UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO CONSTITUCIONAL

TESIS DOCTORAL

The European Directive on Electronic Communications Data Retention and its Implementation in Spain

La Directiva europea sobre conservación de datos de las comunicaciones electrónicas y su trasposición en el Derecho español

Tesis doctoral elaborada por:
Luis Fernando Rodríguez García
Licenciado en Derecho

Directora: Prfa. Dra. Dª. María Yolanda Gómez Sánchez
Catedrática de Derecho Constitucional. UNED
Catedrática Jean Monnet, *ad personam*

MADRID, 2013

TESIS DOCTORAL

The European Directive on Electronic Communications Data Retention and its Implementation in Spain

La Directiva europea sobre conservación de datos de las comunicaciones electrónicas y su trasposición en el Derecho español

Directora: Prfa. Dra. Dª. María Yolanda Gómez Sánchez
Catedrática de Derecho Constitucional. UNED
Catedrática Jean Monnet, *ad personam*

Tesis doctoral elaborada por:
Luis Fernando Rodríguez García
Licenciado en Derecho

Universidad Nacional de Educación a Distancia

Facultad de Derecho

Departamento de Derecho Constitucional

Madrid, 2013

Indice general

Table of Contents

INTRODUCCIÓN

Novedad de la problemática a estudiar

La presente Tesis introduce por primera vez ante la doctrina española un examen crítico de las normativas europea y española sobre conservación de datos de las comunicaciones electrónicas, así como su impacto en los derechos fundamentales reconocidos por el ordenamiento comunitario y la Constitución Española, respectivamente.

Desde hace aproximadamente un lustro, las datos externos de las comunicaciones electrónicas —esto es, prácticamente toda aquella información distinta del contenido— de los más de quinientos millones de ciudadanos europeos han pasado a conservarse en las bases de datos de las empresas proveedoras de tales servicios por un período que puede oscilar entre los seis y los veinticuatro meses, dependiendo de la ley nacional. De acuerdo con la normativa en vigor, cualquier autoridad pública autorizada por la ley nacional puede tener acceso a cualquiera de estos datos con el fin de investigar, detectar o enjuiciar un delito grave: quién llamó a quién, cuándo, desde qué modelo de teléfono, cuánto tiempo duró la conversación o dónde estaban geográficamente localizados emisor y receptor. Datos análogos pueden obtenerse de las comunicaciones a través de internet.

Como veremos, los principales problemas jurídicos que la DCD plantea se concentran en torno a dos aspectos. El primero es de carácter formal, y se refiere a la legalidad de la base jurídica de la norma. Resulta discutible que la Comisión, al tiempo de aprobar la DCD, pudiera usar una medida del Primer Pilar para regular una materia que cae mayormente en el ámbito del Tercer Pilar. La segunda gran controversia se refiere a la legalidad material de la DCD, concretamente, a su respeto por los derechos fundamentales reconocidos por la Unión. Entre un aspecto y el otro, numerosos defectos y precariedades jalonan la directiva en vigor.

Por su parte, en España, la Ley 25/2007, de 18 de octubre, fue la encargada de incorporar en nuestro ordenamiento las disposiciones de la DCD, incluyendo además

una disposición adicional en virtud de la cual se crea un régimen de los servicios de telefonía mediante tarjetas prepago que no está previsto en la norma europea.

Como se echa de ver, la regulación sobre conservación de datos de las comunicaciones electrónicas se integra simultáneamente en tres sectores del ordenamiento: el Derecho administrativo —en tanto que se enmarca y modifica el régimen administrativo de las telecomunicaciones en España y en la Unión Europa—; el Derecho procesal penal —dado que las medidas previstas están llamadas a surtir efectos en el proceso penal como un medio de investigación y prueba—; y finalmente, en el Derecho constitucional —en tanto que sus medidas suponen una limitación de derechos fundamentales—.

Bibliografía y metodología

Esta complejidad legal quizás explica el por qué son tan escasos y parciales los estudios sobre la normativa de conservación de datos disponibles, no sólo en español sino también en lengua inglesa. De hecho, no existe en nuestra literatura jurídica ninguna monografía sobre esta materia. Estudios menores pueden encontrarse en artículos y capítulos de libros sobre Derecho procesal penal, y alguno en revistas jurídicas de otras ramas. Entre los autores españoles, hemos de destacar los excelentes trabajos de los procesalistas J. J. GONZÁLEZ LÓPEZ y J. L. RODRÍGUEZ LAINZ, que han examinado la normativa desde la rama del Derecho que les es propia[1]. Aunque hemos intentado citar el mayor número posible de fuentes autorizadas, la presente Tesis debe mucho a las valiosas aportaciones de estos dos autores en particular.

En el ámbito europeo, tampoco existen monografías sobre el particular publicadas en inglés, si bien sí se han publicado diversos artículos sobre la DCD y su impacto en el

[1] Es evidente que los procesalistas han encontrado en la LCD una nueva herramienta de investigación y represión aplicable en el enjuicimiento criminal español, y que por ello se hayan aprestado a analizar la norma desde su aplicación directa al proceso. Obviamente, estos análisis sólo se cuidan de las implicaciones constitucionales o administrativas de la norma en la medida y con la intensidad que sea realmente necesarias para estos propósitos particulares.

sistema de derechos fundamentales, que son aquí convenientemente citados o comentados.

