Mariano Daranás Peláez★

Sentencia del Tribunal Constitucional Federal

(Sala Primera) de la República Federal de Alemania de 2 de marzo de 2010 sobre los tres recursos de inconstitucionalidad BvR 256/08, BvR 263/08 y BvR 568/708 contra los artículos 113a y 113b de la Ley de Telecomunicaciones (texto modificado de 2007) y 100g, apartado 1, inciso primero, de la de Enjuiciamiento Criminal (texto modificado por la propia Ley de Telecomunicaciones)[1]

Sumario: I. INTRODUCCIÓN: ANTECEDENTES Y PLAN DE LA EXPOSICIÓN.—1.1. Antecedentes.—1.2. Plan de la exposición.—II. REPRODUCCIÓN Y RESUMEN DE LOS PRECEPTOS RECURRIDOS.—2.1. Artículo 113*A* de la Ley de Telecomunicaciones *(TKG*).—2.2. Artículo 113b de la TKG.—2.3 Artículo 100*g* de la *StPO*.—III. IDENTIDAD Y ARGUMENTOS DE LOS RECURRENTES.—3.1. Argumentos relativos a la Directiva 2006/24/CE (párr. 92-94).—3.2. Argumentos basados en la Ley Fundamental (LF) de la República Federal de Alemania (RFA).—3.2.1. *Atentado al secreto de las telecomunicaciones.*—3.2.2. *Atentado a la libertad profesional* —3.2.3. *Atentado al derecho de propiedad.*—3.2.4. *Atentado a las libertades de opinión, información y difusión radiofónica.*—3.2.5. *Atentado al principio de igualdad.*—IV. CONTESTACIÓN DEL GOBIERNO FEDERAL Y POSICIÓN DE LOS ÓRGANOS PERSONADOS EN EL RECURSO.—4.1. Contestación del Gobierno Federal.—4.1.1. *Inadmisibilidad a trámite de los tres recursos*.—4.1.2. *Carencia de fundamento sustantivo*.—4.2. Posición del Tribunal Administrativo Federal (*Bundesverwaltungshof*).—4.3. Posición del Tribunal Supremo Federal (*Bundesgerichtshof*).—4.4. Posición del Comisionado Federal para la Protección de Datos y la Libertad de Información.—4.5. Posición del Comisionado de BERLIN para Protección de Datos y Libertad de Información.—V. CONSIDERANDOS.—5.1. Declaración de admisibilidad.—5.2. Fundamentación en principio suficiente de los recursos.—VI. FALLO.— VII. VOTOS PARTICULARES.—7.1. Voto particular del magistrado SCHLUCKEBIER.—7.2. Voto particular del magistrado EICHBERGER .—VIII. COMENTARIO.

★ Letrado de las Cortes Generales (jubilado).

[1] *Nota del Autor* (en lo sucesivo *N. del Aut.*).— Dictada en virtud de la deliberación de 15 de diciembre de 2009, la sentencia lleva, según el procedimiento del Tribunal, la fecha en que ha sido publicada oficialmente por la Secretaría del propio órgano.

I. INTRODUCCIÓN: ANTECEDENTES Y PLAN DE LA EXPOSICIÓN

1.1. Antecedentes

Los tres preceptos impugnados han sido introducidos en el ordenamiento federal en cumplimiento de la obligación de la República Federal de ALEMANIA (en lo sucesivo RFA o simplemente ALEMANIA), como de los demás Estados miembros de la UNION EUROPEA (en lo sucesivo UE), de incorporar a su ordenamiento nacional la Directiva 2006/24/CE, de 15 de marzo de 2006, del Parlamento Europeo (PE) y del Consejo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de telecomunicaciones, y por la que se modificaba otra Directiva, la 2002/58/CE, sobre la misma materia.

El texto comunitario, que invoca en un extenso preámbulo, entre otros motivos, la necesidad de disponer de información abundante y precisa sobre las comunicaciones electrónicas para combatir con más eficacia el terrorismo y la delincuencia organizada, se propone (art. 1.º) armonizar las disposiciones de los Estados miembros relativas a la obligación de los prestadores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicación de conservar determinados datos … «para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves...», e impone en consecuencia (art. 3.º) a las empresas y entidades de cada Estado miembro dedicadas a la prestación de servicios de telecomunicación electrónica de acceso general, así como a las redes públicas de telecomunicaciones, la obligación de conservar a disposición de 1as autoridades nacionales los datos «de tráfico y de localización» enumerados en su artículo 5.º sobre personas físicas y jurídicas, así como los datos conexos necesarios para identificar al abonado o usuario registrado. El apartado 2 (y último) del artículo 5.º dice, sin embargo: «De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación». Es decir, se trata estrictamente de almacenar los datos que permitan identificar a quién llama, a la persona a la que se llama, cómo, desde dónde y por qué medio concreto de telecomunicación, pero de ningún modo de indagar lo que hayan dicho uno y otro comunicante. Para el acceso de las autoridades a los datos conservados se observarán estrictamente los requisitos de necesidad y proporcionalidad. Cada Estado miembro debe designar una o varias «autoridades de control» responsables de vigilar el cumplimiento por las entidades telecomunicación de las normas que el propio Estado habrá dictado para la seguridad del almacenamiento y conservación de los datos (cosa que, por lo demás, ya habían hecho todos los miembros de la UE en cumplimiento de la Directiva originaria de 2002). Los datos se conservarán por un período mínimo de seis meses y máximo de un año a partir de la fecha de comunicación o contacto, pasado el cual serán destruidos.

En virtud, como decíamos, de la Directiva se han modificado con fecha 21 de diciembre de 2007 la Ley de Telecomunicaciones (*Telekommunikationsge-*

setz, en lo sucesivo *TKG*) mediante la inserción de los citados artículos 113*a* y 113*b* y la también citada Ley de Enjuiciamiento Criminal (*Strafprozessordnung*, en lo sucesivo *StPO*) en su artículo 100*g*, apdo. 1, y contra estos preceptos nuevos o modificados se han dirigido los tres recursos de inconstitucionalidad que el Tribunal Constitucional Federal (en lo sucesivo el TCF o simplemente el Tribunal) ha examinado y fallado conjuntamente.

1.2. Plan de la exposición

Reproducimos en primer lugar el texto de los preceptos recurridos, con una breve explicación general de su contenido; resumimos luego de modo sucesivo los recursos, la contestación del Gobierno Federal, los considerandos del Tribunal, el fallo, los dos votos particulares (por lo demás casi idénticos) y exponemos al final un breve comentario personal. Seguiremos fundamentalmente el orden de la muy extensa y detallada sentencia (47 apretadas pp. con 307 párr., más otras 8, párr. 308 a 345, que reproducen los dos votos particulares, es decir un total de 55 pp.)

II. REPRODUCCIÓN Y RESUMEN DE LOS PRECEPTOS RECURRIDOS

2.1. Artículo 113*A* de la Ley de Telecomunicaciones *(TKG)*[2]

El precepto establece la obligación de cualesquiera personas o entidades prestadoras de servicios de públicos de telecomunicación de acceso público de almacenar los datos relativos al momento en que se haya realizado cada comunicación y al lugar de origen durante seis meses y de mantener esos datos durante seis meses a disposición de las autoridades específicamente facultadas para recabarlos y examinarlos. Dice así:

«Art. 113*a*. Deberes de almacenamiento de datos

»1. Quien preste a usuarios finales servicios de telecomunicación de acceso público está obligado a conservar durante seis meses los datos de tráfico (*die Verkehrs-daten*) producidos o tratados por él con la utilización de su servicio en territorio nacional o en otro Estado miembro de la UNION EUROPEA, conforme a los apartados 2 al 5. Quien preste a usuarios finales servicios de telecomunicación de acceso al público, sin generar ni tratar por sí mismo datos de tráfico, deberá asegu-

[2] *N. del Aut.*— Titulo completo de la Ley de reforma parcial: «Ley de 21 de diciembre de 2007, sobre nueva regulación del control de telecomunicaciones y otras medidas de averiguación oculta, e incorporación de la Directiva 2006/24/CE (Boletín de Legislación Federal, Parte I. p. 3.196)» (*Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmassnahmen sowie zur Umsetzung der Richtklinie 2006/24/EWG vom 21. Dezember 2007 (Bundesgesetzblatt Teil I Seite* 3198). En lo sucesivo, al referirnos al Boletín de Legislación Federal emplearemos la sigla *BGBl.*

rarse de que los datos queden almacenados conforme al inciso primero y comunicar a la Agencia Federal de Telecomunicaciones Electrónicas (*Bundesnetzagentur*), cuando ésta se lo reclame, la identidad de quien almacene dichos datos.

