, C., La configuración constitucional del derecho a la intimidad, Editorial Tecnos, S.A., Madrid, 1995, p. 316, que se decanta por aplicar «a estas formas de comunicación las normas previstas en la LECr. En la medida en la que ello fuera posible».

(25) Vid., sobre la doctrina jurisprudencial recaída en materia de intervención de las comunicaciones, RIVES SEVA, A.P., La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo (3.ª edición), Editorial Aranzadi, S.A., Pamplona, 1999, Capítulo XIV, en concreto, pp. 330 y ss, así como en orden a la licitud de la prueba, DE URBANO CASTRILLO, E., Y TORRES MORATO, M.A., La prueba ilícita penal (Estudio jurisprudencial), Editorial Aranzadi, S.A., Pamplona, 1997, pp.201 y ss.

ción entre lo que puede constituir una injerencia en las comunicaciones de lo que es una vulneración de la protección de los datos personales.

Esta última previsión reviste una particular importancia si atendemos a cuáles son las funciones que, como posteriormente analizaremos, legalmente encomiendan al Centro Nacional de Inteligencia, en virtud de la Ley 11/2002, de 6 de mayo, Reguladora de este Centro, cuyo objeto no es, como se ha puesto de relieve por doctrina, «conseguir pruebas o detener un presunto delincuente, sino obtener información sobre grupos o personas potencialmente peligrosas para el Estado, su economía, su régimen democrático, y de prevenir ataques futuros» (26).

Con lo que se llega al nudo de la cuestión: las funciones legalmente encomendadas al Centro Nacional de Inteligencia, en ningún caso, se enmarcan en lo que pudiera constituir el ámbito de un proceso penal, que es el punto de arranque de la problemática planteada en todas las citadas Sentencias del Tribunal Europeo de Derecho Humanos y del Tribunal Constitucional español, en el que es lógica la aplicación de una teoría restrictiva para el acceso a las comunicaciones, cubriendo el secreto no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores o de los corresponsales (27).

En el caso del Centro Nacional de Inteligencia, estamos ante una actividad de carácter estrictamente administrativo, la del servicio de inteligencia, en la que los datos personales que pudieran recabarse constituirían una mera «prueba material», utilizada con la estricta finalidad de justificar «la existencia de determinados acaecimientos de la vida real», para la elaboración de inteligencia en las materias o acaecimientos que pudieran afectar a la «Seguridad Nacional», pero que, en modo alguno, pueden considerarse destinadas a la obtención de una «prueba judicial o procesal» para un Juez o Tribunal (28,29).

---

(26) SANTAOLALLA LÓPEZ, F., «Actos políticos, inteligencia nacional y Estado de Derecho», Revista Española de Derecho Constitucional, núm. 65, Mayo/Agosto 2002, Madrid, p. 122.

(27) STC 114/1984, de 29 de noviembre.

(28) BORRAJO INIESTA, I., Prueba y jurisdicción revisora (STS Gravamen de la consolidación del dominio, de 17 de septiembre de 1988), REDA, núm. 61, Enero-Marzo 1989, CE-ROM REDA núms. 1-100, haciéndose eco de la doctrina del profesor JAIME GUASP, contenida en Derecho procesal civil, IEP (1.ª edic. 1957), 344-46, con anterioridad en Juez y hechos en el proceso civil, Barcelona (1943) y La prueba en el proceso civil. Principios fundamentales, Revista de la Universidad de Oviedo, 21-82 (1945).

(29) En esta misma línea, por lo que se refiere al ámbito de las relaciones laborales, parecen situarse SEMPERE NAVARRO, A.V., Y SAN MARTÍN MAZZUCCONI, C., Nuevas tecnologías y relaciones laborales, Editorial Aranzadi, S.A., Pamplona, 2002, p. 91, con cita de GARCÍA VIÑAS, J., Relaciones laborales en Internet, RTSS CEF núm. 223, 2001, pp. 68 y 69, así como de alguna jurisprudencia, como la STSJ Murcia, de 7 de julio de 1994 (AS 1994, 3190), que, si bien rechaza la grabación de las conversaciones, admite, no obstante, la introducción de sistemas de identificación del número llamado.

Diferenciación, en todo caso, que no es novedosa, puesto que ya vino a atisbarse en nuestro ordenamiento en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en la que se establece, por un lado, la obligación que pesa sobre los operadores que presten servicios de telecomunicaciones al público o exploten redes de comunicaciones accesible al público de garantizar el secreto de las comunicaciones, concretamente, en los artículos 49 y 51, con remisión a los artículos 18.3 y 55.2 de la Constitución Española y el artículo 579 de la Ley de Enjuiciamiento Criminal, con exigencia de la correspondiente autorización judicial para la interceptación de contenidos, y, por otro lado, la obligación de garantizar la protección de los datos personales en el artículo 50 de la Ley 11/1998, de 24 de abril, en el que se hace una expresa remisión a la legislación sobre esta materia, recogida en la actualidad en la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como a las normas dictadas en su desarrollo y a las normas reglamentarias de carácter técnico, cuya aprobación venga exigida por la normativa comunitaria.

No obstante, como señaló también el referido voto particular del juez L-E. Pettiti, debemos considerar, por un lado, los peligros de una crisis producida por terrorismo (caso Klass, [Sentencia del Tribunal Europeo de Derecho Humanos, Klass y otros vs. Alemania, de 6 de septiembre de 1978]) y, por otro lado, los de la delincuencia común, y, en consecuencia, del establecimiento (en las legislaciones nacionales) dos regímenes distintos al respecto». De este modo, sólo tratándose de delitos, «en virtud del Derecho Penal común», sería «difícil encontrar un motivo para impedir la fiscalización judicial, aunque sólo sea para asegurar posteriormente el derecho a que se destruyan los resultados de una interceptación injustificada». Debiéndose añadir que, en el seno del proceso penal, la problemática deriva hacia la valoración judicial de la prueba, toda vez que, como reiteradamente ha señalado nuestra jurisprudencia, sólo cuando la intervención se acuerda y practica con plenitud de garantías constitucionales y procesales, se alcanza la plena eficacia de la prueba en el juicio oral, y de la que, por el contrario, se carece si aquella prueba se practicó con vulneración de los derechos fundamentales, conforme el artículo 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (30).

Asimismo, como ha señalado la doctrina científica, «la seguridad pública, debido a sus connotaciones de lucha contra el crimen, tiene en la jurisprudencia del Tribunal Europeo de Derechos Humanos unos perfiles

---

(30) B.O.E. núm. 157, de 2 de julio. Corrección errores B.O.E. núm. 264, de 4 de noviembre.

mucho más sustanciales que los que se perciben cuando es la seguridad nacional la que entra en causa. Al menos por lo que al artículo 8 se refiere, esta última trastoca el activismo del Tribunal Europeo de Derechos Humanos en una actitud huidiza y disponible para acoger, en línea de principio, la doctrina del margen de apreciación», como paradigmáticamente encontramos en la Sentencia Leander vs. Suecia, de 1987, en la que se «formula explícitamente la doctrina del amplio margen de apreciación del Estado a la hora de justificar en la seguridad nacional restricciones legítimas de los derechos» (31).

2. Por otro lado, ligado con lo antes expuesto, en la relevancia que ha ido adquiriendo la protección de datos personales, tanto en el ámbito del ordenamiento jurídico comunitario como en el ordenamiento nacional, desde la sin duda importante Sentencia del Tribunal Europeo de Derechos Humanos, Malone vs. Reino Unido de la Gran Bretaña e Irlanda del Norte, de 27 de octubre de 1983, que ha venido marcando la pauta interpretativa del ámbito de aplicación del «derecho fundamental al secreto de las comunicaciones» de nuestra jurisprudencia constitucional, limitada, en el momento en que estas sentencias se dictaron, al Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (32).

Sin embargo, es evidente que, en los últimos tiempos, la protección de los datos personales ha adquirido un estatus jurídico propio, tanto en el ordenamiento comunitario a resultas de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de noviembre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos, y de la reciente Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), como en el ordenamiento español, a través de la Ley Orgánica 15/1999, de 13 de

(31) REVENGA SÁNCHEZ, M., Seguridad nacional y Derechos humanos. Estudio sobre la Jurisprudencia del Tribunal de Estrasburgo, Editorial Aranzadi, S.A., Pamplona, 2002, p. 87.

(32) Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo 28 de enero de 1981. Ratificado por instrumento de 27 de enero de 1984. B.O.E. núm. 274, de 15 de noviembre de 1985.

diciembre, de Protección de Datos de Carácter Personal (33), y con el reconocimiento del denominado «derecho fundamental a la protección de datos personales» en virtud de la STC 292/2000, de 30 de noviembre (34).

1. El «derecho fundamental al secreto de las comunicaciones»: la revisión del ámbito de protección

La doctrina jurisprudencial que, hasta el momento, se ha venido manteniendo en relación a la extensión material del «derecho al secreto de las comunicaciones» cubre no sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como la identidad subjetiva de los interlocutores o de los corresponsales, con el fin de «garantizar así la «impenetrabilidad de la comunicación» por terceros con eficacia *erga omnes* tanto para los ciudadanos de a pie como para los agentes de los poderes públicos y abstracción hecha de la «dimensión material del secreto»», como expresamente señaló la STC 34/1996, de 11 de marzo, fundamento jurídico 4.º, en relación a la STC 114/1984, de 29 de noviembre.

Como ha puesto de manifiesto la reciente STC 70/2002, de 3 de abril (fundamento jurídico 9.º), «nuestra jurisprudencia al respecto —desde STC 114/1984, de 29 de noviembre, fundamento jurídico 7.º— puede resumirse en los siguientes puntos:

— Se protege la libertad de comunicaciones: «Rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último

---

(33) Que, como unánimemente se ha aceptado, constituye un desarrollo del artículo 18.4 de la Constitución.

(34) Este reconocimiento del «derecho fundamental a la protección de datos personales», como derecho de «la tercera generación», constituye una clara manifestación de que existe un «desarrollo histórico» de los derechos humanos y un dinamismo y progresiva «ampliación del catálogo de los derechos constitucionalmente garantizados», con los que se pretenden «satisfacer necesidades que las transformaciones tecnologícas de la sociedad postindustrial ponen de manifiesto», como señaló, en su momento, LUCAS MURILLO DE LA CUEVA, P., El derecho a la autodeterminación informativa, Editorial Tecnos, S.A., Madrid, 1990, citado por CORRIPIO GIL-DELGADO, M.R., y MARROIG POL, L., El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones, Premio Agencia de Protección de Datos, V Edición, 2001, Madrid, p. 77, en sintonía también con HEREDERO HIGUERAS, M., Nota preliminar. Documentación informática núm. 4, Legislación vol. Informática. Leyes de Protección de datos (III), Ministerio de Administraciones Públicas, Dirección General de Organización, Puestos de trabajo e informática, Madrid, 1988, p. 20.

sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas. 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 puede decirse también que el concepto de secreto que aparece en el artículo 18.3 no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como la identidad subjetiva de los interlocutores o de los corresponsales» (STC 114/1984, de 29 de noviembre, fundamento jurídico 7.º).

— Se garantiza la impenetrabilidad de la comunicación para terceros: «Sea cual sea el ámbito objetivo del concepto comunicación, la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia erga omnes) ajenos a la comunicación misma» (STC 114/1984, de 29 de noviembre, fundamento jurídico 7.º).

— El concepto de lo secreto tiene carácter formal: «El concepto de secreto en el artículo 18.3 tiene un carácter formal, en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado» (STC 114/1984, de 29 de noviembre, fundamento jurídico 7.º, y 35/1996, de 11 de marzo, fundamento jurídico 4.º)».