La escasez de doctrina sobre la normativa de conservación de datos se compensa en cambio con una sobreabundancia de informes y dictámenes emitidos durante la tramitación de la DCD y la LCD por instancias tales como la Comisión Europea, el Supervisor Europeo de Protección de Datos, el Grupo sobre Protección de Datos del Artículo 29, el Comité Económico y Social Europeo, el Consejo de Estado, la Agencia Española de Protección de Datos o el Consejo General del Poder Judicial, entre otros. Estos informes son a nuestro entender las fuentes más valiosas sobre la materia, y ello explica que, siempre que ha sido posible, hayamos recurrido a sus observaciones y puntos de vista, aún a riesgo de dar una imagen de escasa profundidad doctrinal.

Estructura

En lo que se refiere a la estructura de la presente Tesis, ésta se divide en cuatro grandes bloques, más un quinto adicional, al que siguen unas conclusiones, una bibliografía clasificada y varios anexos.

La primera aportación que esta Tesis ofrece a la doctrina se concreta en la Primera y Tercera Parte de esta Tesis, y consiste en una exposición estructurada, comprehensiva y contextualizada de la normativa de conservación de datos a nivel europeo y nacional, así como un relato ordenado de las circunstancias políticas, legales e históricas que rodearon su aprobación, junto con una explicación acerca del modo en que han repercutido en la legislación en la que se enmarca. Pese a que tal contenido pudiera parecer una aportación desprovista de valor científico, lo cierto es que no podrá encontrarse hasta la fecha en la literatura jurídica europea ni española un comentario sistematizado tan extenso sobre ambas normas y que considere además las tres vertientes de esta materia: la procesal-penal, la administrativa y la constitucional. Obsérvese además que un examen histórico-político resulta particularmente relevante dado que esta normativa nace de una decisión de política legislativa que venía fuertemente condicionada por el contexto internacional de la primera década del siglo

XXI. Entender este contexto permite valorar la conveniencia o no de la normativa en la actualidad, una vez que estos condicionantes han variado en buena medida.

Las partes Segunda y Cuarta estudian el impacto de la DCD y de la LCD en el sistema de derechos fundamentales de la Unión Europea y de la Constitución Española, respectivamente. La vigente normativa sobre conservación de datos supone una limitación de derechos y libertades que son ejercidas diariamente por el común de los ciudadanos a través del uso de comunicaciones electrónicas, concretamente, el secreto de las comunicaciones y la protección de datos de carácter personal. La compatibilidad de la DCD con el sistema de derechos fundamentales de la Unión, y la constitucionalidad de la LCD son evaluadas de acuerdo con sus respectivos marcos.

Como puede observarse, los contenidos de la DCD y la LCD son estudiados separadamente. Esto se debe a que, si bien una norma ha dado origen a la otra, lo cierto es que ambas se enmarcan en ordenamientos jurídicos distintos, que han condicionado y condicionarán su futuro, como bien demuestran los avatares que la conservación de datos ha conocido en distintos Estados miembros tales como Suecia, Austria o Rumanía. Mezclar los contenidos de ambas normas sólo habría añadido confusión a una materia que clama por clarificación. En cualquier caso, la estrecha relación entre la norma europea y la nacional no puede ser en modo alguno ignorada, y por eso, siempre que ha sido oportuno, no se han escatimado las referencias al contenido de una respecto de la otra.

La Parte Quinta de la Tesis lleva a cabo la exposición del régimen de los servicios de telefonía mediante tarjetas prepago introducido por la Disposición Adicional Única de la LCD. Dicho régimen no encuentra su base en previsión alguna de la DCD, y parte del deseo del legislador español de resolver una posible deficiencia de la directiva, el anonimato en las tarjetas prepago. El análisis que ofrecemos pone en evidencia los muchos defectos de dicho régimen.

Finalmente, la Tesis se cierra con una relación de las conclusiones alcanzadas en nuestra investigación que, al tiempo que resumen su contenido, exponen sus resultados y aportaciones más relevantes.

Coda

La conservación de datos de las comunicaciones electrónicas es una medida de seguridad nacional que ocupa un lugar central entre aquellas leyes que ponen la tecnología digital al servicio del bien común, y supone al mismo tiempo un sacrificio parcial de derechos y libertades individuales. Si bien no cabe poner en duda su utilidad, también es evidente la dificultad de determinar cuánto de bien común y cuánto de libertad individual deben combinarse en la fórmula para que la ecuación sea correcta o —lo que en definitiva es lo mismo— proporcionada y justa. En este sentido, creemos que esta regulación merecería una mucho mayor atención por parte de los operadores jurídicos en general. En este sentido, confiamos esperanzados que quienes se interesen por esta cuestión puedan encontrar en la presente Tesis un trabajo exhaustivo y ordenado que da cuenta, por una parte, de las implicaciones legales y principales carencias de esta normativa; y por otra, de las tensiones jurídico-constitucionales que subyacen a tan relevante materia junto con algunas sugerencias para resolverlas.

PRIMERA PARTE. LA CONSERVACIÓN DE DATOS EN EL DERECHO DE LA UNIÓN EUROPEA

1 Marco histórico, político y jurídico de la normativa europea sobre conservación de datos

1.1 Introducción

La vigente regulación europea sobre la conservación de datos de las comunicaciones electrónicas no puede comprenderse cabalmente sin examinar primero las circunstancias que rodearon su nacimiento y, en particular, la evolución—en las últimas dos décadas—de la legislación comunitaria en tres materias concretas: la protección de datos personales, la regulación de las telecomunicaciones y la cooperación policial, penal y de seguridad.