«2. Los oferentes de servicios telefónicos accesibles al público almacenarán:

1. El número de teléfono u otra designación del abonado que ha hecho la llamada y del receptor de la llamada, así como, en caso de cambio en la conexión o de de conexiones sucesivas, el número de teléfono de los demás comunicantes;
2. El comienzo y el final de la comunicación según la fecha y hora correspondientes a la franja horaria (*Zeitzone*);
3. En los casos en que se puedan utilizar diversos servicios en el marco el servicio telefónico, los datos indicadores del servicio utilizado;
4. Asimismo, en los servicios de telefonía móvil:
   a) el código internacional para teléfonos móviles del enlace (*Anschluss*) de quien hace la llamada y del de quien la recibe;
   b) el código internacional de los terminales *(Endgeräte*) de llamada y de recepción;
   c) el distintivo de los puntos de acceso (*Funkzellen*) utilizados al comienzo de la comunicación por el aparato que hace la llamada y por el que la recibe;
   d) también, si se trata de servicios anónimos pagados por adelantado, la primera activación del servicio con la fecha, hora y distinto del aparato celular;
5. También, en caso de servicios telefónicos por *Internet*, la dirección de Internet (*Internetprotokoll-Adresse*) del aparato de quien hace la llamada y la del aparato receptor.

   Se aplicará por analogía lo dispuesto en el subapartado 1.º a la transmisión de mensajes cortos (*SMS*) y de mensajes multimedia (*MMS*) o análogos, debiéndose en este supuesto conservar, en vez de los datos del punto 2 de dicho subapartado, los momentos exactos de envío y de recepción del mensaje.

«3. Los oferentes de servicios de correo electrónico conservarán:

1. Por cada mensaje enviado, el distintivo del apartado de correo electrónico y la dirección de *Internet* del remitente, así como el distintivo del apartado de correo del receptor;
2. A la recepción de cada mensaje en un apartado de correo electrónico, el distintivo del apartado del remitente y el del receptor, así como la dirección de *Internet* (*Internetprotokoll-Adresse*) de la instalación de telecomunicaciones remitente;
3. Cuando localicen un apartado, su distintivo y la dirección de *Internet* del remitente;
4. Los momentos de las utilizaciones del servicio citadas en los subapartados 1 al 3, con la fecha y la hora según la franja horaria correspondiente.

«4. Los oferentes de servidores de I*nternet* conservarán:

1. La dirección de *Internet* asignada al usuario para la utilización de la red.
2. Un distintivo unívoco del aparato con el cual se haya utilizado *Internet*.
3. El comienzo y el final de la utilización de *Internet* bajo la dirección de *Internet* asignada, con indicación del día y del momento según la franja horaria correspondiente.

«5. Se conservarán igualmente en virtud del presente precepto los datos de tráfico cuando los oferentes de servicios telefónicos almacenen para las finalidades del artículo 96, apartado 2, los datos de tráfico citados en los apartados anteriores o cuando la llamada quede sin respuesta o cuando no surta efecto como consecuencia de una intervención del órgano de gestión de la red.

«6. Quien preste servicios de telecomunicación y modifique con este motivo las indicaciones de conservación obligatoria conforme al presente precepto, estará obligado a almacenar la originaria y la nueva, así como a indicar el día y el momento respectivos según la franja horaria correspondiente.

«7. Quienes exploten redes de telefonía móvil para el público, están obligados, en relación con las identificaciones de puntos de acceso almacenadas conforme a las presentes disposiciones, a conservar también los datos que permitan conocer la localización geográfica de las antenas que den servicio a los respectivos puntos de acceso y sus zonas principales de cobertura (*Hauptstrahlrichtungen*);

«8. No se podrá almacenar con base en las presentes disposiciones el contenido (*Inhalt*) de la comunicación y de los datos obtenidos consultando páginas de *Internet*.

«9. La conservación de los datos conforme a los apartados 1 al 7 se hará de tal modo que se puedan contestar inmediatamente los requerimientos de información de los órganos autorizados para ello.

«10. Los obligados por las presentes disposiciones deberán observar la diligencia requerida en el sector de las telecomunicaciones en cuanto a calidad y protección de los datos de tráfico almacenados, y se asegurarán en este punto, mediante medidas técnicas y organizativas, de que sólo las personas específicamente autorizadas tengan acceso a los datos conservados.

«11. Los obligados por los presentes preceptos deben proceder en el lapso de un mes desde de la expiración del plazo establecido en el apartado 1 a destruir, o a asegurarse de que se destruyan, los datos almacenados únicamente en virtud de dichos preceptos».

2.2. Artículo 113b de la TKG

El precepto enumera los fines para los cuales las empresas de telecomunicación pueden legalmente remitir los datos a las autoridades. Dice así:

«Las personas sujetas a las obligaciones impuestas por el artículo 113*a* podrán remitir a los órganos competentes, a requerimiento de éstos, los datos almacenados únicamente en virtud del deber de conservación establecido por dicho artículo 113*a*

1. para la persecución de hechos delictivos;
2. para la prevención de peligros graves para la seguridad pública o para
3. el cumplimiento de sus cometidos legales por los órganos de defensa de la Constitución, siempre que así esté previsto en los preceptos correspondientes en relación con el artículo 113*a* y que sea preceptiva la remisión en el caso concreto de que se trate. No podrán dichas personas remitir los datos con otra finalidad, con excepción de la información que se facilite en virtud del artículo 113[3], aplicándose por analogía lo dispuesto en el cuarto inciso del artículo. 113, apartado 1.»

2.3. Artículo 100*g* de la *StPO*

Según el apartado 4 del artículo 101 de la propia Ley de Enjuiciamiento Criminal se notificarán al interesado cualesquiera medidas que se adopten al amparo del artículo 100*g* de la *TKG* en su apartado 1, subapartado 1, y el interesado podrá, dentro de las dos semanas siguientes a la notificación, pedir revisión judicial de dichas medidas (mismo art. 101, apdo.7, segundo inciso). Se podrá, sin embargo, prescindir en ciertos casos de la notificación y aplazarla en otros (apdos. 4 y 5 respectivamente del citado artículo 101), Si se dispone el aplazamiento para un plazo largo, requerirá confirmación judicial (apdo. 4 del mismo art. 101). El precepto dice:

«1. Si existiere en virtud de determinados hechos sospecha fundada de que una persona, en calidad de autor o de cómplice,

---

[3] *N. del Aut.*— El artículo 113 TGK, titulado «Procedimiento manual de información» (*Manuelles Auskunftsverfahren*), dice:

«1. Quien explote comercialmente servicios de telecomunicación o colabore en su prestación, deberá en cada caso comunicar inmediatamente a las autoridades competentes, si se lo piden, la información relativa a los datos recogidos conforme a los artículos 95 y 116, en la medida que sea necesaria para la persecución de deditos o de faltas, la prevención de peligros para la seguridad o el orden público o el desempeño de sus funciones por las autoridades federales o estatales de defensa de la Constitución, del Servicio Federal de Inteligencia (*Bundesnachrichtendienst*) o del Servicio de Contraespionaje Militar (*Militärischer Abschirmdienst*). Las personas sujetas a la obligación establecida en el inciso primero deberá, en virtud de requerimiento al amparo del artículo 161, aptdo.1, inciso primero, o del artículo 163 de la Ley de Enjuiciamiento Criminal; de las normas de las leyes de policía de la Federación o de los Estados sobre recogida de datos, en orden a la prevención de peligros para la seguridad o el orden público; del artículo 8.º de la Ley de Defensa de la Constitución (*Bundesverfassungsgesetz*); de los preceptos equivalentes de las leyes de defensa de la Constitución de los Estados; del artículo 2.º, aptdo.1, de la Ley del Servicio Nacional de Inteligencia (*BND-Gesetz*) o del artículo 4.º, aptdo.1, de la Ley del Servicio de Contraespionaje Militar (*MAD-Gesetz)*. No se podrán transmitir dichos datos a otros órganos públicos o no públicos. Sólo se podrán recabar datos sometidos a secreto de las telecomunicaciones en las condiciones de las disposiciones legales correspondientes. El obligado a comunicar la información guardará secreto ante sus clientes sobre dicha remisión».