En este mismo sentido, la STC 34/1996, de 11 de marzo, en su fundamento jurídico 4.º, señala que el «derecho fundamental al secreto de las comunicaciones», y, en especial, de las postales, telegráfica y telefónicas, salvo resolución judicial, como bien dispone el artículo 18.3 de la Constitución, cuya interceptación por tanto significa «una grave injerencia» en aquél (STC 85/1984), «en su vertiente positiva pero implícita, consagra la libertad de las comunicaciones y explícitamente su reserva. El concepto jurídico de lo secreto, visto desde tal perspectiva, tiene un carácter formal, hemos dicho, y abstracto en consecuencia, ya que «se predica de lo comunicado, sea cual sea su contenido y pertenezca o no la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado». Por otra parte, cubre no sólo el mensaje sino también, en su caso, otros aspectos suyos y, entre ellos, la identidad de los interlocutores o corresponsales. En definitiva, se pretende garantizar así la «impenetrabilidad de la comunicación» por terceros con eficacia erga omnes, tanto para los ciudadanos de a pie

como para los agentes de los poderes públicos y abstracción hecha de la «dimensión material del secreto», lo que se transmite (STC 114/1984)».

Todo ello sin perjuicio de la salvaguarda de las garantías constitucionales y procesales en la práctica de las medidas de intervención, como también hace la mencionada STC 70/2002, en el fundamento jurídico 9.º, en el momento en que, expresamente, dice que «más allá, nuestra jurisprudencia se ha orientado a la definición de las garantías constitucionales que permiten la intervención de las comunicaciones, fundamentalmente telefónicas (previsión legal de la medida con suficiente precisión; autorización judicial mediante una decisión suficientemente motivada y ejecución de la medida con estricta observancia del principio de proporcionalidad; cfr., entre las más recientes, SSTC 49/1996, de 26 de marzo, fundamento jurídico 3.º; 121/1998, de 15 de junio, fundamento jurídico 5.º; 49/1999, de 5 de abril, fundamentos jurídicos 4.º, 5.º, 6.º y 7.º; 166/1999, de 27 de septiembre, fundamento jurídico 2.º; 229/2000, de 11 de diciembre, fundamento jurídico 2.º; y 14/2001, de 29 de enero, fundamento jurídico 2.º» (35).

Esta posición del Tribunal Constitucional tuvo, como era lógico, acogida en la Consulta 1/1999, de 22 de enero, de la Fiscalía General del Estado, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones (36), que en el «delicado problema interpretativo» sobre «el alcance de dos derechos fundamentales íntimamente relacionados como son la libertad e inviolabilidad de las comunicaciones —artículo 18.3 Constitución— y la libertad informática —artículo 18.4 de la Constitución—…», surgido como consecuencia de las posturas mantenidas por las compañías operadoras de telecomunicaciones a quienes el Ministerio Fiscal realizaba la petición de datos personales consecuencia de la comunicación, se decantó, tras analizar la legislación aplicable, por entender, como hacían las operadoras, que «la información solicitada» afecta el «estatuto constitucional de inviolabilidad de las comunicaciones —artículo 18.3 Constitución—…», y, en consecuencia, considerar que el

---

(35) Estos requisitos han sido objeto de nuevo análisis en la reciente STC 167/2002, de 18 de septiembre (B.O.E. núm. 242 suplemento, de 9 de octubre de 2002).

(36) Circulares, consultas e instrucciones de la Fiscalía General del Estado (1999), Boletín de Información del Ministerio de Justicia, Año LIV, Suplemento al núm. 1863, de 15 de febrero de 2000, pp. 765 y ss. Sobre la proyección del artículo 18.3 de la Constitución no sólo al contenido de la correspondencia, sino también a las circunstancias externas a la misma, encontramos el Dictamen de la Dirección General de lo Contencioso del Estado de abril de 1981 (Ponente: Manuel Goded Miranda), MARTÍN MORALES, R., El régimen constitucional del secreto de las comunicaciones, Civitas, Madrid, 1995, pie página 83, p. 59.

Ministerio Fiscal no podía inmiscuirse en datos personales incorporados al contenido sustancial del derecho fundamental de las comunicaciones salvo que mediara la oportuna resolución judicial legitimadora de la injerencia.

Se trata, en todo caso, de criterios que, por lo demás, se corresponden con los sustentados por el Tribunal Europeo de Derechos Humanos, sobre la base del artículo 8 del Convenio Europeo para la protección de los derechos humanos y de las libertades públicas, de 4 de noviembre de 1950 (37), en el que se dispone que: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás», y cuyo antecedente encontramos en el artículo 12 de la Declaración Universal de Derechos del Hombre, aprobada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948, según el cual, «nadie será objeto de intromisiones arbitrarias en su vida privada, familiar, domicilio o correspondencia, ni de atentados a su honor y reputación. Cualquier persona tiene derecho a la protección de la ley contra intromisiones o atentados» (38).

En concreto, la Sentencia del Tribunal Europeo de Derechos Humanos, Malone vs. Reino Unido de la Gran Bretaña e Irlanda del Norte, de 27 de octubre de 1983 (39), consideró, en sus fundamentos de derecho 83, 84 y 87, que el «recuento», esto es, el «empleo de un mecanismo (un contador combinado con un aparato impresor) que registra los números mar-

---

(37) En relación al artículo 8 del Convenio Europeo para la protección de los derechos humanos y las libertades públicas, REVENGA SÁNCHEZ, M., Seguridad nacional y Derechos humanos. Estudio sobre la Jurisprudencia del Tribunal de Estrasburgo, Editorial Aranzadi, S.A., Pamplona, 2002, p. 71, pone de manifiesto la «textura» quizá «acaso demasiado clásica» del precepto, que, se «estructura en dos niveles. El primer nivel recoge los derechos protegidos, y el segundo establece las condiciones bajo las cuales la eficacia de tales derechos puede ceder en aras de objetivos exigidos por la sociedad democrática».

(38) Disposiciones internacionales que revisten una indudable importancia desde el momento en formando parte de nuestro ordenamiento jurídico, la Constitución Española, en su artículo 10.2, dispone que: «Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratos y acuerdos internacionales sobre las mismas materias ratificados por España».

(39) Boletín de Jurisprudencia Constitucional, núms. 64-65, Agosto-Septiembre 1986, pp. 1081 y ss.

cados en un determinado aparato telefónico y la duración de cada llamada», dotado de un «aparato impresor» en el que se anotan «las informaciones que el Servicio de teléfonos puede, en principio, conseguir lícitamente, especialmente para asegurar la exactitud de los cargos que se exigen el abonado, examinar sus reclamaciones o descubrir posibles abusos», en cuanto destinado únicamente a utilizar «las señales que se le dirigen para asegurar el servicio de teléfono», sin vigilar ni interceptar «de ninguna otra manera las conversaciones», a diferencia de la interceptación de las comunicaciones, aunque, en principio, no afectaría en nada al derecho protegido por el artículo 8» del Convenio Europeo para la protección de los derechos humanos y de las libertades públicas, de 4 de noviembre de 1950, implicaba, sin embargo, la utilización de datos que contienen informaciones —en especial, los números marcados— que este Tribunal consideró parte de las comunicaciones telefónicas, de modo que la cesión de los mismos, «sin el consentimiento de abonado», se oponía al «derecho confirmado por el artículo 8», al no existir norma jurídica alguna de Derecho interno «sobre el alcance y las modalidades del ejercicio de la facultad discrecional» de que disfrutaban las autoridades para solicitarlos, y, en consecuencia, no estaba «prevista por la ley» a tenor del artículo 8.2 del mencionado Convenio Europeo.

Estableciendo, con ello, unas tesis que, después, como ha señalado la doctrina, en una acentuada senda garantista en materia de escuchas telefónicas, se ha seguido en los casos Kruslin vs. Francia y Huvig vs. Francia, de 24 de abril de 1990, y, más recientemente, en el caso Halford contra el Reino Unido, Kopp vs. Suiza, de 25 de marzo de 1998, y Valenzuela Contreras vs. España, de 30 de julio de 1998 (40).

No obstante, en todos estos supuestos se trata de escuchas realizadas en el contexto de investigaciones penales, en los que, para que la intervención judicial se considere legítima, se exige que el afectado esté procesado o se trate de persona sobre la que existan indicios de responsabilidad criminal, por lo que resulta posible seguir, en otros ámbitos (como puede ser en la actuación administrativa del Centro Nacional de Inteligencia), la tesis mantenida por la STC 70/2002, de 3 de abril (fundamento jurídico 9.º), que, como adelantamos, separa lo que constituye el proceso comunicativo como tal, desde su inicio hasta su fenecimiento, cualquiera que sea el sistema empleado, —que ampara en el «derecho fundamental al

(40) REVENGA SÁNCHEZ, M., Seguridad nacional y Derechos humanos. Estudio sobre la Jurisprudencia del Tribunal de Estrasburgo, Editorial Aranzadi, S.A., Pamplona, 2002, p. 83-85.

secreto de las comunicaciones» del artículo 18.3 de la Constitución Española, indemne frente a cualquier interferencia no autorizada judicialmente»—, de los datos personales del emisor y del receptor de la comunicación una vez finalizada aquélla, los cuales deben recibir la oportuna protección constitucional, no en el marco del tradicional «derecho fundamental al secreto de las comunicaciones», sino, por el contrario, en el marco de «las normas que tutelan la intimidad u otros derechos».

Con ello, la STC 70/2002, de 3 de abril sigue la solución jurisprudencial recientemente acogida en las SSTS (Sala Segunda), de 22 de marzo de 1999 y de 7 de diciembre de 2001, que ha entendido que no es posible establecer una equiparación «entre una conversación intervenida» y «el listado de las llamadas efectuadas desde un determinado número de teléfono», en cuanto se trata, «en definitiva, de datos de carácter personal» cuyo amparo se encuentra en la Ley Orgánica 15/1999, de 13 de diciembre (41).

Desde esta perspectiva, teniendo en cuenta que, según el artículo 3, letra a), de la Ley Orgánica 15/1999, de 13 de diciembre, se considera «dato de carácter personal» a «cualquier información concerniente a personas físicas identificadas o identificables», y teniendo en cuenta, tal como dice el inciso final del Considerando 15 de la reciente Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, que los datos de tráfico asociados a las comunicaciones electrónicas comprenden, «entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización

---

(41) Así, la STS de 22 de marzo de 1999 (fundamento jurídico 2.º) (RJ 1999/2947) señala que «la entrega por la Compañía Telefónica del listado de las llamadas efectuadas desde un determinado número de teléfono no afecta al contenido propio del referido derecho fundamental y que, por ello, no puede considerarse que constituya vulneración del mismo el hecho de ordenar el Juzgado —por simple providencia— que la Compañía Telefónica le remita el listado de las llamadas telefónicas efectuadas desde un determinado número de teléfono. Tal información, propia de la investigación judicial en la fase de instrucción, es similar a la relativa al movimiento de las cuentas corrientes bancarias, y no afecta en forma alguna al secreto de las comunicaciones telefónicas, que es lo que verdadera constituye el objeto de la protección constitucional». Añadiendo que «se trata, en definitiva, de datos de carácter personal, custodiados en ficheros automatizados, a que se refiere la Ley Orgánica 5/1992, de 29 de octubre, Reguladora del tratamiento automatizado de datos de carácter personal [hoy, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal]», en la que se establece que el consentimiento del afectado «no será preciso «cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales, en el ejercicio de las funciones que tiene atribuidas» [artículo 11.2.d) de la referida Ley, y, actualmente, el artículo 11.2, letra d) de la vigente], como es el caso». En idénticos términos, encontramos la STS de 7 de diciembre de 2001 (fundamento jurídico 2.º) (RJ 2002/2070), que reitera que «no hay equiparación posible entre una conversación intervenida y la mera indicación del teléfono y titular al que se efectuó la llamada».

del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión», así como también «al formato en que la red conduce la comunicación», resulta evidente que tienen que encontrar amparo en el «derecho fundamental a la protección de los datos personales» del artículo 18.4 de la Constitución.