Como veremos, la protección de datos personales como materia comunitaria nació de la necesidad de garantizar la unidad del mercado interior. La normativa general dio paso—a la vuelta de unos años—a una normativa específica sobre la protección de datos personales en las comunicaciones electrónicas. No obstante, tanto una como otra excluyeron hasta nuestros días de su ámbito de aplicación los aspectos relativos a la cooperación policial, penal y de seguridad. Los graves atentados terroristas acontecidos en los primeros años del siglo XXI condujeron a las autoridades europeas a la aprobación de la DCD, una norma que por primera vez reguló tales aspectos dentro del marco comunitario. Sin embargo, la legalidad de esta normativa ha sido cuestionada desde un primero momento. En los apartados siguientes analizaremos todas estas cuestiones con mayor detalle.

1.2 Origen de la protección de datos de las comunicaciones electrónicas

Hemos de empezar este examen señalando que las razones que a mediados de los años noventa movieron a las entonces Comunidades Europeas a regular la protección de datos personales se encontraban en la necesidad de garantizar el correcto funcionamiento del mercado único que, conforme al art. 7.A TCE, había establecido la libre circulación de mercancías, personas, servicios y capitales en todo el territorio comunitario[2]. En concreto, el surgimiento de las tecnologías de la información venía facilitando de manera exponencial desde los años setenta el tratamiento e intercambio de datos personales en los diferentes sectores de la actividad económica y social[3]. La Comunidad observó que las diferencias entre los niveles de protección de los derechos y libertades de las personas—y, en particular, de la intimidad—garantizados por los Estados miembros en el tratamiento de datos personales eran susceptibles de impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro, lo que, obviamente, constituía un obstáculo para el ejercicio de las actividades económicas a escala comunitaria[4]. Con el fin de eliminar obstáculos en el flujo transfronterizo de datos personales entre todos los agentes de la vida económica comunitaria, el nivel de protección de los derechos y libertades de las personas en el tratamiento de dichos datos debía ser equivalente en todos los Estados miembros[5]. Tal objetivo se entendía esencial para el mercado interior y, por tanto, era de todo punto necesario que la Comunidad interviniera para aproximar las legislaciones a través de una norma armonizadora[6], que tomó cuerpo en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Dos años más tarde, el desarrollo de la sociedad de la información[7] dio lugar a la introducción de nuevos servicios de telecomunicaciones, nuevas redes digitales

[2] Cf. considerandos tercero y quinto, Directiva 95/46/CE.

[3] Cf. considerando cuarto, Directiva 95/46/CE.

[4] Cf. considerando séptimo, Directiva 95/46/CE.

[5] Cf. considerando octavo, Directiva 95/46/CE.

[6] Ibíd.

[7] Sobre este concepto de "sociedad de la información" y sus implicaciones más allá del Derecho, cf. Ruiz de Querol, R., y Buira, J., La Sociedad de la Información, Editorial UOC, Barcelona, 2007.

públicas y el desarrollo transfronterizo de estos servicios, que crearon necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios. El buen funcionamiento del mercado común exigió traducir los principios establecidos en la Directiva 95/46/CE en normas concretas para el sector de las telecomunicaciones[8]. Vio así la luz 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. De nuevo, como afirma su considerando octavo, la protección del mercado interior de las telecomunicaciones fue el motor de que las disposiciones legales, reglamentarias y técnicas adoptadas por los Estados miembros para proteger los datos personales, la intimidad y los intereses legítimos de las personas jurídicas, en el sector de las telecomunicaciones, fueran armonizadas a fin de evitar obstáculos en aquél[9]. Advertía además la norma, en el mismo lugar, que dicha armonización se limitaría a los requisitos necesarios para garantizar que no se obstaculizasen la promoción y el desarrollo de nuevos servicios de telecomunicación y nuevas redes entre los Estados miembros.

Pocos años después, la Directiva 97/66/CE hubo de ser sustituida por la vigente 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 —más conocida como Directiva sobre la privacidad y las comunicaciones electrónicas—. Las previsiones de la Directiva 97/66/CE debían adaptarse al rápido desarrollo que en pocos años habían experimentado los mercados y las tecnologías de los servicios de comunicaciones electrónicas, de tal manera que el nivel de protección de los datos personales y de la intimidad ofrecido a los usuarios de los servicios de comunicaciones electrónicas disponibles al público siguiera siendo el mismo, con independencia de las tecnologías utilizadas[10]. Al igual que con la anterior directiva, el legislador comunitario pretendió traducir los principios establecidos en la Directiva 95/46/CE a normas específicas para el sector de las comunicaciones electrónicas, con el fin de garantizar el respeto de los

[8] Cf. considerandos tercero y quinto, Directiva 97/66/CE.

[9] Cf. considerando octavo, Directiva 97/66/CE.

[10] Cf. considerando cuarto, Directiva 2002/58/CE.

derechos fundamentales[11] y, sobre todo, la unidad de mercado. Su considerando octavo repetía el argumento acerca de la necesidad de armonizar las disposiciones legales, reglamentarias y técnicas adoptadas por los Estados miembros para proteger los datos personales, la intimidad y los intereses legítimos de las personas jurídicas en el sector de las comunicaciones electrónicas, a fin de evitar obstáculos para el mercado interior de este sector de conformidad con el art. 14 TCE[12]. Al igual que en la Directiva 97/66/CE, la armonización se limitó expresamente a los requisitos necesarios para garantizar que no se vieran obstaculizados el fomento y el desarrollo de los nuevos servicios y redes de comunicaciones electrónicas entre Estados miembros[13].

1.3 Exclusión de la cooperación judicial y policial de la normativa comunitaria sobre protección de datos

Debe subrayarse que las tres directivas expuestas excluyeron absoluta y expresamente de su ámbito de aplicación la cooperación policial y judicial en materia penal, dado que, de conformidad con el TCE, tales materias no se encontraban entre los fines y competencias de la Comunidad Europea, que sí incluían en cambio la misión de promover, mediante el establecimiento de un mercado común y de una unión

---

[11] Cf. considerando segundo, Directiva 2002/58/CE.