1. ha cometido un delito grave, incluso si se trata de un caso individual, especialmente de los tipificados en el artículo 100*a;* que ha incurrido en tentativa de dicho delito, si fuere punible la tentativa, o lo haya preparado cometiendo otro delito, o de que
2. ha cometido un delito por medio de la telecomunicación, se podrán recoger datos de comunicación sin conocimiento del interesado (art. 96, apdo. 1, y art. 113*a* de la Ley de Telecomunicaciones) en lo que fuere necesario para la averiguación de los hechos o para la determinación del lugar de donde se encuentra el culpable. En los supuestos del apartado 1, núm. 2, sólo será lícita la medida si de otro modo no es posible indagar los hechos o investigar el paradero del culpable y la obtención de los datos guarda una relación adecuada con la importancia del caso. Sólo será admisible la obtención de los datos en tiempo real en el supuesto del número 1.
2. Se aplicará por analogía lo dispuesto en el artículo 100*a*, apartado 3, y en el 100*b*, aptdo. 1 *bis*, número 4. Por excepción a lo establecido en el artículo 100*b*, apartado 23, subapartado 2, número 2, bastará en caso de hecho delictivo grave una designación espacial y cronológicamente suficiente de la comunicación, si de otro modo no fuere posible o fuese especialmente difícil, averiguar los hechos o determinar el paradero del culpable.
3. Si no se recaban los datos a los oferentes mismos del servicio de telecomunicación, la obtención se regirá por las disposiciones generales a partir del momento en que haya terminado la comunicación.
4. Se procederá, conforme al apartado 5 de artículo 100*b*, a una supervisión anual sobre las medidas que se adopten al amparo del apartado 1 del presente artículo, debiéndose hacer constar:
1. el número de procedimientos en los que se hayan adoptado medidas en el marco del apartado 1;
2. el número de órdenes dictadas para la adopción de medidas al amparo del apartado 1, con distinción entre las iniciales y las de prórroga;
3. el hecho delictivo de referencia en cada caso, con distinción entre los números 1 y 2 del apartado 1;
4. el número de meses anteriores respecto a los cuales se hayan requerido datos al amparo del apartado 1, calculándose dichos meses desde el momento de la orden de entrega de los datos, y
5. el número de medidas que no hayan dado resultado por no estar total o parcialmente disponibles los datos requeridos».

III. IDENTIDAD Y ARGUMENTOS DE LOS RECURRENTES

Como queda reflejado en el título del presente estudio, los recursos han sido tres, todos ellos presentados el año 2008, a saber:

— el *1BvR* 256/08, de siete personas naturales y una sociedad de responsabilidad limitada, representadas por un letrado colegiado en BERLIN, contra las tres disposiciones transcritas en la Sección precedente.

— el *1BvR* 263/08, de catorce personas naturales, representadas por un letrado-colegiado en DÜSSELDORF, y
— el *1BvR* 563/08, de 43 personas naturales, por conducto de un letrado colegiado en OSNABRÜCK. (Se han adherido al primero de los recursos, durante su tramitación, unas 84.000 —ochenta y cuatro mil— personas, que habían incoado otro procedimiento con el número 1*BvR* 508/08).

Señalemos desde ahora que la argumentación más extensa y pormenorizada es con gran diferencia la del propio recurso 256/08, y que los otros dos coinciden casi totalmente en lo sustancial. Nos centraremos, pues, en la exposición del primero, que podemos dividir en dos partes: a) una muy breve referida al derecho comunitario, concretamente a la varias veces citada Directiva 2006/247CE, y b) otra mucho más extensa y sustantiva, dedicada básicamente a la presunta inconstitucionalidad de los artículos. 113*a* y 113*b* de la *TKG* y 100, apartado 1, de la *StPO.*

3.1. Argumentos relativos a la Directiva 2006/24/CE (párr. 92-94)

En primer lugar el recurso es admisible a trámite (*zulässig),* al ir la ley impugnada más allá de la Directiva que pretende incorporar, pues ésta sólo autoriza para el caso de delitos graves ya cometidos o a punto de cometerse la conservación y utilización de los datos almacenados (*vide supra*, **Antecedentes**, segundo párrafo), mientras que la *TKG* añade dos supuestos no previstos en el texto comunitario, a saber, la prevención de peligros para la seguridad y el orden públicos y el cumplimiento de sus funciones por los organismos nacionales de inteligencia. Más aun, la RFA no está en rigor obligada a incorporar la Directiva en la medida en que ésta se opone al artículo 95 del Tratado de la UNION EUROPEA (no dicen los recurrentes de qué trata) y a los artículos 8.º, sobre respeto a la intimidad y del secreto de la correspondencia, y 10.º, sobre libertad de expresión, del Convenio Europeo de Derechos Humanos de 4 de noviembre de 1950[4], y en consecuencia la Directiva no puede aplicarse en ALEMANIA.

---

[4] *N. del Aut.*— El artículo 8.º del Convenio Europeo dice efectivamente: «**Derecho al respeto a la vida privada y familiar**.— 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 para la seguridad nacional, la seguridad pública, del bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

El artículo 10.º dice: «**Libertad de expresión**.— 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas, sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

3.2. Argumentos basados en la Ley Fundamental (LF) de la República Federal de Alemania (RFA)

Se afirma a continuación que además de ser «admisible», el recurso está «fundamentado» (*begründet*).

3.2.1. *Atentado al secreto de las telecomunicaciones*

El primer y principal alegato, que se repite con variantes y matices a lo largo de numerosos párrafos (95-105), es que se conculca el artículo 10, apartado 1, de la LF, que dice: «1.— Es inviolable el secreto de la correspondencia (*das Briefgeheimnis*), así como el del correo y las telecomunicaciones». Según los recurrentes, el registro de los puntos de acceso (*Funkzellen)* en cuyo ámbito topográfico se hacen las llamadas, permitiría (párr. 95) el establecimiento o elaboración de «perfiles de movimientos» casi totales y la conservación de las direcciones de *Internet* haría posible en el futuro reconstruir los procesos de intercomunicación registrados en lo seis meses presentes. En este último punto los recurrentes afirman que *Internet*, por ser un medio de comunicación de masas, queda comprendida en el apartado 1 del artículo 1.º LF. Más aun, la conservación preventiva de datos haría posible la confección de «perfiles personales» de una exactitud nunca alcanzada hasta ahora. La posibilidad de almacenamiento global de datos resulta, por lo tanto, inconstitucional en sí misma.

Se argumenta además (párr. 97) que la finalidad de garantizar una adecuada aplicación del derecho penal no puede justificar la conservación de datos, ya que la lucha contra la criminalidad organizada en redes, que es lo que se invoca en defensa de los preceptos impugnados, se dirige ante todo a la protección de valores patrimoniales o económicos, siendo así que los medios de telecomunicación se utilizan a menudo en relación con delitos de tipo convencional, que afectan a bienes jurídicos de toda clase. Los recurrentes llegan a sugerir incidentalmente (párr. 100), como fórmula alternativa de menor intensidad, el mencionado «*quick-freezing»,* por la cual las autoridades podrían ordenar en un momento dado almacenar los datos ya disponibles de una persona determinada.

Lo que antecede lleva a los recurrentes a formular otros dos reparos, jurídico el primero, de índole práctica el segundo, a saber la desproporción entre la me-

---

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad o para garantizar la autoridad y la imparcialidad del poder judicial».

dida legal y los resultados previsibles. Desde el punto de vista de los derechos fundamentales se dice (párr. 103) que con el almacenamiento de los datos sube de punto el «riesgo de verse injustamente expuesto a medidas inquisitivas o de que un inocente sea condenado», así como el peligro de «abuso de los datos». Cabría temer en efecto que los datos de las comunicaciones (*Verkehrsdaten*, es decir, datos de tráfico, en la terminología alemana) se utilicen deliberadamente contra personas «no gratas» y sirvan para controlar a personas y grupos, así como para el espionaje económico. «Sólo prescindiendo del almacenamiento de datos», concluyen los recurrentes, «puede haber protección efectiva contra el abuso». Desde una perspectiva práctica se aduce (párrs. 96 *in fine*, 96, 97 y 105) que de todos modos la conservación obligatoria de los datos es de dudosa, o en cualquier caso de poca, eficacia, entre otras razones porque de hecho gran parte de los grupos de criminalidad organizada utilizan medios de telecomunicación anónimos, como los teléfonos móviles prepago o los «cibercafés».

Se alega finalmente que la generalización del almacenamiento obligatorio de datos, al menoscabar unas relaciones de confianza esenciales para la «dignidad humana», es susceptible de coartar la espontaneidad de las telecomunicaciones y puede dar lugar al desarrollo de contramedidas (no se dice cuáles) y con él a la disminución de la masa de datos informáticos disponibles.

3.2.2. *Atentado a la libertad profesional*

Se aduce igualmente (párrs. 106-108) que los dos artículos. 113 *a* y 113*b* infringen el artículo 12, apartado 21, de la LF, el cual proclama el derecho de todos los alemanes a escoger libremente su profesión, su puesto de trabajo y su centro de formación, «…». Ambos preceptos interfieren, según los recurrentes, el libre ejercicio de su libertad profesional por los prestadores de servicios de telecomunicación y también la de quienes ejercen profesiones basadas en relaciones de confianza, más aun de confidencialidad, por ejemplo la de abogado, asesor financiero, periodista, médico personal o de cabecera, al hacer posible que unos datos de carácter íntimo caigan en manos de terceros.