Se ha llegado, así pues, en nuestra opinión, a un punto de inflexión con toda una tradición jurídica en lo relativo al entendimiento del ámbito material de las comunicaciones, fundamentalmente en lo que se refiere al contexto administrativo, de modo que, pese a que en la citada STC 70/2002, de 3 de abril, se afirma que nos encontramos en el espacio del «derecho a la intimidad del artículo 18.1 de la Constitución Española», se ha abierto una brecha en la consideración de que los datos de emisor y receptor de las comunicaciones como datos de carácter personal, que corresponde situar en el ámbito del «derecho fundamental a la protección de los datos personales» del artículo 18.4 de la Constitución Española, y someterse, como tales, a la específica normativa de esta materia contenida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y, en concreto, al artículo 11 de esta Ley Orgánica, en lo que ha sido uno de los preceptos más conflictivos de la ley (42), que regula la cesión de datos personales y las excepciones al consentimiento previo.

Es más, se trata de una consideración que, sin dificultad, puede trasladarse a la propia investigación penal, como resulta evidente si atendemos al artículo 11.2, letra d), de la Ley Orgánica 15/1999, de 13 de diciembre, en el que, aun dudándose de la necesidad de establecer la excepción del consentimiento del titular de los datos personales en la propia Ley Orgánica, en la medida que «las leyes de actuación» de cada una de las instituciones que en dicha letra se citan «establecen la obligación de colaborar con las mismas cuando ejercen sus competencias y les atribuyen, asimismo, competencias de investigación e inspección para el conocimiento de los hechos que fiscalizan» (43), se excepciona del consentimiento previo la comunicación de datos de carácter personal cuando tenga por destinatario al Ministerio Fiscal, en el marco del expediente de investigación que, en algún caso, se ha calificado como «procedimiento extrajudicial o ante-

(42) Sobre todo debido a la calificación de muy grave de las infracciones a la prohibición de cesión de datos, en el artículo 44 de la Ley Orgánica, como señala APARICIO SALOM, J., Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Aranzadi, S.A. Pamplona, 2000, p. 117.

(43) APARICIO SALOM, J., Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Aranzadi, S.A. Pamplona, 2000, p. 125.

judicial» de las diligencias previas de investigación (44), realizadas al amparo del artículo 5 de la Ley 50/1981, de 30 de diciembre, del Estatuto Orgánico del Ministerio Fiscal, y del artículo 785 bis de la L.E.Crim, en su redacción dada por la Ley Orgánica 7/1988, de 28 de diciembre.

Siendo esta, por otra parte, la orientación seguida por la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico, por lo que se refiere al acceso a los datos de tráfico relativos a las comunicaciones electrónicas, que, en su artículo 12, apartados 1 y 3, dispone, respectivamente, el deber de los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos de «retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo», en orden a la conservación de los mismos «para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así lo requieran» y comunicación «a las Fuerzas y Cuerpos de Seguridad» con «sujeción a lo dispuesto en la normativa sobre protección de datos personales».

2. El «derecho fundamental a la protección de los datos de carácter personal» del artículo 18.4 de la Constitución: naturaleza y estatuto jurídico

El «derecho fundamental a la protección de datos personales» aparece configurado en la STC 292/2000, de 30 de noviembre, tras una larga evolución de la doctrina del Tribunal Constitucional español (45), como un

(44) Memoria elevada al Gobierno al inicio del año judicial por el Fiscal General del Estado, 1997, p. 506. Diligencias de investigación que tienen una particular relevancia en el desarrollo de la investigación de los casos de delitos contra la Hacienda Pública, en los que resulta, como se dice, «clara la facultad conferida al Ministerio Fiscal para dirigirse a órganos oficiales y particulares a fin de que remitan documentos relativos a asuntos relacionados con diligencias de investigación abiertas», p. 514.

(45) Un estudio de la evolución de la jurisprudencia del Tribunal Constitucional en la configuración de lo que ha sido el «derecho fundamental a la protección de datos personales» del artículo 18.4 de la Constitución puede encontrarse en CORRIPIO GIL-DELGADO, M.R., y MARROIG POL, L., El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones, Premio Agencia de Protección de Datos, V Edición, 2001, Madrid, pp. 75 y ss.

«poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso» (fundamento jurídico 7.º de la mencionada STC 292/2000), pero, en modo alguno, ilimitado, pues que no cabe duda que entre sus límites están «los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución» (fundamento jurídico 11.º), entre los que, explícitamente, se encuentran, siguiendo el tenor del artículo 105, letra b), de la Constitución Española, «la seguridad y defensa del Estado, la averiguación de los delitos» (fundamento jurídico 9.º).

Como dice la STC 70/2002, de 3 de abril (fundamento jurídico 10.º), siguiendo la doctrina reiterada de este Tribunal, «el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho» (SSTC 57/1994, de 28 de febrero, fundamento jurídico 6.º; 143/1994, de 9 de marzo, fundamento jurídico 6.º; 98/2000, de 10 de abril, fundamento jurídico 5.º; 186/2000, de 10 de julio, fundamento jurídico 5.º; y 156/2001, de 2 de julio, fundamento jurídico 4.º)».

Por tal motivo, «precisando la anterior doctrina», la comentada STC 70/2002, de 3 de abril, trae a colación la STC 207/1996, de 16 de diciembre (fundamento jurídico 4.º), en la que se señala que resulta necesario establecer, en primer lugar, los requisitos que proporcionan una justificación constitucional objetiva y razonable a la injerencia en el derecho a la intimidad los siguientes: la existencia de un fin constitucionalmente legítimo (46); en segundo lugar, que la medida limitativa del derecho que pretenda aplicarse esté prevista en la Ley (principio de legalidad); en tercer lugar, como regla general, que la misma se acuerde, en principio, mediante una resolución judicial motivada (47); y, por fin, que deberá aplicarse

(46) Considerando como tal, según señala esta Sentencia, «el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal».

(47) No obstante, hay que reconocer que debido a la falta de reserva constitucional a favor del Juez, la Ley puede autorizar a la policía judicial para la práctica de inspecciones, reconocimientos e incluso intervenciones corporales leves, siempre y cuando se respeten los principios de proporcionalidad y razonabilidad.

con una estricta observancia del principio de proporcionalidad, concretado en tres requisitos o condiciones: idoneidad de la medida, necesidad de la misma y proporcionalidad en sentido estricto.

Además, la STC 70/2002, de 3 de abril (fundamento jurídico 10.º), «en relación con la exigencia de previsión legal» establece que «por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (artículo 81.1 CE) o limite o condiciones su ejercicio (artículo 53.1 CE), precisa una habilitación legal». Una reserva de ley que «constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas» y que «no es una mera forma, sino que implica exigencias respecto del contenido de la Ley que, naturalmente, son distintas según el ámbito material de que se trate», pero «que en todo caso el legislador ha de hacer el «máximo esfuerzo posible» para garantizar la seguridad jurídica o dicho de otro modo, «la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho» (STC 36/1991, fundamento jurídico 5.º)».

Y, como ya sostuvo la STC 169/2001, de 16 de julio (fundamento jurídico 6.º), apoyándose en una abundante cita de Sentencias del Tribunal Europeo de Derechos Humanos, las características que se han venido exigiendo por la seguridad jurídica en relación a la «calidad de la ley» habilitadora de las injerencias en un derecho reconocido en el Convenio Europeo de Derechos Humanos de 1950, se basan en que «la ley debe definir las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad».

En este sentido, siguiendo lo que ha sido constante doctrina del Tribunal Constitucional en el ejercicio de los derechos fundamentales, basado en la consideración de que los derechos fundamentales no tienen «otros límites que los fijados explícita o implícitamente en la Constitución, que son los demás derechos y los derechos de los demás, sin prevalencia apriorística de cualquiera de ellos y, por tanto, en un equilibrio inestable, sin que ninguno tenga carácter absoluto ni rango superior a los colindantes», encontramos la STC 292/2000, de 30 de noviembre (fundamento jurídico 11.º), que, en concreta relación al «derecho fundamental a la protección de datos personales», ha señalado que el mismo «no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros dere-

chos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, fundamento jurídico 7.º; 196/1987, de 11 de diciembre, fundamento jurídico 6.º; y respecto del artículo 18, STC 110/1984, fundamento jurídico 5.º), de modo que la tutela jurídica, como ha señalado la doctrina científica, «no puede estructurarse sobre modelos simplistas, como el principio de consentimiento del titular de los datos, que implica la renuncia al intervencionismo del Estado» (48), en tanto en cuanto se trata de una consideración instalada en un planteamiento que, como estamos viendo, se encuentra plenamente superado en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (49).

En la medida que no puede predicarse una prevalencia apriorística del «derecho fundamental a la protección de los datos personales» sobre cualquiera de los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, en cuanto no tiene un carácter absoluto ni rango superior a los colindantes, se está en presencia de un equilibrio inestable, que motiva que la STC 292/2000, de 30 de noviembre (fundamento jurídico 11.º), diga que «esos límites o bien pueden ser restricciones directas del derecho fundamental mismo,…, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera regular su ejercicio, lo que puede el legislador ordinario a tenor de lo dispuesto en el artículo 53.1 Constitución Española». Por lo tanto, se constata que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental, que pueden ceder, desde luego, «ante bienes, e incluso intereses constitucionalmente relevantes», como son los derivados de la Defensa

---

(48) MORALES PRATS, F., comentario al artículo 197 del Código Penal, VV.AA. Comentario al nuevo Código Penal, Gonzalo Quintero Olivares (Director), Editorial Aranzadi, S.A., Pamplona, 1996, p. 951.

(49) No en vano, en última instancia, ello nos remite, como recuerda VELASCO CABALLERO, F., en el estudio hecho en colaboración con BACIGALUPO SAGGESE, M., «Límites inmanentes» de los derechos fundamentales y reserva de ley (Dos puntos de vista a propósito de la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 15 de julio de 1993), REDA, núm. 85, Enero-Marzo 1995, CD-Rom, núms. 1-100, Civitas, Madrid, a una idea, «tan elemental» como «conocida por nuestro Derecho común (la ley no ampara el abuso del derecho: artículo 7.2 Código Civil)», reiteradamente declarada para los derechos fundamentales desde la STC 5/1983 (fundamento jurídico 7.º).

nacional, «siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero, fundamento jurídico 6.º; 18/1999, de 22 de febrero, fundamento jurídico 2.º)» (50).

Esta reserva de ley, a la que se someten los «límites inmanentes» de los derechos fundamentales, no es, por otra parte, como señala la doctrina, «absoluta, esto es, no exige, en todo caso, una estricta y exhaustiva predeterminación legal de los mismos. Todo lo contrario: una predeterminación legal de los «límites inmanentes» de tal intensidad sería contradictoria con la exigencia, igualmente constitucional, de una ponderación en el caso concreto de los derechos, bienes o valores constitucionales en conflicto. La exigencia de esta ponderación modula necesariamente, por tanto, la intensidad de la reserva de Ley a la que están sometidos los «límites inmanentes» de los derechos fundamentales» (51).

Postura doctrinal que, en definitiva, sustancialmente coincide con la del Tribunal Europeo de Derechos Humanos, en la Sentencia Klass y otros vs. Alemania, de 6 de septiembre de 1978 (52), que tras razonar, en su

---

(50) Nos encontramos, en definitiva, ante la cuestión dogmático-constitucional de los «límites inmanentes» de los derechos fundamentales, objeto de estudio por BACIGALUPO SAGGESE, M., y VELASCO CABALLERO, F., en «Límites inmanentes» de los derechos fundamentales y reserva de ley (Dos puntos de vista a propósito de la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 15 de julio de 1993), REDA, núm. 85, Enero-Marzo 1995, CD-Rom, núms. 1-100, Civitas, Madrid, cuyo origen se encuentra en la doctrina alemana de principios de la década de los '50, siendo acogida por el Tribunal Constitucional alemán, que, desde un primer momento, entendió que «la ausencia de una expresa reserva de limitación no significaba que dichos derechos fundamentales fueran ilimitables, pues operarían siempre al menos, incluso en ausencia de una expresa reserva de limitación, los «límites inmanentes» de los derechos fundamentales, derivados de la necesidad de su articulación con otros derechos, bienes, valores o intereses constitucionalmente protegidos con los que pudieran entrar en conflicto (principio de unidad de la Constitución), así como por la doctrina y jurisprudencia españolas, lo que no ha impedido una viva polémica en orden a la conceptuación y el alcance de los «límites inmanentes» como «límites» externos al derecho fundamental, que, en cuanto se sitúan «más en el ámbito de la irremediabilidad de la limitación fruto de su incorporación a un sistema complejo como el ordenamiento jurídico…», están sometidos a la reserva de ley del artículo 53.1 de la Constitución, frente a los «límites intrínsecos» (o «límites» que operan en el interior del propio derecho fundamental), que son inmediatamente operativos.