[12] Concretamente, como manifiesta el considerando quinto, se entendía por la Unión que el éxito del desarrollo transfronterizo de los nuevos servicios de comunicaciones electrónicas dependía en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad.

Por su parte, el art. 14 TCE disponía en sus dos primeros apartados que "1. La Comunidad adoptará las medidas destinadas a establecer progresivamente el mercado interior en el transcurso de un período que terminará el 31 de diciembre de 1992, de conformidad con las disposiciones del presente artículo, de los artículos 15 y 26, del apartado 2 del artículo 47 y de los artículos 49, 80, 93 y 95 y sin perjuicio de lo establecido en las demás disposiciones del presente Tratado.

2. El mercado interior implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones del presente Tratado".

[13] Cf. considerando octavo, Directiva 2002/58/CE: "la armonización debe limitarse a los requisitos necesarios para garantizar que no se vean obstaculizados el fomento y el desarrollo de los nuevos servicios y redes de comunicaciones electrónicas entre Estados miembros".

económica y monetaria, un desarrollo armonioso, equilibrado y sostenible de las actividades económicas en el conjunto de la Comunidad —art. 2 TCE— así como la aproximación de las legislaciones nacionales "en la medida necesaria para el funcionamiento del mercado común" —art. 3.1.h) TCE—. De hecho, la política exterior y de seguridad común y la prevención y la lucha contra la delincuencia eran materia de un marco legal diferente, al ser incluidos entre los objetivos de la Unión Europea a través del art. 2 del Tratado de la Unión Europea —en adelante, TUE—. Su Título VI, sobre "disposiciones relativas a la cooperación policial y judicial en materia penal", recogía el compromiso de los Estados miembros de elaborar una "acción en común" en los ámbitos de la cooperación policial y judicial en materia penal —art. 29 TUE—[14]. Las concretas condiciones para llevar a cabo esta acción se fijaban a lo largo de este Título VI, e incluían la adopción progresiva de medidas que establecieran normas mínimas relativas a los elementos constitutivos de los delitos y a las penas en los ámbitos de la delincuencia organizada, el terrorismo y el tráfico ilícito de drogas —art. 31 TUE—. A iniciativa de cualquier Estado miembro o de la Comisión, el Consejo podría, por unanimidad, adoptar *decisiones marco* para la aproximación de las disposiciones legales y reglamentarias de los Estados miembros. Las decisiones marco no tenían efecto directo pero obligaban a los Estados miembros en cuanto al resultado que debiera conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios —art. 32.1.b) TUE—.

---

[14] El Tratado de la Unión Europea, firmado en 1992, introdujo una nueva estructura institucional en las Comunidades Europeas que se mantuvo hasta la entrada en vigor del Tratado de Lisboa en 2009. Dicha estructura institucional estaba compuesta por lo que se dio en llamar los "tres pilares":

— el Primer Pilar, también denominado Pilar Comunitario, correspondía a las tres comunidades: la Comunidad Europea, la Comunidad Europea de la Energía Atómica —Euratom— y la antigua Comunidad Europea del Carbón y del Acero —CECA— y cubría materias tales como la ciudadanía de la Unión, políticas comunitarias, la unión económica y monetaria, etc.;

— el Segundo Pilar, que correspondía a la política exterior y de seguridad común, que estaba regulada en el Título V del TUE;

— el Tercer Pilar, sobre la cooperación policial y judicial en materia penal, cubierta por el Título VI del TUE. Estos tres pilares funcionaban siguiendo procedimientos de decisión diferentes: procedimiento comunitario para el Primer Pilar y procedimiento intergubernamental para los otros dos. El Tratado de Lisboa ha eliminado esta estructura de pilares en beneficio de la creación de la Unión Europea.

Así pues, dado este reparto de competencias, las directivas comunitarias no podían sino excluir de su ámbito de aplicación cualquier aspecto relativo a la cooperación policial y judicial en materia penal. Eso explica que el art. 3.2 de la aún vigente Directiva 95/46/CE disponga que la misma no se aplicará al tratamiento de datos personales que sea efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, "como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea[15] y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal". La misma cláusula de exclusión incluyeron la Directiva 97/66/CE y su sucesora, la Directiva 2002/58/CE. Ambas reiteraron en su art. 1.3 que sus disposiciones no se aplicarían a las actividades no comprendidas en el ámbito de aplicación del TCE[16].

La exclusión de las cuestiones penales y de seguridad respecto de las normas europeas sobre protección de datos era, por tanto, cuestión clara y pacífica. No obstante, quizás para mayor seguridad, el legislador comunitario tuvo a bien incluir, dentro del articulado de las tres citadas directivas, epígrafes que confirmaban adicionalmente esta exclusión y la competencia de los Estados para legislar libremente sobre estas

---

[15] El Título V versaba sobre Disposiciones relativas a la política exterior y de seguridad común y el Título VI sobre Disposiciones relativas a la cooperación policial y judicial en materia penal. Es importante remarcar, como lo hacía el considerando décimo tercero de la Directiva 95/46/CE, que "las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; que el tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado".

[16] Y así, la vigente norma establece que "la presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, como las reguladas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal".

cuestiones, al margen de los principios comunitarios sobre protección de datos. Así, el art. 13.1 de la Directiva 95/46/CE advierte aún que los Estados miembros pueden adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos cuando tal limitación constituya una medida necesaria para la salvaguardia de, entre otras, la seguridad del Estado, la defensa, la seguridad pública o la prevención, la investigación, la detección y la represión de infracciones penales.