Los recurrentes aducen además (párr. 107 *in fine*): «A la vista del reducido número de procedimientos en los que resulta determinante la comunicación con y por titulares de secretos profesionales, ya están garantizados los intereses de la protección de los bienes jurídicos sin que exista conservación de datos». Aquí se insinúa el argumento ya expuesto de la desproporción entre fines y medios, que luego se expone explícitamente, pero esta vez desde una perspectiva económica (párr. 108), a saber que a los prestadores de servicios de telecomunicación la obligación de conservar los datos les causa unos gastos cuya compensación o resarcimiento no se prevé en disposición alguna y que estos profesionales no tienen por qué soportar sin indemnización unos gastos que debería asumir el Estado en el ejercicio de funciones exclusivamente suyas como son la persecución de delitos y la prevención de riesgos.

3.2.3. *Atentado al derecho de propiedad*

En la medida, alegan los recurrentes (en un brevísimo párr. 109), en que los dispositivos ya utilizados de los oferentes de servicios de telecomunicación ya no pueden volver a usarse como consecuencia de la conservación obligatoria de datos, los preceptos impugnados incurren en infracción del artículo 14, apartado 1, inciso primero, de la LF, por el cual se garantizan «la propiedad y el derecho de herencia, con el contenido y las limitaciones que la ley determine». Se aduce escuetamente que, al no preverse indemnización alguna a los titulares de redes o instalaciones de telecomunicación, se infringe el derecho de propiedad.

3.2.4. *Atentado a las libertades de opinión, información y difusión radiofónica*

Según los dicentes, al causar la conservación obligatoria de datos un encarecimiento de las telecomunicaciones, resultan inevitablemente limitadas las posibilidades de los ciudadanos, empresas y organizaciones de menor capacidad económica, conculcándose así el artículo 5.º LF, apartado 1, según el cual todos «tienen derecho a expresar y difundir su opinión de palabra, por escrito y mediante la imagen y a informarse en las fuentes de acceso general» y se garantizan las libertades de prensa y de información radiofónica y cinematográfica.

3.2.5. *Atentado al principio de igualdad*

Los recurrentes invocan por último (párrs. 111-116) el artículo 3.º, apartado 1, de la LF («1.— Todos los seres humanos son iguales ante la ley»), en la medida en que no rige la obligación de almacenar datos para todo «intercambio topográfica o espacialmente inmediato de información» entre dos o más personas, sino únicamente para el «intercambio de información a través de redes de telecomunicación». En otras palabras, se incurre en discriminación contra determinados medios.

Además, sólo se exige que quede constancia del uso o utilización de ofertas de información en *Internet*, pero no la del uso de medios tradicionales como las revistas, los libros y la televisión.

En tercer lugar resulta asimismo discriminatorio que no se aplique la obligación de conservar datos al uso del ordenador personal sin fines de telecomunicación.

En cuarto término se aprecia una desigualdad de trato entre la telecomunicación como intercambio electrónico de información y el correo como «intercambio a distancia de informaciones corporeizadas».

También va contra el principio de igualdad que toda una categoría constituida por empresas más bien pequeñas se vea considerable afectada por unas cargas técnicas y económicas «sin razón suficiente».

Por último es también injustificable desde el punto de vista del citado artículo 3.º, apartado 1, que las autoridades utilicen las empresas de telecomunicación sin indemnización alguna para el ejercicio de unas funciones estrictamente públicas que, como tales, deben financiarse sólo por vía de impuesto.

Los autores del recurso *1BvR* 263/08 (apdos. 119-134) presentan alegatos análogos, si bien algo menos extensos y variados. Únicamente se aprecian diferencias de extensión y de intensidad en lo referente a la Directiva 2006/24/CE. En primer lugar los recurrentes enuncian cuatro puntos en los que la ley impugnada se excede de los límites de la Directiva, a saber la finalidad de almacenamiento de los datos, el tipo de delitos que justifican la utilización de los datos, la renuncia del legislador alemán a dictar normas precisas de procedimiento y la designación de los órganos autorizados a utilizar los datos. En segundo lugar la propia Directiva se ha dictado *ultra vires* comunitarias, por lo que no se puede aplicar en ALEMANIA, aparte de que infringe el mencionado artículo 8.º del Convenio Europeo (derecho a la intimidad). Finalmente se alega, y aquí sí hay novedad sustantiva, que si un acto jurídico de la Comunidad Europea, como sucede con la Directiva, va contra el artículo 1.º de la LF (derecho fundamental a la dignidad), es al Tribunal Constitucional Federal a quien corresponde pronunciarse, sin que proceda consulta previa al Tribunal de Justicia de las Comunidades Europeas (hoy de la Unión Europea), la cual sólo procedería en el caso de que la jurisdicción alemana no se considerase legitimada.

En cuanto a la presunta inconstitucionalidad de los preceptos impugnados, los dicentes repiten los argumentos ya expuestos sobre atentados al derecho a la intimidad y falta de proporcionalidad. Hay, bien es verdad, una aportación novedosa, que se cifra en la alegación de que el artículo113 infringe los principios de especificidad y de claridad normativa al hablar globalmente de perseguir delitos, prevenir peligros graves para la seguridad pública y desempeñar misiones de inteligencia.

Se aduce también falta de especificidad en la redacción del apartado 1 del artículo 100*g* de la Ley de Enjuiciamiento Criminal, que tampoco define los tipos de delito que justificarían la remisión forzosa de los datos almacenados.

Por último los autores del recurso *1BvR* 563/08 coinciden con los otros dos recursos en denunciar la presunta infracción del derecho a la intimidad y la falta de proporcionalidad de las medidas previstas en los artículos impugnados con los fines perseguidos. El único matiz digno de relieve en este punto es la insistencia con que se aduce el riego de exposición de las personas a sospechas infundadas y a medidas perturbadoras de investigación policial. Por lo demás se denuncia (es la única novedad) el incumplimiento de lo dispuesto en el apdo. 10 del artículo 113*a* TKG, a saber, que no se han dictado las «medidas técnicas y organizativas» para que los datos objeto de conservación obligatoria sólo sean accesibles a las «personas especialmente autorizadas», por lo cual no queda suficientemente garantizada la seguridad de los datos.

IV. CONTESTACIÓN DEL GOBIERNO FEDERAL Y POSICIÓN DE LOS ÓRGANOS PERSONADOS EN EL RECURSO

Han contestado o enviado su toma de posición el Gobierno Federal, el Tribunal Administrativo Federal, el Tribunal Supremo Federal, el Comisionado Federal para la Protección de Datos y la Libertad de Información y, en nombre de los Comisionados de los Estados (*Länder*) para la Protección de Datos, el Comisionado de BERLIN para la Protección de Datos y la Libertad de Información. Exponemos por este orden las respectivas contribuciones

4.1. Contestación del Gobierno Federal

Sigue básicamente (pero con menos extensión) el mismo método que el recurso *1BvR* 256/08.

4.1.1. *Inadmisibilidad a trámite de los tres recursos*

Se alega (párrs. 149-150) en primer lugar que es inadmisible (*unzulässig*) la impugnación de los dos preceptos sustantivos, esto es, los artículos 113*a* y 113*b* de la *TKG*, con el argumento fundamental de que no están sujetos a la jurisdicción revisora del TCF por ajustarse a las exigencias impuestas al Estado Federal por la Directiva 2006/24/CE. No hay acto jurídico ilícito desde el momento en que no se trata del reparto de competencias entre la Comunidad Europea (*sic*) y los Estados miembros, sino simplemente de un asunto de competencias «dentro de la CE». Al nivel europeo basta que exista suficiente respeto a los derechos fundamentales y, por lo demás, no se aprecia atentado alguno a la dignidad humana. Tampoco pueden los recurrentes apoyarse en la primacía del derecho comunitario, toda vez que, contrariamente a lo que ellos alegan, la Directiva en cuestión «sí permite extender la finalidad del almacenamiento de datos a la utilización de éstos para la prevención de peligros (*zur Gefahrenabwehr*) y para el cumplimiento de las misiones de inteligencia (*zur nachrichtendienstlichen Aufgabenerfüllung*), y esto es estrictamente lo que dice el apdo. 1, números 2 y 3, del artículo 113 *b*».

Niega, por lo demás, el Gobierno (párr. 150 cit.) que los dos preceptos recurridos abriguen tendencia alguna a una «regulación de profesiones», por ejemplo la abogacía o el periodismo. Ninguno de los dos artículos afecta en absoluto al artículo 14 LF invocado por los recurrentes. Tampoco cabe hablar de atentado a la libertad de expresión, ya que el almacenamiento que se dispone es «neutral en términos de opinión».