(51) Como mantiene BACIGALUPO SAGGESE, M., en el estudio hecho en colaboración con VELASCO CABALLERO, F., «Límites inmanentes» de los derechos fundamentales y reserva de ley (Dos puntos de vista a propósito de la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 15 de julio de 1993), REDA, núm. 85, Enero-Marzo 1995, CD-Rom, núms. 1-100, Civitas, Madrid.

(52) Tribunal Europeo de Derechos Humanos. 25 años de jurisprudencia 1959-1983, Cortes Generales, Madrid, pp. 469 y ss.

apartado 48, que «el Tribunal no puede constatar más que dos hechos importantes: los progresos técnicos realizado en materia de espionaje y paralelamente de vigilancia; en segundo lugar, el desarrollo del terrorismo en Europa en el curso de los últimos años», advierte que «las sociedades democráticas se encuentran amenazadas en nuestros días por formas muy complejas de espionaje y por el terrorismo, de suerte que el Estado debe ser capaz, para combatir eficazmente estas amenazas, de vigilar en secreto los elementos subversivos que operan en su territorio», viene a admitir «la existencia de disposiciones legislativas acordando los poderes de vigilancia secreta de la correspondencia, de los envíos postales y de las telecomunicaciones» (a los que cabría añadir actualmente la cesión de datos de carácter personal, y, concretamente, de los datos de tráfico en las comunicaciones electrónicas), en cuanto que, «ante una situación excepcional», son «necesarias en una sociedad democrática en la seguridad nacional y/o en la defensa del orden y en la prevención de infracciones penales», de modo que, llegados a este punto, como dice en el apartado 50, la cuestión inevitablemente se traslada a verificar «la existencia de garantías adecuadas y suficientes contra los abusos», tratándose de una apreciación, no obstante, que «no tiene más que un carácter relativo: depende de todas las circunstancias que envuelven el caso, por ejemplo la naturaleza, la extensión y la duración de las medidas eventuales, las razones requeridas para ordenarlas, las autoridades competentes para autorizarlas, ejecutarlas y controlarlas y el tipo de recursos previstos por el Derecho interno».

Complementando estas consideraciones, debemos indicar que en la Sentencia Leander vs. Suecia, de 25 de abril de 1987 (53), en su apartado 58, tras establecer que «la noción de necesidad exige que la interferencia responda a una imperiosa necesidad social, así como que la respuesta a la misma resulte proporcionada con relación al legítimo objetivo perseguido» también señala en el apartado 59, que «no puede haber duda alguna con respecto a la necesidad de los Estados contratantes de contar, al objeto de proteger la seguridad nacional, con una regulación que permita a las autoridades competentes recopilar y almacenar en registros no abiertos al público información sobre determinadas personas, así como que autorice a usar la información disponible…». En el «margen amplio» que el Estado tiene en la apreciación de la «imperiosa necesidad social» de la medida que pretenda adoptarse, en aras a la seguridad nacional, cuyo alcance, como señala el apartado 59 de esta Sentencia, «depende no sólo del tipo de

(53) En página web del Tribunal Europeo de Derechos Humanos. Concretamente, en http://hudoc.echr.coe.int/Hudoc2doc/HFJUD/si8ft/104.txt

legítimo objetivo buscado, sino también de la interferencia en cuestión», de modo que el Estado puede contar, al objeto de proteger la seguridad nacional, «con una regulación que permita a las autoridades competentes recopilar y almacenar en registros no abiertos al público información sobre determinadas personas, así como que autorice a usar la información disponible…» (54), siempre que el nivel de garantías «de estructura» que haya sido establecido evite posibles abusos en la realización de los controles como era el caso de la legislación sueca (55), circunstancia que, en el supuesto enjuiciado, desde una lectura unitaria del Convenio Europeo de Protección de Derechos Humanos de 1950, determinó que se considerase que «la falta de notificación (al demandante) de las informaciones que le conciernen no entraña por sí misma, y habida cuenta de las circunstancias del caso, una violación del artículo 13» del Convenio Europeo [derecho a un recurso efectivo ante una instancia nacional]».

III. EL CENTRO NACIONAL DE INTELIGENCIA Y LOS DATOS DE TRÁFICO DE LAS COMUNICACIONES ELECTRÓNICAS

Es en este marco normativo, teniendo en cuenta las consideraciones precedentes, donde debemos encuadrar la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (56), y la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia (57).

Como indicó el Dictamen del Consejo de Estado, de 15 de noviembre de 2001, «el anteproyecto de Ley sometido a consulta», hoy Ley Orgánica

---

(54) Lo que no impidió que los magistrados del Tribunal Europeo de Derechos Humanos, Petitti y Russo, en voto particular conjunto a esta Sentencia, de una manera contundente señalaran que «no puede ignorarse el peligro planteado por la comunicación electrónica entre los archivos de los diferentes Estados y los de la Interpol. El individuo ha de tener a su disposición el derecho a apelar contra un dato que puede proceder de un error garrafal, incluso aunque la fuente informante sea mantenida en secreto…»

(55) Como señala REVENGA SÁNCHEZ, M., Seguridad nacional y Derechos humanos. Estudio sobre la Jurisprudencia del Tribunal de Estrasburgo, Editorial Aranzadi, S.A., Pamplona, 2002, p. 90, pie de página 150, ciertamente, en este caso, «el número de garantías aducido por el Gobierno sueco, en defensa del sistema, es ciertamente espectacular…», recogiendo la Sentencia hasta «doce tipos distintos de salvaguarda», entre los que se encuentra, lógicamente en un país nórdico, la institución del «Omdusman».

(56) B.O.E. núm. 109, de 7 de mayo de 2002. pp. 16440 y ss.

(57) B.O.E. núm. 109, de 7 de mayo de 2002, pp. 16439-16440.

2/2002, de 6 de mayo (58), tiene el acierto de establecer «un régimen jurídico» que permita conciliar, por un lado, «la efectividad de derechos fundamentales como son la inviolabilidad del domicilio y el secreto de las comunicaciones garantizados, respectivamente, por lo dispuesto en los números 2 y 3 del artículo 18 de la Constitución», con las exigencias derivadas «de la seguridad nacional y la defensa del Estado, que también son cometidos propios que se imponen en una sociedad democrática al Estado de Derecho», sin «desconocer las dificultades que entraña la intervención de un órgano de procedencia judicial pero al margen el procedimiento jurisdiccional en trámite o por tramitar», obligando, «sin mengua de las peculiaridades de las actividades» del Centro, «a extremar el respeto a la tutela judicial efectiva», toda vez que «cualquier injerencia de las autoridades públicas en el ejercicio de estos derechos requiere que esté prevista en una ley y que las medidas que se establezcan sean estrictamente necesarias para los objetivos y fines que se han señalado. Así se proclama en el artículo 8 del Convenio Europeo para la protección de los derechos humanos y de las libertades públicas de 4 de noviembre de 1950, ratificado por España en 26 de septiembre de 1979, que, con relación al derecho a la inviolabilidad del domicilio y al secreto de la correspondencia, declara que no puede haber injerencia de una autoridad pública en el ejercicio de este derecho a menos que esta injerencia esté prevista por la ley y que ella constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de infracciones penales, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás».

Y todo ello sin perjuicio de tener en cuenta, además, como dice el Dictamen del Consejo de Estado, de 25 de octubre de 2001, relativo al anteproyecto de la ley reguladora del Centro, hoy Ley 11/2002, de 6 de mayo, que no se establece, con carácter general, «el control judicial de las actividades del Centro y de sus miembros», que en tanto cuanto Administración Pública, como con respecto de sus miembros, «será el que se resulte del ordenamiento jurídico general, administrativo, o, en su caso, penal», toda vez que la mencionada Ley Orgánica 2/2002, de 6 de mayo, en su articulado se limita a regular determinados «controles judiciales con carácter preventivo en forma de autorizaciones judiciales exigibles para la adop-

(58) Ley Orgánica 2/2002, de 6 de mayo, que es «complementaria» de la Ley 11/2002, de 6 de mayo, reguladora del Centro, como consecuencia de la remisión que a la misma hace el 12 de esta última Ley.

ción de aquellas 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».

Por este motivo, la expresión «control judicial» utilizada es «demasiado amplia, en cuanto que con ella no se designa más que unos determinados controles preventivos de la actividad del Centro Nacional de Inteligencia», y, en consecuencia, se debe seguir teniendo muy en cuenta que la Ley 11/2002, de 6 de mayo, al fijar la naturaleza, objetivos y funciones, así como los aspectos sustanciales de su organización y régimen jurídico del Centro Nacional de Inteligencia, es la normativa que permite el adecuado desenvolvimiento de las funciones encomendadas a este Centro en la esfera de los intereses de la Seguridad Nacional, con plena inserción en el Estado de Derecho definido en la Constitución Española.

1. Los objetivos del Centro Nacional de Inteligencia, según la Ley 11/2002, de 6 de mayo, como «fin legítimo» para acceder a los datos de tráfico de las comunicaciones electrónicas

Las funciones que legalmente han sido encomendadas al Centro Nacional de Inteligencia, en virtud de la Ley 11/2002, de 6 de mayo, son las que permiten acreditar la existencia de «fin legítimo», que responda a la «necesidad de protección de las instituciones democráticas», en aras a la protección de la «Seguridad Nacional», permitiendo que este Centro acceda a los datos de tráfico de las comunicaciones electrónicas.

Como señala concluyentemente la Exposición de Motivos de la Ley 11/2002, de 6 de mayo, «la principal misión del Centro Nacional de Inteligencia será la de proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones», en su consideración de bienes y valores de carácter constitucional, que por su importancia son susceptibles de protección. En este sentido, el artículo 1 de la Ley 11/2002, de 6 de mayo, establece que «el Centro Nacional de Inteligencia es el Organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar 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».

De acuerdo con el tenor literal del citado artículo 1 de la Ley 11/2002, de 6 de mayo, es posible destacar, como hizo el Dictamen del Consejo de Estado de 25 de octubre de 2001, que la responsabilidad que recae sobre el Centro Nacional de Inteligencia, respecto del Presidente del Gobierno y el Gobierno de la Nación, con independencia de la adscripción al Ministerio de Defensa, es facilitar informaciones, análisis, estudios o propuestas que afectan no solo a «las necesidades e intereses de la Defensa Nacional y de las Fuerzas Armadas», como pudiera ser, fundamentalmente, la independencia o integridad territorial de España, sino también a todo lo que atañe a «los intereses nacionales y a la estabilidad del Estado de derecho y sus instituciones», en perfecta correspondencia con una conceptuación moderna de lo que constituye la «Seguridad Nacional», que, en nuestro ordenamiento, vamos a identificar con la «Defensa Nacional» (59), definida en el artículo 2 de la Ley Orgánica 6/1980, de 1 de julio, por la que se regulan los criterios básicos de la Defensa Nacional y la organización militar, como «la disposición, integración y acción coordinada de todas las energías y fuerzas morales y materiales de la Nación, ante cualquier forma de agresión, debiendo todos los españoles participar en el logro de tal fin», asignándole como finalidad «garantizar de modo permanente la unidad, la soberanía e independencia de España, su integridad territorial y el ordenamiento constitucional, protegiendo la vida de la población y los intereses de la Patria, en el marco de lo dispuesto en el artículo 97 de la Constitución».