Tanto la Directiva 97/66/CE como la vigente 2002/58/CE, al tiempo que desarrollaban los principios de la Directiva 95/46/CE en los servicios de telecomunicaciones, incluyeron cláusulas de exclusión similares a las del art. 13.1. Así, en el desarrollo de dichos principios, la Directiva 97/66/CE estableció en su art. 5.1 que los Estados miembros garantizarían, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público, prohibiendo en particular la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados[17]. Asimismo, el art. 6 estableció que los datos sobre tráfico relacionados con los usuarios y abonados tratados para establecer comunicaciones y almacenados por el proveedor de una red o servicio público de telecomunicación debían destruirse o hacerse anónimos en cuanto terminase la comunicación, excepto aquellos necesarios a efectos de la facturación de los usuarios hasta la expiración del plazo durante el cual pueda impugnarse la factura o cuando el abonado habiera dado su consentimiento[18]. Frente a estos principios, el art. 14.1 —a imitación del art. 13.1 de la

[17] El tenor literal del art. 5.1 establecía que "1. Los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente, de conformidad con el apartado 1 del artículo 14".

[18] Transcribimos aquí, para su examen directo, el tenor literal de la norma derogada: "1. Sin perjuicio de lo dispuesto en los apartados 2, 3 y 4, los datos sobre tráfico relacionados con los usuarios y abonados tratados para establecer comunicaciones y almacenados por el proveedor de una red o servicio público de telecomunicación deberán destruirse o hacerse anónimos en cuanto termine la comunicación.

Directiva 95/46/CE— dispuso que los Estados miembros podrían adoptar medidas legales para limitar el alcance de tales obligaciones y derechos cuando dichas limitaciones constituyan una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos. Tal excepción había de entenderse como una mera clarificación, dado que, como ya hemos señalado, el art. 1.3 de la misma directiva establecía que sus disposiciones no se aplicarían a las actividades no comprendidas en el ámbito de aplicación del Derecho comunitario —"como las reguladas por las disposiciones de los títulos V y VI [TUE] ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado", etc.—.

La vigente Directiva 2002/58/CE, al actualizar la Directiva 97/66/CE en materia de protección de datos en las comunicaciones electrónicas, contiene previsiones similares. Así, el art. 5.1 establece 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 las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, lo que en todo caso no impedirá el almacenamiento técnico necesario para la conducción de una

---

2. A los efectos de la facturación de los usuarios y de los pagos de las interconexiones, podrán ser tratados los datos indicados en el anexo. Se autorizará este trata miento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

3. El proveedor de un servicio público de telecomunicación podrá tratar los datos a que se hace referencia en el apartado 2 para la promoción comercial de sus propios servicios de telecomunicación siempre y cuando el abonado haya dado su consentimiento.

4. El tratamiento de los datos de tráfico y facturación deberá limitarse a las personas que actúen bajo las órdenes del proveedor de la red o del servicio público de telecomunicación que se ocupe de la gestión de la facturación o del tráfico, de las solicitudes de información de los clientes y de la detección de fraudes y promoción comercial de los propios servicios del proveedor, y deberá limitarse a lo necesario para realizar tales actividades".

comunicación, sin perjuicio del principio de confidencialidad[19]. Seguidamente, el art. 6 determina que los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deben eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación, exceptos aquellos datos de tráfico necesarios a efectos de la facturación de los abonados hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago —art. 6.2— o cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento —art. 6.3—[20]. Reglas similares y específicas se prevén en el art. 8, para la presentación y restricción de la identificación de la línea de origen y de la línea conectada, y en el art. 9, para los datos de localización

[19] Conforme al tenor literal del art. 5.1, "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 las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y 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. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad".

[20] Bajo la rúbrica de "datos de tráfico", el art. 6 dispone en sus tres primeros apartados que 1. Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.

2. Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

3. El proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido en la medida y durante el tiempo necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento. Los usuarios o abonados dispondránde la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento".

distintos de los datos de tráfico. Frente a estos principios —que concretan los generales de la Directiva 95/46— el art. 15 confirma la capacidad de los Estados miembros para adoptar medidas legales que limiten el alcance de los derechos y obligaciones de los citados artículos 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". El tenor literal del artículo continúa advirtiendo que "para ello, los Estados miembros 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. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea". La previsión del art. 15.1 ha de entenderse como una mera clarificación, dado que, como ya hemos señalado, el art. 1.3 de la misma directiva establecía que sus disposiciones no se aplicarían a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, como las reguladas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal. A su vez, el art. 15.1 no es sino una transcripción del citado art. 13.1 de la Directiva 95/46/CE, que hace la misma aclaración con respecto a la regulación comunitaria genérica de la protección de datos. Por otra parte, al indicar el art. 15.1 que los Estados podrán adoptar medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado "por los motivos establecidos en el presente apartado", o al advertir que estas medidas deberán ser "conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea", el precepto no hace sino recordar a los Estados miembros el debido respeto al Derecho primario vigente, tanto en lo que se refiere al reparto de competencias en la Comunidad, como a la garantía de los derechos fundamentales.

De todo lo expuesto se concluye por tanto que, desde un principio, y de acuerdo con el Derecho comunitario vigente en el momento de aprobación de la DCD, los Estados miembros gozaban de plena libertad y competencia para adoptar medidas de conservación de datos con fines de penales, a pesar de que tal medida limitara los principios de protección de datos establecidos por la normativa comunitaria.