4.1.2. *Carencia de fundamento sustantivo*

Se aduce en primer lugar (párrs.154-155) que la modificación legislativa no interfiere en el ámbito de protección definido por el artículo 10.º LF (secreto

de la correspondencia, el correo y las telecomunicaciones). El artículo 113*a* prevé sólo una «intervención de intensidad media» en el ámbito de dicho precepto. Lo único que pretende, junto al siguiente, es «adaptar la lucha contra el terrorismo y la delincuencia grave a las técnicas modernas de comunicación» En este punto se afirma (párr. 156) que la «valoración de los datos… es algo irrenunciable», tanto más cuanto que la alternativa del *quick freezing* citada incidentalmente por los recurrentes no puede nunca tener la misma eficacia que la conservación prevista en la *TKG*.

En segundo lugar no hay desproporción; antes bien, el artículo 113*a* es «adecuado» a las finalidades que persigue, sin que la variedad y la generalidad de los datos lo hagan en sí mismo inconstitucional. Los datos se conservan para finalidades determinadas y el Estado sólo tiene acceso a ellos en virtud de otras normas. Por otra parte, ya existe en el ordenamiento alemán conservación obligatoria de datos, por ejemplo, en el Código de Comercio, en la Ley General Tributaria o en la de Régimen del Crédito.

En cuanto a los gastos que ocasiona la conservación de datos a los titulares de servicios de telecomunicación, no cabe alegar infracción alguna de los artículo 12 (libertad profesional) ni 14 (derecho de propiedad) de la LF (párr. 159). Respecto al segundo recuerda el Gobierno que en él no se garantiza ninguna «protección especial del patrimonio empresarial» y que el hecho de estar obligado a colaborar en el cumplimiento de un cometido oficial no da derecho por sí mismo a indemnización.

La parte recurrida recuerda (párr. 161) que ya otro artículo de la *TKG*, el 109 en su apartado. 1, obliga a los prestadores de servicios de telecomunicación a la adopción de precauciones adecuadas de orden técnico para la protección de los datos contra posibles injerencias de sus colaboradores o de terceros, y a facilitar además a la Oficina Federal de Redes de Telecomunicación un programa completo de seguridad. Todo esto aparte del control por la citada Oficina al que están todos ellos sometidos.

También el artículo 113*b* se ajusta a la Constitución, pues enumera taxativa, es decir limitativamente, las finalidades para las autoridades pueden utilizar los datos que reclamen. La utilización se rige además por otras disposiciones legislativas (no se dice cuáles) que la someten a comprobación separada. Existe asimismo la posibilidad de reservas judiciales que se deben regular en las normas de autorización para cada caso. Por otra parte, ya en algunas ocasiones el propio TCF ha declarado el control sin causa concreta del contenido mismo (y no sólo de los «datos de tráfico») de determinadas comunicaciones con fines de inteligencia.

Por último, también (párr. 163-164) el artículo 100*g StPO*, apdo. 1, es «conforme a la Constitución (*verfassungsgemäss*), desde el momento en que se remite a la lista de delitos del artículo 100.ª, apartado 2, de la propia Ley de Enjuiciamiento Criminal, y en que el precepto impugnado impone como condición necesaria para la intervención de los datos que se trate de un delito grave, requisitos estos que el TFC «ha reconocido como suficientemente precisos» (no se dice cuándo).

4.2. Posición del Tribunal Administrativo Federal (*Bundesverwaltungshof*)

Es dudosa la constitucionalidad de los preceptos impugnados por lo que suponen de injerencia en el secreto de la correspondencia, el correo y las telecomunicaciones (art. 10, apdo. 1, LF, como se recordará).Así, los fines enunciados en el artículo 113b como justificativos de la intervención gubernamental «están formulados con tal amplitud que resulta imposible prever en el momento del almacenamiento con qué fin se pueden utilizar los datos» (párr. 165). Esto hace posible la construcción de todo un perfil del usuario no sólo en lo personal, sino también de su ambiente social y de sus movimientos en general y, en el supuesto de procedimientos penales podría tener consecuencias graves para aquél, aparte de la posibilidad del abuso de los datos.

4.3. Posición del Tribunal Supremo Federal (*Bundesgerichtshof*)

Se empieza recordando (párr. 166) que la práctica habitual hasta el momento presente, cuando se trataba de delitos cometidos mediante la telecomunicación, ha sido destruir en el momento mismo de reclamarse la información los datos que hubieran permitido la identificación del autor. En el caso concreto de *Internet* queda excluida, según el TSF, toda posibilidad de rastrear el contenido de la comunicación. Por otra parte, considerando el gran uso que se hace de contratos de tarifa plana, se mantiene a menudo conectada durante las veinticuatro horas del día la referencia de los datos. En este caso lo normal es que ya no se pueda extraer de los datos almacenados información sobre la frecuencia y la duración del uso de *Internet.* En el sector del correo electrónico (*E-mail*) es en cambio imprescindible la conservación de las direcciones de *Internet*, pues sin ella no sería posible, por ejemplo, perseguir delitos económicos ni la pornografía infantil, Más aun, concluye el TSF, sin conservación preventiva de los datos «en *Internet* no hay prácticamente riesgo para los delincuentes de ser descubiertos». Surgiría así «un espacio sin derecho» (*ein rechtsfreier Raum*). Bien es verdad que el Presidente del TSF concluye formulando una reserva, a saber que los «datos de tráfico» sólo tienen valor de indicios y tienen por tanto que apoyarse en investigaciones de otra índole.

4.4. Posición del Comisionado Federal para la Protección de Datos y la Libertad de Información

Como cabía esperar, este órgano califica de anticonstitucionales los tres preceptos impugnados (párrs. 167-170), por tres razones:

— Primera, no está bien definido en el artículo 100*g StPO* el «umbral» de utilización de los datos por la autoridad; en otras palabras no se dice con precisión a partir de qué nivel de gravedad o de importancia está justifi-

cado el uso de los datos por la autoridad, con lo cual se infringen además los artículos 8.º (derecho al respeto de la vida privada) y 10.º (libertad de expresión) del Convenio Europeo de Derechos Humanos.

— Segunda, la conservación de datos invade la intimidad de los usuarios o comunicantes, menoscabando así la confianza del público en los medios de telecomunicación y abriendo la puerta a posibles abusos (argumento que, como se recordará, aducían los recurrentes).

— Tercera, definición insuficiente, por imprecisa, de los hechos delictivos que podrían justificar la reclamación de los datos con vistas a un proceso penal; indefinición asimismo de los casos o circunstancias en que la autoridad podría prescindir de la correspondiente notificación al titular de los datos; insuficiente previsión del requisito de revisión judicial en el caso de que no se haya cursado dicha notificación y peligro, finalmente, de que por el juego combinado de los dos artículos 113 *a* y 113*b* con el 113 *TKG* se puedan perseguir también simples faltas.

4.5. Posición del Comisionado de BERLIN para Protección de Datos y Libertad de Información

Coincide (párr. 171) con la calificación de inconstitucionalidad formulada por el Comisionado Federal, con el matiz de que se invocan preceptos y fundamentos no siempre coincidentes. Así, por ejemplo, hace hincapié en la violación del secreto de las telecomunicaciones, advierte del peligro de abusos de los datos por personas privadas y critica que no se hayan tenido en cuenta alternativas de menor intensidad como la del «*quick freezing*».

V. CONSIDERANDOS

Se examinan y enjuician conjuntamente los tres recursos.

5.1. Declaración de admisibilidad

Interés personal de todos y cada uno de los recurrentes (párr. 175-179). Todos ellos acreditan en efecto que están o podrían quedar afectados directamente por la aplicación de los preceptos impugnados.

Competencia del TCF en el presente caso para enjuiciar la constitucionalidad de leyes dictadas en virtud de una Directiva europea (párr. 181-183). Se reconoce que en principio el Tribunal no es competente para pronunciarse sobre la aplicabilidad de normas de derecho comunitario que se invoquen como fundamento para determinada línea de acción o comportamiento para los tribunales y autoridades alemanes y que el Tribunal no puede, por tanto, exami-

nar dichas normas con el patrón de los derechos humanos garantizados por la LF alemana, siempre que la UNION EUROPEA (en particular su Tribunal Europeo) garantice una protección efectiva de los derechos fundamentales en términos equiparables a los niveles irrenunciables de la LF. Estos principios rigen asimismo para las disposiciones del ordenamiento nacional que traspongan o incorporen derecho comunitario, por lo que es básicamente inadmisible todo recurso de inconstitucionalidad dirigido contra derecho vinculante de la UNION EUROPEA.