Por ello, la actual consideración de la «Seguridad Nacional» debe entenderse como la promoción y la protección de los intereses nacionales, esto es, como el conjunto de los valores y condiciones materiales que hacen posible el progreso social, económico y político de una comunidad nacional y de las entidades supranacionales de las que forma parte el Estado, participando en la protección y promoción de los intereses políticos, económicos, industriales, comerciales y estratégicos de España, entendidos no como intereses particulares o sectoriales, sino como intereses generales a toda la sociedad española, haciendo de este modo presente, una vez

(59) Nos decantamos por esta equiparación, conscientes de las dificultades inherentes al logro de una definición del término «Seguridad Nacional», que comprenda no sólo la postura tradicional que continúa aferrada al ámbito militar como elemento decisivo, sino también incorpore una aptitud innovadora que tienda a resaltar los componentes no militares. Vid., las consideraciones de SUÁREZ PERTIERRA, G., en el prólogo a la edición de Legislación sobre la Defensa nacional, Editorial Técnos, Madrid, 1988, pp. 13 y siguientes, o REVENGA SÁNCHEZ, M., El imperio de la política. Seguridad nacional y secreteo de Estado en el sistema constitucional norteamericano, Editorial Ariel, Barcelona, 1995, pp. 6 y sigueintes.

más, el viejo adagio que dice: «gouverner c'est prevoir» («gobernar es prevenir»), y con el que se quiere subrayar que una de las principales funciones de gobernar es la de «prevenir» (60).

Para el cumplimiento de los objetivos asignados, conforme el artículo 4, fundamentalmente en las letras a) y b), de la Ley 11/2002, el CNI procederá, por un lado, a «obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional»; y, por otro, a «prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población».

En consecuencia, el Centro Nacional de Inteligencia, al igual que sucede con el resto de los servicios de inteligencia, debe proceder a «la recopilación de elementos concretos de valoración en el campo de la seguridad de las instituciones y la predisposición de análisis… precisos y exactos sobre distintos perfiles de la amenaza, capaces de permitir la adopción de decisiones concretas en materia de asuntos internos e internacionales», operando «a través de la observación y la interpretación de todos aquellos fenómenos sociales, económicos y geopolíticos, susceptibles de incidir sobre el desarrollo ordenado de la comunidad nacional y sobre la propia estabilidad del Estado» asumiendo «un carácter no sólo de prevención general», sino además, como componente esencial, la formulación de propuestas «de apoyo en el ámbito del proceso de toma de decisiones de la actividad del gobierno», lo cual significa ir más allá de proporcionar «la notificación simple simple y desnuda de la verificación de un hecho —de la que cualquiera puede tener conocimiento en tiempo real gracias a la "globalización" de la información de la prensa—», introduciendo «puntos» de «análisis y valoración sobre las posibles causas, las áreas ideológicas interesadas y la eventual y presumible evolución de la situación» (61).

---

(60) BERARDINO, F., Modalitá e strumenti dell'attivitá di informazione e sicurezza tra legittimitá ed illegalitá: la problemática delle garanzie funzionali, Rivista di intelligence e di cultural professionale, n.º 9, sttembre-dicembre 1997, SISDE Servizio per le Informazioni e la Sicurezzaa Democratica, http://www.sisde.it/Rivista9.nsf/ServNavig/5.

(61) BERARDINO, F., Modalità e strumenti dell'attività di informazione e sicurezza tra legittimità ed illegalità: la problematica delle garanzie funzionali, Rivista di intelligence e di cultural professionale, n.º 9, sttembre-dicembre 1997, SISDE Servizio per le Informazioni e la Sicurezzaa Democratica, http://www.sisde.it/Rivista9.nsf/ServNavig/5.

Estas operaciones de análisis y valoración de la información están dirigidas, tanto a lo que es la inteligencia criminal, esto es, «la delincuencia internacional organizada en sus diferentes variantes, grupos terroristas, redes de narcotráfico, organizaciones dedicadas a la inmigración ilegal, al tráfico de armas, al contrabando en gran escala», que exige no «únicamente una acción policial», sino, «antes que nada, una labor de inteligencia que permita conocer, entre otros muchos factores, la dimensión de las organizaciones, sus ramificaciones de topo tipo, los verdaderos responsables, sus conexiones internacionales, el grado de penetración logrado en diferentes organizaciones y en el propio Estado, su entramado financiero», como a la inteligencia económica, es decir, «la obtención de aquella información que resulte necesaria para la defensa de los intereses económicos del Estado». Sin olvidar la inteligencia militar, que continúa «siendo un componente importante del conjunto de la política de inteligencia de un país» (62).

Por tal motivo, como ha puesto de relieve la doctrina, son muchos los interrogantes que pudiera suscitar la Ley Orgánica 2/2002, de 6 de mayo, puesto que «da la sensación de que se han trasladado precipitadamente los esquemas propios de la persecución del delito y de los delincuentes a la temática de la seguridad del Estado», aplicando «el esquema propio de la persecución criminal: exigencia de autorización judicial previa para realizar acciones que supongan invasión de espacios privados», olvidando, quizá, que se trata «de dos facetas que en parte coinciden, como lo revela el que entre los delitos más graves estén los que afectan a la seguridad del Estado (rebelión, sedición, terrorismo, delitos que comprometen la paz y la independencia del Estado y otros previstos en el Código Penal)», pero que también resulta posible diferenciar, toda vez que «no toda la actividad delictiva, sino sólo una pequeña parte, afecta a la seguridad del Estado», por cuanto que «la inmensa mayoría de los delitos no tienen dimensión política… ni comprometen la independencia del Estado y la estabilidad del sistema democrático. En todo caso, lo propio de la inteligencia estatal es prevenir acciones, sean o no delitos, de particular gravedad, y cuya persecución sería harto difícil y costosa si llegasen a perpetrarse» (63).

Se olvida, así, incluso por el propio legislador, que «la Seguridad del Estado» afronta peligros que son «normalmente de mucha mayor envergadura que los de la criminalidad ordinaria» y, lo que es fundamental en la tesis que mantenemos, «que entre sus fines no están sólo los represivos,

(62) La reforma de la comunidad de inteligencia en España, 12 de noviembre de 1999.

(63) SANTAOLALLA LÓPEZ, F., «Actos políticos, inteligencia nacional y Estado de Derecho», Revista Española de Derecho Constitucional, núm. 65, Mayo/Agosto 2002, Madrid, p. 122.

sino también, muy marcadamente, los preventivos. En muchas ocasiones no se trata de conseguir pruebas o de detener un presunto delincuente, sino de obtener información sobre grupos o personas potencialmente peligrosas para el Estado, su economía, su régimen democrático, etcétera. y de prevenir ataques futuros» (64).

Todo ello sin perjuicio de reafirmar el sometimiento de la actuación del Centro Nacional de Inteligencia al principio de legalidad, consagrado como principio universal de la actuación de las Administraciones públicas en los artículos 9.1 y 103.1 de la Constitución, que, por lo demás, constituye una preocupación constante del legislador en el momento de proceder a la configuración y actuación del Centro, como pone de relieve la Exposición de Motivos de la Ley 11/2002, de 6 de mayo, reguladora del Centro, que ya en su primer párrafo hace referencia a la necesidad de unos «servicios de información» «regidos por los principios de control y pleno sometimiento al ordenamiento jurídico», y que explícitamente se reafirma en el artículo 2.1 de la Ley, en cuanto dispone que «el Centro Nacional de Inteligencia se regirá por el principio de sometimiento al ordenamiento jurídico y llevará a cabo sus actividades específicas en el marco de las habilitaciones expresamente establecidas en la presente Ley y en la Ley Orgánica 2/2002, de 7 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia» (65).

En definitiva, en nuestra opinión, ha quedado plenamente acreditado el primer condicionamiento o requisito que, conforme la doctrina del Tribunal Europeo de Derechos Humanos, pudiera exigirse a nuestro ordenamiento jurídico para que el Centro Nacional de Inteligencia, como servicio de inteligencia, pueda legalmente acceder a los datos de tráfico de las comunicaciones electrónicas, esto es, un «fin legítimo», que se encuentra indudablemente basado en las necesidades de la «Seguridad Nacional».

---

(64) SANTAOLALLA LÓPEZ, F., «Actos políticos, inteligencia nacional y Estado de Derecho», Revista Española de Derecho Constitucional, núm. 65, Mayo/Agosto 2002, Madrid, p. 122.

(65) Siendo, precisamente, este sometimiento al «ordenamiento jurídico», en el «marco de las habilitaciones expresamente establecidas» en la Ley 11/2002, de 6 de mayo, y en la Ley Orgánica 2/2002, de 6 de mayo», lo que permite que las actividades del Centro Nacional de Inteligencia puedan ampararse en la consideración de información clasificada, con el grado de secreto del artículo 5.1 de la Ley 11/2002, evitándose, así, una «concepción del secreto de estado como prerrogativa infiscalizable del poder público». Vid., LOZANO, B., El episodio judicial de los documentos del CESID como ejemplo de las tensiones e incertidumbres del nuevo equilibrio de poderes, p. 26, trabajo que, junto con otros, se reúne en La descalificación de los secretos de Estado, Cuadernos Civitas, Madrid, 1998, recogiendo las palabras de Ferrajoli, en Jurisdicción y democracia, «Jueces para la democracia», núm. 29, julio 1997, pp. 3 y sigs.

2. Las previsiones contenidas en la Ley 11/2002, de 6 de mayo, como fundamento legal suficiente para el acceso a los datos de tráfico de las comunicaciones electrónicas

Sin ánimo de extendernos, el examen de la problemática que analizamos debe partir de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en conexión con la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. En efecto,

a) Por un lado, encontramos la Ley Orgánica 15/1999, de 13 de diciembre, que, tras disponer, en su artículo 1, que «la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar», comprende en su ámbito de aplicación, según el artículo 2.1, «los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado», con las excepciones y matizaciones que se fijan.

En esta Ley Orgánica 15/1999, de 13 de diciembre, se contienen una serie de preceptos fundamentales para una adecuada comprensión del acceso a los datos de carácter personal por parte del Centro Nacional de Inteligencia, que son los siguientes:

— El artículo 3, letra a), que considera «datos de carácter personal» a «cualquier información concerniente a personas físicas identificadas o identificables»

— El artículo 3, letra i), que define la «cesión o comunicación de datos» como «toda revelación de datos realizada a una persona distinta del interesado».

— El artículo 11.1 en el que se dispone «los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado», el cual se exceptúa, entre otros casos, conforme el artículo 11.2, letra a), «cuando la cesión está autorizada en una ley».

— Precepto este último, el del artículo 11.2, letra a), de la Ley Orgánica 15/1999, que viene a establecer, cuando así ocurra, una patente excepción al régimen general de cesión de datos personales entre Administraciones Públicas contenido en el artículo 21.1 de la Ley Orgánica 15/1999 (objeto éste último de pronunciamiento en la Sentencia del Tri-

bunal Constitucional 292/2000, de 30 de noviembre, sustancial en el análisis del presente dictamen jurídico), en el que se dispone que «los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos».

b) De otro lado, encontramos la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, que contempla, en el artículo 12, el acceso a los datos de tráfico relativos a las comunicaciones electrónicas, estableciendo, en los apartados 1 y 3, respectivamente, el deber de los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos de «retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo», en orden a la conservación de los mismos «para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así lo requieran» y comunicación «a las Fuerzas y Cuerpos de Seguridad» con «sujeción a lo dispuesto en la normativa sobre protección de datos personales» (66).