1.4 Hacia una normativa europea sobre conservación de datos de las comunicaciones electrónicas

Si volvemos nuestra mirada a la política legislativa europea en la materia de nuestro estudio, se constata que los Estados miembros no mostraron interés por la adopción de medidas de conservación de datos de las comunicaciones electrónicas con fines penales hasta los primeros años del siglo XXI. De hecho, sólo fue a partir de la popularización de internet y la telefonía móvil a finales de los años noventa cuando las autoridades policiales empezaron a estudiar la posibilidad de arbitrar medidas que les permitieran vigilar el tráfico de datos en las comunicaciones electrónicas. Un importante hito en este proceso fue la reunión en Washington de los Ministros de Justicia e Interior de los países del G-8, los días 9 y 10 de diciembre de 1997, como resultado de la cual los Estados adoptaron un plan de acción de diez puntos que había de ponerse en práctica con ayuda de un Subgrupo Especializado en Delitos de Alta Tecnología, formado por representantes de las autoridades policiales de estos países. Uno de los apartados más destacados del plan, y sin duda el más novedoso, era la necesidad de establecer medidas de conservación de los datos sobre tráfico, tanto histórico como futuro, por parte de los proveedores de internet a efectos de cumplimiento de las disposiciones legislativas y su puesta a disposición de las autoridades policiales[21].

---

[21] Cf. Reunión de Ministros de Justicia e Interior de los Ocho, 9-10 de diciembre de 1997, Comunicado, Washington D.C., 10 de diciembre, Anexo al comunicado: Principios y plan de acción para combatir el delito de alta tecnología. El comunicado oficial declaraba que era "el sector industrial el que diseña, despliega y mantiene estas redes globales, y él es el responsable principal de la elaboración de normas técnicas. Así pues, corresponde al sector industrial desempeñar su parte en el desarrollo y la distribución de sistemas seguros diseñados para ayudar a detectar el abuso informático, conservar las pruebas

La reacción de las Comunidades Europeas a esta propuesta del G-8 vino de la mano del Grupo de Trabajo del Artículo 29 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales[22] —en adelante, GT29— que, el 7 de septiembre de 1999 aprobó su Recomendación 99/3 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación. La Recomendación constituye el primer documento comunitario relevante que se ocupa de la conservación de datos. Su importancia descansa principalmente en dos motivos.

En primer lugar, es digno de subrayarse que el GT29 —recordando la normativa comunitaria al respecto que hemos expuesto más arriba—, consideró en aquel momento que los datos sobre tráfico no debían conservarse a efectos penales y que las legislaciones nacionales no debían obligar a los operadores de telecomunicaciones a conservar los datos sobre tráfico durante un plazo superior al necesario a efectos de facturación. Basaba esta opinión en el hecho de que la posesión por un tercero de datos sobre tráfico relativos al uso de los servicios de telecomunicación constituía una limitación del derecho a la intimidad de las personas y a la confidencialidad de las comunicaciones. La conservación generalizada de datos de tráfico para fines penales resultaba además contraria, a su entender, no sólo a las prácticas tradicionales de los Estados miembros, sino a los requisitos del art. 8.2 CEDH y de la jurisprudencia del TEDH, que prohibían la vigilancia exploratoria o general a gran escala. De este modo, advertía el Grupo, los poderes públicos podían tener acceso a datos sobre tráfico

---

electrónicas y contribuir a determinar la situación e identidad de los delincuentes". Cita extraída de la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones - Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos, disponible en http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=es&type_doc=COMfinal&an_doc=2000&nu_doc=890.

[22] Recomendación 99/3, de 7 de septiembre de 1999, sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada por el Grupo de Trabajo del Artículo 29 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales (DG XV D 5085/99/final WP 25). Puede accederse a su texto en el siguiente enlace: http://www.informatica-juridica.com/anexos/anexo494.asp.

únicamente de manera individualizada, pero nunca sistemática ni general, como pretendía el G-8.

Por otra parte, en segundo lugar, la Recomendación del GT29 es importante porque, al hilo de este análisis pero sin relación con materias penales o de seguridad, el GT29 llamaba la atención de la Comisión sobre las disparidades entre los países miembros en lo que se refería al período durante el cual se podían conservar los datos sobre tráfico. Si bien la Directiva 97/66/CE solamente permitía su tratamiento a efectos de facturación y hasta la expiración del plazo de impugnación de la factura, lo cierto es que este plazo variaba significativamente entre los Estados miembros[23]. Tampoco era homogénea la práctica de los proveedores de internet pues, como observaba el GT29, mientras los pequeños proveedores conservaban los datos sobre tráfico durante períodos muy breves —unas horas— debido a una falta de capacidad de almacenamiento, los proveedores más importantes podían permitirse conservar los datos sobre tráfico durante unos meses. Todas estas divergencias —advertía el órgano— podían plantear obstáculos en el mercado interior para la prestación transfronteriza de servicios de telecomunicación e internet, al tiempo que la existencia de plazos tan diferentes podía dificultar el control del cumplimiento legislativo, pues se podía dar el caso de que un proveedor de internet establecido en un Estado miembro no tuviera derecho a almacenar datos sobre tráfico durante más tiempo del permitido en el Estado miembro donde el cliente utiliza sus servicios, o bien que se viera obligado a