Ahora bien, los recurrentes en el presente caso sí pueden invocar los derechos definidos como fundamentales por la LF alemana «en tanto en cuanto el legislador tenga margen de maniobra al incorporar el derecho de la UNION (*bei der Umsetzung von Unionsrecht*), es decir que no esté vinculado por el derecho de la UNION». Precisamente se dan los dos requisitos: afectación, por una parte, de derechos fundamentales en el orden constitucional alemán y concesión, por otro, de un «espacio discrecional de decisión» *(Entscheidungsspielraum*, párr. 186) a los Estados miembros destinatarios de la Directiva.

5.2. Fundamentación en principio suficiente de los recursos

En lo que es lógica y obligadamente la parte más extensa de la sentencia (párrs. 183-184 y 188-04), se analizan los argumentos de fondo, es decir, la presunta violación de derechos alegada por los recurrentes a la luz de los artículos que ellos mismos invocan de la LF. Cabe extraer las siguientes afirmaciones principales:

1. Las restricciones al secreto de las telecomunicaciones previstas en el artículo 113*a* TKG son en principio «constitucionalmente irreprochables» (*verfassungsrechtlich undedenklich*) en la medida en que ya el apartado. 2 del citado artículo 10.º LF prevé expresamente la posibilidad de limitar por ley el secreto de las telecomunicaciones (párr.198).
2. No es inconstitucional, en principio, la obligación genérica de conservar los «datos de tráfico» (no el contenido) de las comunicaciones durante seis meses para «utilizaciones específicas en el marco de la persecución de delitos, la prevención de peligros y los cometidos de los servicios de inteligencia» (párr. 205); es decir no hace falta demostrar necesidad de motivo concreto en cada caso.
3. Ahora bien, el principio de proporcionalidad entre medios y fines impone el respeto efectivo de cuatro criterios (párr. 220): la seguridad de los datos, la definición del alcance y ámbito de su utilización, la transparencia (notificación al titular de los datos, cuando sea posible, y posibilidad de supervisión por la autoridad competente en materia de protección de datos) y la protección de los derechos de los comunicantes mediante intervención judicial.

4. Corresponde al legislador federal (art. 73, apdo. 1, núm. 7 LF) garantizar la seguridad de los datos, así como fijar con claridad unos límites a las posibles finalidades de la utilización de los datos. Se rigen, en cambio, por la distribución de competencias legislativas entre la Federación y cada uno de los Estados el modo y procedimiento de reclamación de los datos por la autoridad competente y la elaboración de las normas aplicables en materia de transparencia y de protección de derechos. Por lo tanto, es procedente que el recurso vaya específicamente dirigido contra la *TKG* como tal ley federal (señalemos que hasta cierto punto éste sería más bien un argumento previo de admisibilidad que de fondo).
5. El artículo 113*a TKG* no ofrece los «niveles especialmente altos de seguridad» de todo punto exigibles tratándose de la conservación obligatoria de un gran número de indicadores susceptible de proporcionar información sobre la personalidad, el modo de vida y el ambiente social de los titulares. Se aprecia en particular (párr. 224 *in fine*) la falta de separación entre los diversos datos, de un encriptado riguroso, de un régimen de garantías para la petición de los datos mediante la utilización, por ejemplo, del principio de confidencialidad o «puerta cerrada»(*Vier-Augen-Prinzip*) y de una constancia formal que garantice la comprobación de los requerimientos y de la destrucción final de los datos. En definitiva no se han dictado normas claras y vinculantes de seguridad y falta, por fin, un sistema equilibrado de sanciones para los casos, por un lado, de contravención a la seguridad de los datos y, por otro, de simple incumplimiento de normas de conservación (párr. 275), o sea más bien lo contrario del sistema establecido, que castiga más duramente lo segundo que lo primero.
6. El artículo 113*b TKG* y también el 100*g*, apdo.1 *StPO* infringen frontalmente el principio de proporcionalidad al no definir con un mínimo de rigor y precisión los tres supuestos legítimos de reclamación y subsiguiente utilización de los datos, a saber, persecución de delitos, prevención de peligros y actuación de los servicios de inteligencia. En cuanto al primero, la reclamación sólo puede justificarse para delitos graves, y en este punto el legislador puede optar (párr.228) entre el «catálogo existente» de hechos delictivos o la elaboración de una lista de delitos especialmente significativos en el plano de los datos «de tráfico», sin que sea suficiente una «cláusula general» o la simple referencia a «delitos de especial significación».

   El mismo reproche es aplicable a la prevención, formulada muy genéricamente, de riesgos o peligros (párrs. 230 y 285), con la reserva de que no parece aconsejable en buena técnica legislativa tomar como referencia una lista de determinados delitos que se trataría de prevenir, sino que es preferible describir en la propia ley los bienes jurídicos cuya protección se pretende con el uso de los datos, así como definir el grado de peligro para esos bienes a partir del cual se justificaría el re-

querimiento (se citan tres grandes categorías: peligro para la integridad física, la vida o la libertad de la persona, peligro para la existencia o la seguridad de la Federación o de uno de sus Estados y «peligro para la colectividad» y tres criterios de medida: caso individual, proximidad en el tiempo de que el peligro aboque a un daño y posibilidad de identificar a determinada persona como presunto causante).

Otro tanto puede decirse hasta cierto punto de los servicios de inteligencia (párrs. 230-234 y 285). No sólo no se fija un «umbral», es decir un nivel mínimo de gravedad o importancia para la reclamación de datos, sino que tampoco se especifica el destino que se les pueden dar lícitamente; todo esto parece dejarse a una regulación legislativa posterior, en particular a la actividad legislativa de los Estados. Se apunta a mayor abundamiento (párr. 285 cit.) el peligro de que con la redacción actual del artículo 113 *b* los proveedores de servicios de telecomunicación se vean obligados a constituir un verdadero «fondo de datos» (*Datenpool*) expuesto a toda clase de usos por la policía y por los servicios de inteligencia;

7. Tampoco se garantiza que los datos reclamados se utilicen inmediatamente y se destruyan acto seguido (párr. 235).
8. No se cumple suficientemente el imperativo de transparencia en el requerimiento de datos para su uso, en la medida en que el artículo 100*g*, apdo. 1 *StPO* admite la posibilidad de recabarlos sin notificación al titular (párr. 280). El Tribunal recuerda que «los imperativos constitucionales de transparencia sólo permiten la obtención en secreto de los datos almacenados al amparo del artículo 113*a TKG* cuando resulte necesaria por razones superiores que deberán especificarse por ley y así se ordene judicialmente». Se reconoce ciertamente a continuación (párr. 281) que el artículo 101 (apdos. 1,4 y 5) de la propia *StPO*, de conformidad en este punto con la jurisprudencia del TCF, prevé regulaciones especiales para casos en los que estaría justificada la notificación *a posteriori*, pero se formulan dos reparos: primero, que hay que tener en cuenta los intereses de personas posiblemente implicadas de modo indirecto, y segundo (párr. 281) que no se regula suficientemente el control judicial en los supuestos en que quepa prescindir de la notificación, toda vez que sólo se prevé esta clase de control para la notificación pospuesta o retrasada, pero no para la ausencia de notificación.
9. Si bien queda garantizado en principio el control por los tribunales de la reclamación y del uso subsiguiente de datos (y aun así se apuntan reservas sobre la eficacia del control *a posteriori*), no se especifican con claridad los requisitos formales del auto judicial (párr. 284). Sólo se exigen unas indicaciones mínimas sobre identificación informática de los interesados (aparte del requisito genérico de razonar la decisión). Se recomienda una nueva regulación legislativa que imponga una motivación más sustanciada a las decisiones judiciales.