Conforme pone de manifiesto el Considerando 11 de la Directiva 2002/58/CE, de 12 de julio de 2002, del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y comunicaciones electrónicas), precisamente sobre la base del artículo 8.2 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, de 4 de noviembre de 1950, los

(66) Precepto legal que, de alguna manera, desarrolla y complementa la previsión recogida en el artículo 4.5 de la Ley Orgánica 15/1999, de 13 de diciembre, en el que se establece la obligación de cancelar los datos de carácter personal cuando éstos dejen de ser necesarios para la finalidad para la cual hubieran sido recabados o registrados, determinando que «no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrado». Sin perjuicio que, como también se dispone, reglamentariamente, se determine el procedimiento por el que, por excepción, «atendidos a los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos».

Estados miembros de la Unión Europea deben disponer de la posibilidad «de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal», a cuyo fin, según el apartado 1 del artículo 15 de la Directiva, «podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado».

El ordenamiento jurídico español se encuentra, en este punto, a consecuencia de la reciente promulgación de Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en cuya elaboración ya se tuvieron en cuenta las distintas propuestas y trabajos desarrollados en el seno de las instituciones de la UE, perfectamente adaptado a la Directiva 2002/58/CE, de 12 de julio de 2002, del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y comunicaciones electrónicas) (67), que, en su Considerando 11, sobre la base del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, prevé que los Estados miembros de la UE dispongan de la posibilidad «de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal», a cuyo fin, al amparo del apartado 1 del artículo 15 de la mencionada Directiva 2002/58/CE, se «podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado», que se difiere a un oportuno desarrollo reglamentario en el artículo 12.4 de la Ley 34/2002 (68).

c) Desde estas premisas ha de abordarse si el Centro Nacional de Inteligencia se encuentra legalmente habilitado para acceder a los datos de trá-

---

(67) D.O.C.E. L 201/37, de 31 de julio de 2002.

(68) En relación a este punto, el artículo 12.4 de la Ley 34/2002, de 11 de julio, dispone que, en todo caso, «reglamentariamente, se determinarán las categorías de datos que deberán conservarse según el tipo de servicio prestado, el plazo durante el que deberán retenerse en cada supuesto dentro del máximo previsto en el este artículo, las condiciones en que deberán almacenarse, tratarse y custodiarse y la forma en que, en su caso, deberán entregarse a los órganos autorizados para su solicitud y destruirse, transcurrido el plazo de retención que proceda, salvo que fueran necesarios para estos u otros fines previstos en la Ley».

fico de las comunicaciones electrónicas, pese a que, como tal, no aparece expresamente mencionado en el artículo 12 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, teniendo en cuenta que la interdicción de las conductas de cesión o comunicación de datos personales, salvo consentimiento del interesado, del artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, como parte sustancial de los «principios de protección de datos», cede en el caso de que la «cesión esté autorizada en una ley», esto es, cuando concurran circunstancias que, a juicio del legislador, permitan considerar razonable la medida que pretenda adoptarse.

El artículo 11.2, letra a), de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, es donde, en nuestra opinión, se pudieran encontrar acogidas las previsiones del artículo 5.5 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y, en concreto, la posibilidad de acceder a los datos de tráfico de las comunicaciones electrónicas; en él se establece que «para el cumplimiento de sus funciones, el Centro Nacional de Inteligencia podrá llevar a cabo investigaciones de seguridad sobre personas o entidades en las formas previstas en esta Ley y en la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia. Para la realización de estas investigaciones podrá recabarse de organismos e instituciones públicas o privadas la colaboración precisa».

En nuestra opinión, visto lo expuesto en la Exposición de Motivos de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, en la que, entre otras cosas, se dice, de una manera expresa y concluyente, que «la principal misión del Centro Nacional de Inteligencia será proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones», que ha sido posteriormente recogida en el artículo 1, en consonancia con el comentado artículo 4, letras a) y b), y el principio de coordinación con las Administraciones Públicas del artículo 5, todos ellos de la Ley 11/2002, y en aras a «los criterios de eficiencia y servicio a los ciudadanos» como específica el artículo 3.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, resulta evidente concluir que lo dispuesto en el artículo 5.5 de la Ley 11/2002, de 6 de mayo, como tal, constituye la necesaria previsión legal que autoriza la cesión o comunicación de datos de carácter personal que pudieran solicitarse de organismos e instituciones públi-

cas y privadas, como consecuencia de las investigaciones de seguridad que dicho Centro esté llevando a cabo, y entre los que deben encontrarse los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información de acuerdo con el artículo 12 de la Ley 34/2002, de 12 de julio, y artículo 11.2, letra a), de la Ley Orgánica 15/1999, de 13 de diciembre.

3. La cláusula de la «calidad de ley» en el fundamento legal para que el Centro Nacional de Inteligencia acceda a los datos de trafico de las comunicaciones electrónicas

El examen del fundamento legal que permite al Centro Nacional de Inteligencia acceder a los datos de tráfico de las comunicaciones electrónicas constituye la clave de la problemática que analizamos, pues, tal y como ha señalado el Tribunal Europeo de Derechos Humanos, no basta sólo verificar la existencia de una normativa que ampare esta posibilidad, sino que, además, deben concurrir las necesarias características de la «calidad de ley», en cuya virtud se fijen, con la suficiente claridad, las suficientes garantías frente a cualquier injerencia arbitraria (aunque no se requiera que se incluyan detalladamente los requisitos y procedimientos correspondientes), en este caso, sobre la base del «derecho fundamental a la protección de datos personales».

Según hemos apuntado, sobre la base del Considerando 11 de la Directiva 2002/58/CE, sin entrar en contradicción con el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, de 4 de noviembre de 1950, se prevé que los Estados miembros de la UE dispongan de la posibilidad «de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal», a cuyo fin, al amparo del apartado 1 del artículo 15 de la mencionada Directiva, se «podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado».

De acuerdo con lo dispuesto en artículo 8.2 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, y por la doctrina asentada por la jurisprudencia del Tribunal

Europeo de Derechos Humanos (69), no cabe considerar que exista «injerencia de la autoridad pública» (70) en el ejercicio del derecho a la vida privada y familiar, cuando dicha injerencia, «esté prevista por la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás», dentro del necesario equilibrio «entre el ejercicio por el individuo del derecho que le garantiza el párrafo 1 (del artículo 8) y la necesidad, según el párrafo 2 (de la citada norma), de imponer una vigilancia secreta para proteger a la sociedad democrática en su conjunto» (en tesis que fue posteriormente acogida por la reciente Sentencia del Tribunal Europeo de Derecho Humanos, de 13 de febrero de 2001, Caso Ezzouhdi contra Francia (71), esto es, con arreglo a un juicio de evaluación de la proporcionalidad de la medida que se pretenda adoptar, previamente acompañado de una detallada regulación de los requisitos y procedimientos que permitan hacerla efectiva, así como de las suficientes garantías frente a cualquier injerencia arbitraria.

En este sentido, el Dictamen 10/2001, de 14 de diciembre de 2001, relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo, del Grupo 29 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, subraya «la obligación de respetar el principio de proporcionalidad en relación con toda medida de restricción del derecho fundamental del respeto a la vida privada establecido en el artículo 8 del Convenio Europeo sobre Derechos Humanos y la jurisprudencia correspondiente, lo que supone, entre otras cosas, la obligación de demostrar que toda medida adoptada responde a una «exigencia social imperativa»». Especificando, en consecuencia, que «las medidas simplemente «útiles» o «convenientes» no pueden restringir los derechos y las libertades fundamentales», de modo que se siente obligado a plantear «la necesidad de entablar un amplio debate sobre las medidas destinadas a luchar contra el terrorismo, analizando todas sus consecuencias en materia de derechos y libertades fundamenta-

---

(69) Entre otras, la Sentencia de 6 de septiembre de 1978, caso Klass y otros contra Alemania, de 6 de septiembre de 1978,

(70) Esta referencia a la «autoridad pública» no debe identificarse con «autoridad judicial», en tanto en cuanto «la exclusión del control judicial no transgrede los límites que han de predominar necesariamente en una sociedad democrática», aunque hay que reconocer que debiera «considerarse deseable», como señala la citada Sentencia del Tribunal Europeo de Derechos Humanos, de 6 de septiembre de 1978.

(71) TEDH 2001/85

les de las personas, rechazando la confusión entre la lucha contra el terrorismo real y la lucha contra la delincuencia en general y limitando asimismo las medidas procesales que interfieren en la vida privada a las restricciones necesarias» (72).

En definitiva, resulta necesario introducir en este planteamiento, en primer lugar, el oportuno juicio de evaluación de la proporcionalidad en la medida de acceso a los datos personales, en concreto, de los datos del tráfico de las comunicaciones electrónicas, que debe inferirse inmediatamente «tanto de la regulación como la práctica de las mismas», en cuanto que han de limitarse «a las que se hallen dirigidas a un fin constitucionalmente legítimo que pueda justificarlas» y «sólo en la medida que supongan un sacrificio del derecho fundamental estrictamente necesario para conseguirlo», de tal forma que «resulten (tales medidas) proporcionadas a ese sacrificio», partiendo de los presupuestos materiales de la intervención (investigación, conexión de las personas con los hechos) y de la necesidad y adecuación de la medida (razones y finalidad de la misma), en consonancia con la doctrina que ha sido acogida, entre otras muchas, en la STC 202/2001, de 15 de octubre, o en la STC 49/1999, de 5 de abril, y reiteradamente manifestada por la jurisprudencia del Tribunal Supremo español.

Este principio de proporcionalidad debe traducirse, asimismo, en el orden práctico, siguiendo el criterio de la Agencia de Protección de Datos, por ejemplo, en el informe de 26 de septiembre de 1997, respecto de la actuación de la Policía Judicial en materia de datos personales, en los siguientes requisitos:

Primero. Ha de tratarse de la obtención de los datos necesarios para la prevención de un peligro, amenaza o agresión real contra los intereses nacionales de orden político, económico, industrial, comercial y estratégico, y el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, la independencia o integridad territorial de España, la seguridad del Estado, estabilidad de sus instituciones, así como el bienestar de la población, en cumplimiento de los objetivos del Centro Nacional de Inteligencia asignados en virtud de la Ley 11/2002.

Segundo. En atención al principio de proporcionalidad de la medida adoptada, que afecta a un derecho de carácter fundamental, no pueden realizarse peticiones masivas de datos, lo que exige que se trate de peticiones concretas y específicas.

Tercero. La petición de datos de carácter personal tiene que realizarse mediante petición suficientemente motivada, sin perjuicio de la considera-

(72) http://europa.eu.int/comm/internal_market/en/dataprot/wpdoc/index.htm.

ción de clasificada, con el grado de secreto, que poseen las actividades del Centro Nacional de Inteligencia, conforme el artículo 5.1 de la Ley 11/2002, de 6 de mayo.

Cuarto. Deber de conservación de los datos, que, conforme al precepto anteriormente citado, constituyen información clasificada, con el grado de secreto.

Requisitos que, a su vez, se relacionan con la denominada «calidad de la ley» (según terminología reiteradamente utilizada por la jurisprudencia del Tribunal Europeo de Derechos Humanos), con la que se hace referencia a la accesibilidad y previsibilidad de la ley, esto es, que sea lo suficientemente clara a la hora de señalar las circunstancias y condiciones por las que se autoriza a los Poderes públicos a recurrir a la medida de acceso a los datos de tráfico de las comunicaciones electrónicas, en cuanto medida secreta y potencialmente peligrosa para la vida privada contemplada en el artículo 8.1 del Convenio Europeo de Derechos Humanos, necesitado de la incorporación de las garantías o condiciones para una adecuada protección frente a cualquier tipo injerencia que pudiera ser calificada como arbitraria (73).