[23] Por ejemplo, según relata la Recomendación, en Alemania los operadores de telecomunicaciones y los proveedores de servicios de telecomunicación podían almacenar los datos necesarios para facturación durante un plazo máximo de ochenta días a efectos de demostrar la corrección de la factura. En Francia, dependía del tipo de operador: el operador de telecomunicaciones "tradicional" podía conservar los datos sobre tráfico hasta un año basándose en la ley que fijaba el plazo durante el cual podía impugnarse la factura. Este plazo queda fijado en diez años para los demás operadores. En Austria, la ley sobre telecomunicaciones no fijaba ningún plazo concreto para guardar los datos sobre tráfico a efectos de facturación, sino que lo limitba al plazo durante el cual podía impugnarse la factura o exigirse el pago. En el Reino Unido, de conformidad con la ley, la factura podía impugnarse durante seis años, pero los operadores y proveedores de servicio almacenaban los datos pertinentes durante unos dieciocho meses. En Bélgica la ley no definía el plazo, pero el mayor proveedor de servicios de telecomunicación lo establecía en tres meses en sus condiciones generales. Otra práctica distinta podía observarse en Portugal pues, dado que el plazo no estaba fijado por ley, la autoridad nacional de control de la protección de datos decidía de manera individualizada. En Noruega, en cambio, el plazo estaba fijado en catorce días.

conservar los datos sobre tráfico durante más tiempo del permitido en su propio Estado miembro porque el país de los usuarios así lo exigiera legalmente. A la vista de estas disparidades, el Grupo recomendaba que la Comisión propusiera medidas apropiadas para una mayor armonización del plazo durante el cual se permitía a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de internet conservar los datos sobre tráfico para facturación y pago de interconexiones. Este plazo debía a su entender ser suficiente para permitir a los consumidores impugnar la factura, pero lo más breve posible para no sobrecargar a los operadores y proveedores de servicios y para respetar los principios de proporcionalidad y especificidad como componentes del derecho a la intimidad. En concreto, el GT29 recomendaba que el plazo debía ser conforme con los mayores niveles de protección observados en los Estados miembros, al tiempo que subrayaba el hecho de que en varios Estados miembros se habían aplicado satisfactoriamente plazos no superiores a tres meses. Como veremos más adelante, la constatación de estas disparidades en los plazos de conservación de los datos serviría como argumento siete años después para justificar la aprobación de la DCD.

En todo caso, ni el plan del G-8 ni la Recomendación del GT29 tuvieron efecto inmediato en el Derecho europeo. De hecho, el interés de los Estados por la conservación de datos no surgiría hasta pasados varios años, concretamente después de los atentados el 11 de septiembre de 2001, que pusieron de manifiesto que las telecomunicaciones electrónicas podía resultar un cauce idóneo para la preparación y comisión de graves delitos contra la seguridad nacional. De esa manera, la interceptación o conservación de los datos de las comunicaciones electrónicas pasó de considerarse un asunto de interés secundario —que ocupaba la atención principalmente de los expertos en seguridad— a constituir una de las piezas claves en las legislaciones antiterroristas que algunos países pusieron en marcha a partir de aquella fecha.

El mejor y más temprano ejemplo de este fenómeno histórico se encuentra en la famosa *USA Patriot Act* que, aprobada el 26 de octubre de 2001 —apenas un mes después del 11-S— estableció como su fin principal el "detener y castigar actos terroristas", al tiempo que ponía en marcha una batería de incisivas medidas legales para la

investigación y enjuiciamiento de tales actos[24]. Así, verbigracia, en relación con la privacidad y la interceptación de las comunicaciones electrónicas las secciones 201 y 202 de dicha ley autorizaron la interceptación de comunicaciones electrónicas relacionadas con el terrorismo o con delitos informáticos, en tanto que, por su parte, la sección 209 previó la posibilidad de intervenir mensajes de voz mediante mandato judicial[25].

Así, desde 2001, fecha en que comenzaron las reuniones del Foro Cibercrimen, la cuestión de la conservación de los datos de tráfico no dejó de ser objeto de consultas con representantes de las autoridades represivas, la industria de las comunicaciones

[24] Sobre la Patriot Act y el restante marco de la normativa antiterrorista que surge en Estados Unidos tras los atentados del 11-S existe numerosa literatura española y extranjera. Entre lo más relevante cabe destacar: ACKERMAN, B., "The Emergency Constitution", en 113 Yale Law Journal, 2004, pp. 1029 y ss.; BASSU, C., "Libertá personale e lotta al terrorismo: i casi di Canada e Stati Uniti", en Groppi, Tania (a cura di), Democrazia e Terrorismo, Lezioni Volterrane, volumen I, Editoriale Scientifica, Napoli, 2005, pp. 425 y ss.; BELLAZZI, M., "I 'Patriot Acts' e la limitazione dei diritti costituzionali negli Stati Uniti'", Politica del Diritto, a. XXXIV, n. 4, 2003, pp. 681 y ss.; BELTRÁN DE FELIPE, M. y GONZÁLEZ GARCÍA, J. V., Las sentencias básicas del Tribunal Supremo de los Estados Unidos de América, Centro de Estudios Políticos y Constitucionales – BOE, Madrid, 2005; BOLLO AROCENA, Mª D., "Hamdan v. Rumsfeld. Comentario a la Sentencia dictada por el Tribunal Supremo de Estados Unidos el 29 de junio de 2006", Revista Electrónica de Estudios Internacionales, 12, 2006; CASSEL, E., The war on civil liberties: how Bush and Ashcroft have dismantled the Bill of Rights, Chicago, Lawrence Hill Books, 2004; COLE, David, "Enemy Alliens", en 54 Standord Law Review, 2002, pp. 954 y ss.; ETZIONI, A.i, How patriotic is the Patriot Act?: freedom versus security in the age of terrorism, New York, Routledge, 2004; GIMENO SENDRA, V., "Repercusiones de la lucha norteamericana contra el terrorismo en la tutela de los derechos humanos", Derechos, justicia y estado constitucional: un tributo a Miguel C. Miravet, Valencia, Tirant lo Blanch, 2005; GOLDSMITH, J., The terror presidency: law and judgment inside the Bush Administration, New York, W. Norton & Company, 2007; GUDÍN RODRÍGUEZ-MAGARIÑOS, F., "El Derecho Penal del enemigo y la Military Commissions Act de 2006: ¿Requiem por las garantías de los presuntos terroristas?", en Revista de Derecho y Proceso Penal, núm. 17, Thomson-Aranzadi, 2007, pp. 13 y ss.