10. Se infringe asimismo el principio de proporcionalidad entre medios y fines en la medida en que no se prevé protección alguna de las «relaciones confidenciales» (*Vertrauensbeziehungen*) en el caso de remisión de los datos respectivos a las autoridades (párr. 287). El Tribunal entiende que es obligado garantizar esta protección «al menos para un núcleo íntimo de contactos a distancia sujetos a una especial confidencialidad».
11. No hay violación, por el contrario, de la libertad de empresa garantizada por el artículo 121, apartado.1, LF, contra lo que alega una sociedad de responsabilidad limitada que figura entre los firmantes del recurso *1BvR* 256/08 (párr. 293-298). Es verdad, se añade (párr. 295), que, al explotar comercialmente dicha sociedad unos servidores con anonimato garantizado (*Anonymiesierungsserver*) para el público en general, la imposición de un deber de almacenamiento de datos implica, por definición, cierto grado de injerencia del legislador en el libre ejercicio de una actividad profesional, pero no es menos cierto que en este caso el deber de conservación «no aboca a que ya no se puedan ofrecer en principio servicios de comunicaciones con ocultación de identidad» (*Anonymisierungsdienste*), toda vez que éstos «pueden seguir ofreciendo a sus usuarios el navegar por *Internet* sin posibilidad para los particulares de identificar su dirección de *Internet*». El anonimato se deshace únicamente frente a las autoridades estatales y sólo cuando esté excepcionalmente autorizada la intervención de los datos según los estrictos requisitos para la utilización inmediata de datos conservados conforme al artículo 113*a*. Por lo demás, la intervención no ocasiona costes excesivos por razones técnicos ni cargas financieras desproporcionadas.
12. La obligación de conservar datos no impone tampoco a los prestadores de servicios de telecomunicación en general costes desproporcionados de origen técnico (párr. 300-301).
13. Más aun, es perfectamente constitucional que las empresas deban soportar en principio el coste derivado de la obligación de conservar los datos, pues pueden, como tales empresas privadas, repercutirlo libremente en sus precios o, dicho con más precisión, incluirlo en el precio como un componente más de sus costes (párr. 302-304). Sólo en el supuesto, que no se aprecia y que, por lo demás, no se ha alegado con apoyo de pruebas concretas, de que el almacenamiento ocasionara costes desproporcionados a un grupo significativo de empresas (y no sólo a alguna en particular), cabría hablar de violación el principio de proporcionalidad.
14. No se aprecia finalmente violación alguna de los demás derechos fundamentales invocados por los recurrentes (derecho a la dignidad, derecho a la igualdad y derecho de propiedad), pronunciamiento éste que es el más breve de la sentencia (párr. 305, que no llega dos renglones), por ser el único que se formula sin examen alguno de las alegaciones.

VI. FALLO

Por mayoría de seis votos contra dos, el TCF ha dictado la siguiente sentencia (*Urteil*):

> «1. Infringen el artículo 10.º, apartado 1, de la Ley Fundamental y se declaran nulos *(nichtig)* los artículos 113*a* y 113*b* de la Ley de Telecomunicaciones, texto modificado por el artículo 2.º, número 6, de la Ley por la que se da nueva regulación a la vigilancia de las telecomunicaciones (*Telekommunikationsüberwachung*) y a otras medidas ocultas de prueba, y se incorpora la Directiva 2006/24/CE de 21 de diciembre de 2007 (Boletín de Legislación Federal - *Bundesgesetzblatt*, abreviadamente *BGBl.*- I, p. 3.198).
> «2. Infringe el artículo 10.º, apartado 1, de la Ley Fundamental y se declara nulo el artículo 100*g,* apdo.1, de la Ley de Enjuiciamiento Criminal, texto modificado por el artículo 1.º, núm. 11, de la Ley por la que se da nueva regulación a la vigilancia de las telecomunicaciones y a otras medidas ocultas de prueba, y se incorpora la Directiva 2006/24/CE de 21 de diciembre de 2007 (*BGBl.* I, p. 3.198), en la medida en la que se pueden recabar datos de trafico según el artículo 113*a* de la Ley de Telecomunicaciones.
> 3. ... (Se ordena la inmediata destrucción de los datos recogidos por las empresas de telecomunicaciones por requerimiento de las autoridades al amparo de sucesivos autos provisionales a partir del 11 del auto provisional de marzo de 2008 sobre el citado recurso *1BvR* 256/08, pero no entregados aún a dichas autoridades).
> 4. La República Federal de ALEMANIA resarcirá a los recurrentes las costas judiciales que hayan sido consecuencia necesaria del procedimiento».

VII. VOTOS PARTICULARES

Han sido dos (*abweichende Meinungen*), firmados por los jueces SCHLUCKEBIER y EICHBERGER (párr. 310-336 y 337-345 respectivamente), el segundo de los cuales empieza, por cierto, declarando que se adhiere «básicamente» (*grundsätzlich*) a lo dicho por el primero y anuncia que se limitará, en consecuencia, a un breve resumen de su propia posición.

Exponemos abreviadamente a continuación, y por el mismo orden, estos dos votos particulares.

7.1. Voto particular del magistrado SCHLUCKEBIER

Podemos resumirlo en los términos siguientes:

1. La conservación o almacenamiento obligatorio de datos de tráfico (*Verkehrsdaten*) por un período de seis meses no constituye una inje-

rencia en el derecho fundamental del artículo 10.º.1 LF (secreto, como se recordará, de la correspondencia, el correo y las telecomunicaciones) de tal magnitud que se pueda clasificar como «especialmente grave» y equivalente como tal a una interferencia directa del Estado en el contenido de las comunicaciones. La realidad es que los datos de tráfico permanecen en el ámbito de los proveedores privados, en cuyos servidores quedan registrados por razones técnicas, pero de quienes todo usuario individual puede razonablemente esperar, por su relación contractual con ellos, que esos datos se protegerán y tratarán de modo estrictamente confidencial. Con tal que se garantice un nivel de seguridad técnicamente actualizado, no hay por lo tanto razón objetiva para suponer que el ciudadano pueda sentirse intimidado como consecuencia del almacenamiento, tanto más cuanto que éste no es extensivo al contenido de las telecomunicaciones.

2. Es meridianamente menos intensa, menos invasora, la obligación citada de conservar de datos de telecomunicación que otras injerencias especialmente acusadas como la vigilancia acústica en las viviendas, el seguimiento del contenido de mensajes o comunicaciones o en lo que se conoce como busca «*on line*» en los sistemas IT (Información y Telecomunicación) mediante el acceso directo de organismos estatales. En estos casos sí existe un gran riesgo de injerencia o intromisión en la zona íntima de la vida privada, que goza en principio de protección absoluta. datos.
3. Los preceptos impugnados no son fundamentalmente inadecuados; por el contrario son razonables para las personas afectadas y proporcionados, por consiguiente, en el sentido estricto de la palabra. Al establecer por ley la obligación de conservar durante seis meses los datos de tráfico y al prever su recogida y subsiguiente utilización para posibles procedimientos penales, el Poder Legislativo se ha mantenido dentro de sus límites constitucionales.
4. El deber del Estado de proteger a sus ciudadanos incluye el de adoptar las medidas adecuadas para prevenir daños a intereses legítimos, el de investigar esos daños cuando se hayan ocasionado y el de declarar las responsabilidades resultantes. En consecuencia, la protección de los ciudadanos y de sus derechos fundamentales y de las bases de la vida en común, así como la prevención e investigación de los delitos graves, forman parte de los presupuestos de toda coexistencia pacífica y para el goce tranquilo por los ciudadanos de sus derechos fundamentales. La investigación eficaz de los crímenes y la prevención efectiva de los peligros no constituyen, por tanto, en sí mismas una amenaza a la libertad del ciudadano.
5. En el conflicto entre el deber del Estado de tutelar los intereses de la ley y el interés de los individuos en la salvaguardia de sus derechos constitucionales, el Poder Legislativo debe, al menos inicialmente, adoptar un planteamiento abstracto y conseguir un equilibrio entre intereses

hasta cierto punto contrapuestos, para lo cual tiene que disponer de cierto margen de apreciación y de formulación. El Parlamento tenía inexcusablemente que tener en cuenta las necesidades inexcusables de una administración de la justicia penal eficaz y al mismo tiempo ajustada a la Constitución, a la luz de unos cambios esenciales en las posibilidades de comunicación y de los comportamientos sociales en materia de comunicación en los últimos años, una exigencia que no se puede conseguir si no hay medios de comprobar los hechos necesarios para la investigación.

6. El Poder Legislativo ha dado ante todo por sentado que los datos de telecomunicaciones, por la continua evolución de éstas hacia la generalización de las conexiones de tarifa plana, o bien no se conservan en absoluto o bien se destruyen antes de que llegue a dictarse auto judicial para la recogida de datos, incluso antes de que las autoridades dispongan de la información necesaria para requerirlos. Por su parte, la mayoría de los componentes de la Sala ha reconocido que prácticamente todos los ámbitos de la vida en sociedad están invadidos por medios electrónicos o digitales de comunicación y que esto entorpece en determinados sectores la persecución de los delitos, así como la prevención de riesgos, pero al sopesar luego la proporcionalidad en el sentido estricto del término, esos mismos magistrados no han concedido suficiente significación a estos dos imperativos con los criterios de adecuación y de proporción razonable.
7. A pesar de que la ley modificadora de la *TKG* se ha aprobado por una amplia mayoría después de examinar el Poder Legislativo diversos dictámenes de índole técnica y de haber escuchado a numerosos expertos independientes, y de que incluso se ha procurado incorporar la jurisprudencia elaborada hasta entonces por el TCF, la mayoría de la Sala Primera viene virtualmente a restringir de modo casi completo el margen de apreciación y de redacción que el Parlamento necesita para aprobar disposiciones adecuadas y razonables en orden a la investigación de delitos graves y a la prevención de riesgos para la población.
8. La sentencia tampoco toma suficientemente en consideración el imperativo de auto-moderación judicial en relación con las decisiones del Parlamento democráticamente. Proclama en efecto que el período legal de seis meses de conservación (el mismo que establece la Directiva comunitaria) constituye el límite máximo y es apenas digno de considerarse constitucionalmente justificado; «dicta» al Poder Legislativo como norma técnica que el precepto sobre finalidad del uso de los datos incluya también los requisitos de acceso; le constriñe a adoptar una técnica estrictamente penal para la catalogación de hechos perseguibles; excluye la posibilidad de utilizar los datos incluso para investigar delitos de difícil indagación cometidos por medios informáticos, y amplía el deber de notificación y los requisitos mínimos de protección de los derechos. Así, pues, el Poder Legislativo se ve reducido a adaptar y modificar sólo marginalmente el

catálogo de figuras penales que justifiquen la recogida de datos; en otras palabras (párr. 327 *in fine*) tiene que trasponer la sentencia si no quiere prescindir de dictar una nueva ordenación, lo cual constituiría infracción del derecho comunitario, y una virtual suplantación de la función legislativa por la propia sentencia.