Condiciones estrictas que, como señalan las Sentencias del Tribunal Europeo de Derechos Humanos, entre otras, en el Caso Klass y otros vs. Alemania, de 6 de septiembre de 1978, tienen que ir referidas tanto «a la aplicación de las medidas de vigilancia» como «al tratamiento de las informaciones obtenidas», con las que se impide, lógicamente, como dice el apartado 51 de la citada Sentencia, que estas medidas se tomen «al azar, irregularmente o sin estudio apropiado» o que se adopte una vigilancia «exploratoria o general», al tiempo que justifica, como dice el apartado 58 de esta Sentencia, la falta de «una notificación ulterior a cada individuo afectado» en cuanto que ello podría suponer la revelación de «los métodos de trabajo de los servicios informativos, sus campos de observación e, incluso, la identidad de sus agentes».

---

(73) Condiciones estrictas que, como señala las Sentencias del Tribunal Europeo de Derechos Humanos, entre otras, en el Caso Klass y otros vs. Alemania, de 6 de septiembre de 1978, tiene que ir referidas tanto «a la aplicación de las medidas de vigilancia» como «al tratamiento de las informaciones obtenidas», con las que se impide, lógicamente, como dice el apartado 51 de la citada Sentencia, que estas medidas se tomen «al zar, irregularmente o sin estudio apropiado» o que se adopte una vigilancia «exploratoria o general», al tiempo que justifica, como dice el apartado 58 de esta Sentencia, la falta de «una notificación ulterior a cada individuo afectado» en cuanto que ello podría suponer la revelación de «los métodos de trabajo de los servicios informativos, sus campos de observación e, incluso, la identidad de sus agentes».

No en vano, como ha señalado la Sentencia del Tribunal Europeo de Derechos Humanos, de 4 de mayo de 2000, Caso Rotaru vs. Rumanía (74), el expreso reconocimiento de la necesidad «en una sociedad democrática», de «servicios de información puede considerarse legítima», no debe hacernos olvidar que «el poder de vigilar en secreto a los ciudadanos únicamente es tolerable según el Convenio en la medida estrictamente necesaria para la protección de las instituciones democráticas» (Sentencia Klass y otros vs. Alemania), máxime cuando, «tanto el almacenamiento por parte de una autoridad pública de datos relativos a la vida privada de un individuo como su utilización y la negativa de conceder la facultad de refutarlos, constituyen una injerencia en el derecho al respecto de su vida privada garantizado por el artículo 8.1 del Convenio» (Sentencias Leander vs. Suecia; Kopp vs Suiza de 25 de marzo de 1998; y Amann vs.Suiza), de modo que la posibilidad de un poder público adopte esta medida exige que la misma se encuentre «prevista por la Ley», esto es, que tenga «una base en el derecho interno», y, además, que concurra una «calidad de ley» en la norma que pretenda invocarse, que no sólo la haga «accesible al justiciable y previsible», sino que también fije con la precisión suficiente las condiciones en las que puedan recogerse, almacenarse y utilizarse informaciones relativas a la vida privada que deriven de datos personales a los que se haya podido tener acceso, y las garantías adecuadas y suficientes contra posibles abusos, sustrayendo la posibilidad de establecer un control de «la legitimidad del fin legítimo perseguido por las medidas ordenadas», sin olvidar que, como dice esta Sentencia, «un sistema de vigilancia secreto destinado a proteger la seguridad nacional supone el riesgo de minar o destruir la democracia con la excusa de defenderla (Sentencia Klass y otros anteriormente citada)» (75).

Como también se encarga de recordar la STC 292/2000, de 30 de noviembre (fundamento jurídico 15), en lo que se refiere a nuestro ordenamiento, estas limitaciones deben estar «justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril,

---

(74) TEDH 2000/130

(75) En la misma subyacen los peligros de la razón de Estado que acechan incluso a los Estados democráticos. Como bien señaló en su momento TEIGTEN, P.H., que junto a Sir David Maxwell-Fyfe y Fernand Dehousse participó en la elaboración del Convenio Europeo de Derechos Humanos, «tras el Estado, como tentación permanente, cualquiera que sea la forma que asuma, incluso la democrática, aparece siempre el peligro de la razón de Estado» (Recueil des Travaux Préparatorires, La Haya, Martinus Nijhoff, vol I, p. 41) (citado por REVENGA SÁNCHEZ, M., Seguridad nacional y Derechos humanos. Estudio sobre la Jurisprudencia del Tribunal de Estrasburgo, Editorial Aranzadi, S.A., Pamplona, 2002, p. 23).

fundamento jurídico 8.º, y las allí citadas)» y ser «proporcionadas al fin perseguido con ellas (SSTC 11/1981, fundamento jurídico 5.º, y 196/1987, fundamento jurídico 6.º)», esto es, han de tener «un fundamento constitucional» y ser «proporcionadas las limitaciones del derecho fundamental establecida por una Ley (STC 178/1985)», pero también es necesario que no adolezcan de «falta de certeza y previsibilidad en los propio límites que impone y su modo de aplicación…», puesto que, si así fuera, se lesionaría «el principio de seguridad jurídica (artículo 9.3 de la Constitución), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, fundamento jurídico 7.º, por todas)», y «el contenido esencial del derecho fundamental así restringido», en cuanto se establecerían unos límites que «lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, fundamento jurídico 15.º; 142/1993, de 22 de abril, fundamento jurídico 4.º; y 341/1998, de 18 de noviembre, fundamento jurídico 7.º)».

De ahí la importancia del establecimiento de mecanismos objetivos de control de los que carece, al menos en la intensidad que sería deseable, la normativa que estamos analizando de la Ley 11/2002, de 6 de mayo, al contrario de lo que sucedía, por ejemplo, con la legislación alemana, con la denominada Ley G 10, de 13 de agosto de 1968 (objeto de análisis en la Sentencia del Tribunal Europeo de Derecho Humanos, Caso Klass y otros vs. Alemania, de 6 de septiembre de 1978), o con la legislación sueca (Sentencia Caso Leander vs. Suecia, de 25 de abril de 1987), en la que el Gobierno Sueco, en el oportuno trámite procesal, se preocupó en señalar hasta «doce tipos distintos de salvaguarda» de la medida, entre los que se encuentra, tratándose de un país nórdico, la institución del «Ombusman» (76).

Y, en este punto, nuestro ordenamiento jurídico, tal como sucedía en la legislación rumana analizada en la citada Sentencia y como se consignó en los apartados 57 y 69 de la misma, en particular la previsión contenida en el artículo 5.5 de la Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia, es claramente insuficiente para definir con nitidez la extensión y las modalidades de ejercicio del poder que pueda tener el Centro Nacional de Inteligencia para acceder a los datos de carácter personal, toda vez que ninguna disposición del derecho interno fija los límites que hay que respetar en el ejercicio de estas prerrogativas, define el tipo de

(76) REVENGA SÁNCHEZ, M., Seguridad nacional y Derechos humanos. Estudio sobre la Jurisprudencia del Tribunal de Estrasburgo, Editorial Aranzadi, S.A., Pamplona, 2002, p. 90, pie de página 150.

informaciones que pueden ser registradas, las categorías de personas susceptibles de ser objeto de medida de vigilancia tales como la recogida y la conservación de datos, las circunstancias en las que se pueden tomar dichas medidas, el procedimiento a seguir, o los límites en cuanto a la antigüedad de las informaciones que se poseen ni a la duración de su conservación, así como tampoco se fija una protección adecuada contra arbitrariedades que pudieran tener lugar, al no estar previsto un suficiente «mecanismo objetivo de control mientras las medidas permanezcan secretas» (a diferencia de la legislación alemana, objeto de análisis en la mencionada Sentencia Klass y otros vs. Alemania), a lo que pudiera añadirse, enseguida, la tentación de pretender otorgar, en todo caso, a los datos de carácter personal la clasificación de secreto al amparo del artículo 5.1 de la Ley 11/2002, sustrayéndolas al ámbito de aplicación de la Ley Orgánica 15/1999, en cuanto que se incorporarían a ficheros sometidos a la normativa sobre protección de materias clasificadas y que se encuentran explícitamente fuera de su ámbito de aplicación, según el artículo 2.2, letra b), de esta Ley Orgánica.

Es, pues, en este aspecto, donde se detecta, a nuestro parecer, la carencia más relevante de nuestro ordenamiento jurídico respecto a la legitimidad del acceso por el Centro Nacional de Inteligencia a los datos personales, que deriva, en el fondo, de una situación que arrastra en el tiempo y que responde, en definitiva, a un cierto olvido de la función de inteligencia por el legislador español, puesta de manifiesto, incluso, en la propia redacción de la Constitución Española de 1978, en la que ya fue significativo cómo los integrantes de la Comisión de redacción del anteproyecto de Constitución sólo se preocuparon de las restricciones al «derecho fundamental al secreto de las comunicaciones» exclusivamente como un medio policial de investigación criminal y como medio de prueba, sometido a las normas del proceso penal, exigiendo la oportuna autorización judicial, sin tener en cuenta las restricciones que pudieran afectar a otros derechos fundamentales (como es el caso del «derecho fundamental a la protección de datos personales» del artículo 18.4 de la Constitución) que pudieran derivar de la razones de «Seguridad Nacional», distintas de la lucha contra el delito y que no obedecen a parámetros procesales penales.

De ahí que, sin perjuicio de que pudiera tenerse en cuenta, como dijo el voto particular del juez L-E. Pettiti a la Sentencia del Tribunal Europeo de Derechos Humanos, Malone vs. Reino Unido de la Gran Bretaña e Irlanda del Norte, de 27 de octubre de 1983 (en una reflexión que trasladamos a la cesión de datos de tráfico de las comunicaciones electrónicas), que «es preferible prever la legalidad de determinadas escuchas en un marco jurídico establecido que dejar una laguna legal que puede colmarse

arbitrariamente», deberían, además, adoptarse, en nuestra opinión, una serie de medidas normativas que atemperaran las dudas sobre la legalidad del acceso a los datos de tráfico de las comunicaciones por el Centro Nacional de Inteligencia. Estas actuaciones normativas se moverían en dos planos distintos:

En primer lugar, sería necesario que por parte del Centro Nacional de Inteligencia, mediante la correspondiente Instrucción del Secretario de Estado Director, se fijaran cuáles son las bases de datos de carácter personal que no tendrían por qué tener la consideración de información clasificada, con el grado de secreto, conforme lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales, tal y como establece el artículo 5.1 de la Ley 11/2002, de 6 de mayo, reguladora del Centro, posibilitando, de este modo, contrario sensu el artículo 105, letra b), de la Constitución Española, el acceso a los archivos o registros administrativos en los que dichos datos personales se encontraran almacenados, estableciendo la identificación de la base de datos, suministro o ingreso, autorización de acceso, plazos para la verificación y duración del almacenamiento, entre otros condicionamientos.

Esta posibilidad existe, desde el momento en que la Disposición final primera del Real Decreto 593/2002, de 28 de junio, por el que se aprueba el régimen económico presupuestario del Centro Nacional de Inteligencia (77), ha previsto, aunque no sea en unos términos muy precisos, la difusión de datos de este Centro, «cuando en cumplimiento de la normativa vigente sea precisa la comunicación de datos…, a efectos estadístico, de solicitudes, de altas en bases de datos u otros, se faculta al mismo para acordar con las personas, Organismos o Instituciones públicas o privadas responsables un procedimiento de comunicación que salvaguarde la protección de las informaciones clasificadas».

En segundo lugar, sería necesario que se colmara el déficit normativo que se advierte en nuestro ordenamiento jurídico, tal y como ha venido admitiendo la propia jurisprudencia del Tribunal Europeo de Derechos Humanos, mediante la incorporación de disposiciones de rango inferior al legislativo, como pudiera ser mediante la oportuna Instrucción de la Agencia de Protección de Datos, dictada al amparo del artículo 37, letra c), de la Ley Orgánica 15/1999, de 13 de diciembre, que, entendemos, no vulneraría la reserva de ley (artículos 53.1 y 83.1 de la Constitución Española), por cuanto que se trataría de una regulación infralegal limitada a fijar, por exigencias prácticas, en este concreto campo de las funciones

(77) B.O.E. núm. 155, de 29 de junio.

del Centro Nacional de Inteligencia, determinados aspectos de carácter secundario y auxiliar de la regulación del ejercicio del «derecho fundamental a la protección de datos personales», con sujeción a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (78).