9. En un plano más concreto la Sala niega al Poder Legislativo el derecho a implantar la recogida de los datos de tráfico almacenados en virtud del artículo 113*a TKG* con el fin de investigar delitos que, aun no figurando en la lista vigente del artículo 100*a*, apartado 2, *StPO*, revisten considerable importancia en casos individuales, o bien delitos cometidos por medios electrónicos o informáticos (art. 100*g*, inciso primero. núms.1 y 2, *StPO*). Respecto al primer grupo, resulta, según el Magistrado SCHLUCKEBIER, que el legislador se ha orientado precisamente por criterios que la propia Sala ha aprobado en época aún reciente, concretamente una sentencia de 12 de marzo de 2003, a saber que se trate, por un lado, de delitos definidos normalmente como importantes por la ley y, por otro, que el delito revista en un caso determinado significación especial en vista del daño causado o del riesgo para la comunidad. No se entiende por qué este patrón no pueda aplicarse en principio a la recogida de datos de tráfico almacenados, a condición naturalmente de que la recogida se autorice por auto judicial. En cuanto a la segunda categoría, no se ha tenido suficientemente en cuenta que aquí el Poder Legislativo parte de considerables dificultadas iniciales de esclarecimiento del delito. Parece justificada la recogida de los datos por las autoridades como medida de investigación, tanto más cuanto el legislador ha añadido una «cláusula de subsidiariedad (párr. 331) según la cual la recogida sólo puede decretarse si no existe posibilidad razonable de aclaración de los hechos o de localización de su autor y si la obtención de los datos guarda una proporción adecuada con la entidad del asunto (art. 100*g,* apdo.1, inciso segundo, *StPO*).
10. Finalmente, la Sala habría podido, basándose también para ello en su propia jurisprudencia, fijar plazo al Parlamento para aprobar una nueva legislación y decretar que mientras tanto siguiesen provisionalmente en vigor las disposiciones recurridas, con sujeción, eso sí, a las instrucciones temporales emanadas de la propia Sala. Esto habría sido perfectamente posible, por cuanto la misma sentencia reconoce como correcta la norma legislativa de conservación de los datos por seis meses, durante los cuales el legislador elaboraría normas concretas de intervención de conformidad con esas instrucciones.

7.2. Voto particular del magistrado EICHBERGER

Como hemos adelantado, sigue en lo fundamental el razonamiento de su colega SCHLUCKEBIER. Empieza calificando de «infundado y en cualquier

caso empíricamente no probado» el temor expresado por la mayoría de la Sala de que los preceptos impugnados produzcan un efecto inhibidor en el público, disuadiéndole de utilizar los medios de telecomunicación. Más adelante estima que la concepción de «responsabilidad legislativa escalonada» (*gestufte gesetzgeberische Verantwortung*) subyacente a esos preceptos «es conforme a la Constitución», especialmente en lo que se refiere a la utilización de los datos almacenados en virtud del artículo 113*a TKG*, que se rige por el artículo 100*g StPO*, para fines de enjuiciamiento criminal. El Poder Legislativo no tiene obligación de medir la proporcionalidad de las disposiciones sobre recogida de datos tomando como único patrón el grado máximo posible de interferencia, es decir, una recogida global presuntamente encaminada a crear un «perfil social» del ciudadano o a rastrear todos sus movimientos; antes bien, le es lícito tomar en consideración el hecho de que numerosos ejemplos de recuperación de datos tienen mucha menos trascendencia, y que es en definitiva el juez competente quien debe decidir en cada caso si la obtención de los datos se ha efectuado o no de modo razonable y proporcionado.

VIII. COMENTARIO

Nos inclinamos básicamente a favor de los dos votos particulares, haciendo nuestra en primer lugar la afirmación citada del magistrado EICHBERGER de que no se ha probado que la población vaya a sentirse intimidada y a retraerse, por lo tanto, del uso de los medios de telecomunicación por razón de los preceptos legales impugnados.

En segundo lugar estimamos convincente el argumento comparativo desarrollado por el magistrado SCHLUCKEBIER, es decir el cotejo entre el fallo que comentamos y la doctrina sentada por el propio TFC en sentencias anteriores sobre revelación de datos de tráfico a las autoridades que los requieran (por cierto, habría que preguntarse, ya que la sentencia también invoca en algunos de sus considerandos fallos anteriores del Tribunal, por qué no ha tenido también cuenta la de 12 de marzo de 2003). Si los criterios para la recogida de datos se consideraban constitucionalmente correctos en 2003, no resuelta claro por qué esos mismos criterios son anticonstitucionales o, al menos, no totalmente constitucionales en 2008, siendo así que en este punto las disposiciones impugnadas no suponen cambio sustancial respecto a la legislación anterior.

En tercer término no nos parece adecuada la fórmula que propone el Tribunal en sus considerandos 230 7 285 de tomar como referencia no tanto los delitos como los bienes jurídicos protegibles, por cuanto la segunda noción, cuyo valor nadie niega en el plano de loa principios, es forzosamente menos precisa que una lista, por imperfecta que sea, de delitos que en todos los ordenamientos se califican como graves y que se basan por definición en el imperativo de defensa de algún bien jurídico en particular. Así, por ejemplo, la vida como bien jurídico supremo se tutela mediante la definición y condena del homicidio, del asesinato, etc.; la propiedad, mediante la definición y condena

del hurto, del robo, etc. Naturalmente, no pretendemos con esto negar de raíz la validez del criterio alternativo apuntado, al menos en casos concretos, pero sí afirmamos que el sistema vigente de catálogo de hechos delictivos (*Straftaten*) de la legislación federal alemana (especialmente en la propia StPO) y que, por cierto, no se ha declarado inconstitucional, es más seguro y efectivo.

Sí nos parecería adecuado, por el contrario, incluir en la *TKG*, como insinúa la sentencia en su párrafo 224 (*vide supra*, **V**, B,5), las mejoras técnicas de conservación de datos que dicho párrafo enumera, o al menos, que el legislador, de no estimar procedente incluirlas directamente en la ley, dispusiera su adopción preceptiva por vía reglamentaria, ya a cargo de la Federación, ya a cargo de los Estados. Pero que no se haya hecho así no nos parece suficiente motivo para tachar de inconstitucionales y declarar nulos los preceptos recurridos.

Se podría asimismo mejorar, como sugiere el párrafo 281 (*vide supra*, **V,** B,8) el sistema de notificación a los interesados del requerimiento de datos por la autoridad competente, especialmente a los afectados de modo indirecto. Pero también es aplicable aquí nuestra observación al punto precedente, a saber, que no se trata de una cuestión fundamental que entrañe en sí misma vicio de inconstitucionalidad.

Creemos en consecuencia que, influido quizá subconscientemente por un clima de temor difuso en la República Federal de ALEMANIA a la interferencia de los poderes públicos en la vida privada de los ciudadanos, el TCF ha incurrido, permítasenos la expresión, en un acceso de puritanismo constitucional, más aun de fundamentalismo garantista, que le ha llevado a ver peligros cercanos y directos donde en rigor sólo los hay remotos y eventuales. Sin ánimo de enfoques ni planteamientos políticos retrospectivos, terminemos diciendo que la sentencia no es de extrañar si recordamos el espionaje diario de su vida privada mediante escuchas telefónicas y micrófonos ocultos en su propia vivienda, que sufrieron muchos ciudadanos de la extinta República Democrática Alemana, prácticas tan vívidamente descritas en la película «La vida de los otros» (*Das Leben der anderen*).