Se trata, en consecuencia, de respetar el contenido esencial del «derecho fundamental a la protección de datos personales», de manera que no puede entenderse que existe un apoderamiento a la Administración (en este caso, el Centro Nacional de Inteligencia) que le permita restringir derechos fundamentales a su discreción, decidiendo sin el adecuado control la obtención, almacenamiento, tratamiento, uso y cesión de datos de tráfico de las comunicaciones electrónicas cuando estime conveniente y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional sobre la base de las previsiones del artículo 5.5 de la Ley 11/2002, en relación con la habilitación del artículo 11.2, letra a), de la Ley Orgánica 15/1999.

Lógicamente, todo ello sin perjuicio de proceder, en su momento, a la necesaria reforma de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, en un sentido similar a como hizo la Disposición adicional Cuarta de la Ley Orgánica 15/1999, de 13 de diciembre, en el ámbito tributario, modificando el artículo 112.4 de la Ley General Tributaria, o tomando, incluso, como ejemplo la significativa Ley Federal para la Protección de la Constitución alemana (§§ 10 y siguientes), en relación a las actividades de la Oficina Federal para la Protección de la Constitución (Verfassungschutz) (79).

---

(78) En este sentido, como señaló la mencionada STC 292/2000, de 30 de noviembre (fundamento jurídico 14.º, párrafo segundo), «la remisión a la regulación reglamentaria de materia ligada a la reservada a la Ley es preciso, pues, que se formule en condiciones tales que no contraríe materialmente la finalidad de la reserva, de la cual derivan, según la STC 83/1984, «ciertas exigencias en cuanto al alcance lde las remisiones o habilitaciones legales a la potestad reglamentaria, que pueden resumirse en el criterio de que las mismas sean tales que restrinjan efectivamente el ejercicio de esa potestad a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley»», sin defraudar, con ello, «la previsión del artículo 53.1 de la Constitución (STC 101/1991, de 13 de mayo, fundamento jurídico 3.º)».

(79) Resumidamente, la Ley Federal para la Protección de la Constitución alemana contiene una detallada regulación del almacenamiento, procesamiento y utilización de datos relativos a las personas (§ 10), la enmienda, eliminación y el bloqueo de datos (§§ 12 y 13), la regulación de archivos que contengan datos personales (§ 14), así como la información al titular de los datos y causas que la excepcionan (§ 15).

IV. CONSIDERACIONES FINALES

PRIMERA. La tesis que hemos mantenido en las páginas precedentes se basa en un nuevo entendimiento de lo que debe ser el ámbito material de las comunicaciones, que permite separar el proceso comunicativo como tal, desde su inicio hasta su fenecimiento, amparado en el «derecho fundamental al secreto de las comunicaciones», de los datos de carácter personal de emisor y receptor una vez finalizada la comunicación, que debe recibir la oportuna protección constitucional «a través de las normas que tutelan la intimidad u otros derechos» como ha reconocido la STC 70/2002, de 3 de abril, confirmando la solución jurisprudencial de las SSTS de 22 de marzo de 1999 y 7 de diciembre de 2001.

Entendemos que constituye la necesaria evolución que debe seguir la protección de los datos personales en el ámbito de lo que hoy vienen denominándose «comunicaciones electrónicas», a consecuencia del desarrollo normativo comunitario y nacional, que ha permitido configurar en nuestro ordenamiento jurídico el nuevo «derecho fundamental a la protección de los datos personales» en la comentada Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, sobre la base de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

SEGUNDA. Desde esta perspectiva, teniendo en cuenta que el artículo 3, letra a), de la Ley Orgánica 15/1999, de 13 de diciembre, define «dato de carácter personal» como «cualquier información concerniente a personas físicas identificadas o identificables», deben considerarse como tales, siguiendo el inciso final del Considerando 15 de la reciente Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), a los datos de tráfico asociados a las comunicaciones electrónicas, que comprenden, «entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión», así como también «al formato en que la red conduce la comunicación», y que estos no forman parte de la confidencialidad de las comunicaciones electrónicas, pese a estar íntimamente relacionados con ellas, como cabe deducir del artículo 5 de esta Directiva, pese a comprenderlos bajo el epígrafe común de «confidencialidad de las comunicaciones».

En efecto, el artículo 5 de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, de alguna manera procede a distinguir ambos ámbitos, cuando establece, por un lado, que «los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público», motivando la prohibición de «la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones», y, por otro, haciendo particular referencia a «los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15» de la presente Directiva, esto es, y en ambos casos, con las excepciones que derivan de la protección de «la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas».

TERCERA. Por consiguiente, en tanto en cuanto se trata de datos personales, es en correspondencia con el marco legislativo contenido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, desde el que debe examinarse la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, respecto de la posibilidad legal de cesión al servicio de inteligencia español de los datos de tráfico de las comunicaciones electrónicas, analizando no sólo la legitimidad de la cesión de estos datos, sino también si esta cesión goza de la oportuna cobertura legal.

En consecuencia, como señalaron las Sentencias del Tribunal Europeo de Derecho Humanos, Klass y otros vs. Alemania, de 6 de septiembre de 1978, y Rotaru vs. Rumanía, de 4 de mayo de 2000, si bien es cierto que en una sociedad democrática, la existencia de servicios de información puede considerarse legítima, el poder de vigilar en secreto a los ciudadanos únicamente es tolerable, según el Convenio Europeo de Derechos Humanos, cuando sea estrictamente necesario para la protección de las instituciones democráticas, y siempre que se reúnan dos presupuestos: 1.º. Que tenga un «fin legítimo», respondiendo a la «necesidad de protección de las instituciones democráticas»: en este caso, sería la protección de la «Seguridad Nacional»; y, 2.º. Que dicha limitación se encuentre «prevista en una ley».

Esta segunda condición, a su vez, implica, por un lado, que la medida que pretenda adoptarse tenga una base legal o algún fundamento en el Derecho interno. En este sentido, como dice la Sentencia Tribunal Europeo de Derechos Humanos, Caso Huvig vs. Francia, de 14 de abril de 1990, en su apartado 28, el término «ley» deberá entenderse en su sentido «material» y no «formal»», incluyendo las disposiciones de rango inferior al legislativo y el «derecho no escrito», y, al propio tiempo, a la jurisprudencia, toda vez que «en un ámbito amparado por el derecho escrito, la «ley» es el texto en vigor tal como los Tribunales competentes lo han interpretado teniendo en cuenta, en su caso, la constante evolución jurídica»; y, en segundo lugar, la presencia de los requisitos derivados de la «calidad de la ley»: que sea accesible y previsible, esto es, debe ser lo suficientemente clara para señalar a todos las circunstancias y condiciones en que autoriza a los Poderes públicos a recurrir a una injerencia así, secreta y posiblemente peligrosa, así como las garantías precisas. De modo que, como señaló la Sentencia Tribunal Europeo de Derechos Humanos, de 14 de abril de 1990, Caso Huvig vs. Francia, recogiendo las observaciones contenidas en la Sentencia Silver y otros vs. Reino Unido de la Gran Bretaña e Irlanda de Norte, de 25 de marzo de 1983, en su apartados 88, «la ley que conceda facultades discrecionales debe fijar su alcance, aunque no se requiera que se incluyan en ella detalladamente los requisitos y procedimientos correspondientes». «Hasta dónde ha de llegar la precisión de la ley a este respecto», continúa esta Sentencia, deberá hacerse evitando cualquier clase de pronunciamiento abstracto sobre la conformidad de una determinada legislación con el Convenio Europeo de Derechos Humanos, en tanto en cuanto «dependerá de la materia de que se trate». La ley «debe definir el alcance y la manera de utilizar dicha facultad con la suficiente claridad y proporcionar al individuo la adecuada protección contra la injerencia arbitraria»; en caso contrario, si la facultad de apreciación concedida al Poder ejecutivo o al juez no tuviera límites, la ley «sería contraria a Derecho».

CUARTA. Y es precisamente, en este último requisito, donde se constata, a nuestro parecer, la carencia más relevante de nuestro ordenamiento respecto a la legitimidad del acceso por el Centro Nacional de Inteligencia a los datos personales, que obliga a un necesario desarrollo normativo e, incluso, a la oportuna modificación legislativa. Como ha sido pacíficamente aceptado doctrinalmente, para que un Estado pueda ser calificado como de Derecho tienen que ser reconocidos los Derechos Fundamentales y el principio de legalidad de la Administración. En consecuencia, el Centro Nacional de Inteligencia, sólo en la medida que se acomode al «marco

de las habilitaciones» establecido en la Ley 11/2002, de 6 de mayo, y en la Ley Orgánica 2/2002, de 7 de mayo, y dentro del más escrupuloso respeto de los Derechos fundamentales (artículo 53.1 de la Constitución) (80), podrá llevar a cabo sus actividades, sin necesidad de acudir, sin más, a considerarla información clasificada, con el grado de secreto, conforme el artículo 5.1 de la Ley 11/2002. De este modo, se evitaría una criticable «concepción del secreto de estado como prerrogativa infiscalizable del poder público» (81) que obstaculiza el pleno control de legalidad por los Tribunales, y que genera, a su vez, una desconfianza o recelo en el conjunto de los ciudadanos, así como una falta social de sintonía de lo que son las necesidades derivadas de la «Seguridad Nacional» (82).

---

(80) Como dice JORDANO FRAGA, J., en La nulidad de los actos que lesionen el contenido esencial de los derechos y libertades fundamentales susceptibles de amparo constitucional, REDA núm. 90, Abril-Junio 1996, CD-ROM REDA núms. 1-100, «no sin razón ha afirmado HÄBERLE que hoy «el Estado constitucional se transforma en «Estado de derechos fundamentales» y la sociedad, en «sociedad de derechos fundamentales»». Siendo así que, como señala SCHNNEIDER, el Estado de Derecho libre es equivalente «a Estado de derechos fundamentales», motivando que el propio legislador deba ser consciente «del impacto transformador de los derechos fundamentales».

(81) LOZANO, B., El episodio judicial de los documentos del CESID como ejemplo de las tensiones e incertidumbres del nuevo equilibrio de poderes, p. 26, trabajo que, junto con otros, se reúne en La descalificación de los secretos de Estado, Cuadernos Civitas, Madrid, 1998, recogiendo las palabras de FERRAJOLI, L., en Jurisdicción y democracia, «Jueces para la democracia», núm. 29, julio 1997, pp. 3 y ss.

(82) Siguiendo las reflexiones de PAREJO ALFONSO, L., Público y privado en la Administración Pública, Estudios jurídicos en homenaje al profesor Aurelio Menéndez, Vol.- IV, Editorial Civitas, S.A., Madrid, 1996, p. 4684, en orden al «principio del Estado democrático (artículo 1.1 de la Constitución) y, más concretamente, la determinación básica de la emanación del pueblo de todos los poderes del Estado (artículo 1.2 de la Constitución)», que «puede (y debe) ciertamente interpretarse en el sentido de un mayor acercamiento entre sociedad y Estado, si se quiere incluso de una determinada y fuerte imbricación entre una y otro», hubiera sido conveniente que la Ley 11/2002, de 6 de junio, no sólo proclamara la sujeción de este Centro al «principio de sometimiento al ordenamiento jurídico», sino que, además, permitiera conocer el sentido y los fines de sus actividades, como hace, según dice GONZÁLEZ-VARAS IBÁÑEZ, S. (El CESID, La Ley, Año XXII, Número 5300, de 3 de mayo de 2001), el Verfassungsschutz, el Servicio de Protección de la Constitución alemán, que anualmente informa «con especial detalle —a los ciudadanos— acerca de los distintos grupos extremistas o terroristas que pueden atentar contra el orden constitucional y la convivencia pacífica».