[25] Su título oficial y completo es *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 115 Stat. 272 (2001)*. Puede consultarse su publicación oficial en http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

electrónicas o los expertos en protección de datos[26]. La posibilidad de regular el deber de conservación de datos como herramienta de lucha contra una delincuencia transnacional que aprovechaba cada vez con más intensidad las enormes potencialidades de internet para la consecución de sus ilícitos fines fue estudiada un año después en la Conferencia Internacional de los Comisarios Europeos responsables de protección de datos —celebrada en Cardiff entre el 9 y el 11 de septiembre de 2002 [27] —, cuya Declaración final propuso la mejora de las infraestructuras de información y la lucha contra los delitos informáticos. Entre otras cosas, la declaración apostaba decidida y explícitamente por una necesaria armonización de las escasas legislaciones de los Estados miembros que por entonces habían previsto algún punto en materia de conservación de datos de tráfico.

El precedente de la *Patriot Act,* y de los debates previos en materia de conservación de datos de las comunicaciones electrónicas con fines penales[28] dejaron su marca en la ya expuesta Directiva 2002/58/CE que, al establecer y actualizar las garantías para la seguridad y privacidad de los comunicaciones electrónicas, reconoce específicamente en su art. 15.1 —como vimos— la competencia de los Estados miembros para establecer medidas de conservación de datos, adoptando, entre otras, "medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado" cuando tal limitación constituya "una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la

[26] Información citada en la Exposicion de Motivos de la Propuesta de Directiva, *Consulta a las partes interesadas y evaluación del impacto*.

[27] La declaración fue objeto de examen en el interesante Dictamen 5/2002, aprobado el 11 de octubre de 2002 por el GT29, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales (11818/02/ES/Final WP 64). El texto del mismo está disponible en el siguiente enlace: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[28] En este sentido resulta ineludible la cita de la Comunicación de la Comisión COM(2000) 890 final, al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, sobre la creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos (eEUROPE 2002); así como las conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002. Como ya señalamos, el texto puede consultarse en http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=es&type_doc=COMfinal&an_doc=2000&nu_doc=890.

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". La previsión, como hemos señalado al principio de este capítulo, no es más que una cláusula de permisividad, que elimina cualquier incertidumbre sobre el poder de los Estados miembros para regular bases de datos sobre comunicaciones electrónicas con fines públicos de especial relevancia. Así lo confirma por extenso el considerando undécimo de la Directiva 2002/58/CE, que afirma que la norma no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según la interpretación que se hace de éste en las sentencias del Tribunal Europeo de Derechos Humanos. "Dichas medidas —añade a prevención— deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas".

No obstante, el mero hecho de que la Directiva 2002/58/CE se refiera expresamente a esta posibilidad confirma la irrupción, en el ámbito de la protección de datos personales en las telecomunicaciones, de una creciente preocupación por las cuestiones penales y de seguridad, al tiempo que servía de invitación y luz verde para que los Estados miembros aprobaran medidas de conservación generalizada.

De hecho, el interés de la Unión en la adopción de estas medidas recibió renovado impulso con la Comunicación de la Comisión Europea COM (2000) 890 final, al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones[29], así como poco después, en las Conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002[30]. La Comunicación llevó a cabo el primer estudio comunitario sobre la conveniencia y obstáculos de las medidas de conservación de

[29] Cf. Comunicación de la Comisión al Consejo…, op. cit.

[30] Cf. Sesión nº 2477 del Consejo - Justicia y Asuntos de Interior - Bruselas, 19 de diciembre de 2002, C/02/404. Las actas del Consejo están publicadas en http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/02/404&format=HTML&aged=1&language=ES&guiLanguage=en.

datos, al tiempo que creaba un foro[31] en el que, entre otras cosas, la Comisión *exhortaba* "a todas las partes implicadas a discutir a fondo, como cuestión prioritaria, el complejo problema de la conservación de los datos sobre tráfico con vistas a encontrar conjuntamente soluciones apropiadas, equilibradas y proporcionadas que respeten plenamente los derechos fundamentales a la intimidad y a la protección de datos"[32]. Basándose en los resultados de estos debates, la Comisión evaluaría "la necesidad de acciones legislativas o no legislativas a escala de la UE"[33]. Por su parte, las Conclusiones del Consejo de Justicia e Interior instaron a todas las partes interesadas —"gobiernos, parlamentos, fuerzas policiales y autoridades judiciales, sector empresarial, autoridades de protección de datos y otras partes interesadas"— a que, *con carácter prioritario*, iniciasen "un diálogo abierto y constructivo a nivel nacional y de la UE orientado a hallar soluciones para el problema de la conservación de datos sobre tráfico que atiendan tanto a la necesidad de disponer de instrumentos eficaces de prevención, descubrimiento, investigación y persecución de delitos como a la necesidad de proteger los derechos y libertades"[34]. El Foro sobre la delincuencia cibernética recién creado por la Comisión se señalaba como un mecanismo particularmente idóneo para aumentar la coordinación en este asunto[35].

Una vez iniciados, en estas circunstancias, los debates en el seno de la Unión, el impulso definitivo a una legislación comunitaria en materia de conservación de datos sólo se produjo —desgraciadamente— con la conmoción social y política que sacudió Europa tras los atentados terroristas sufridos en Madrid —el 14 de marzo de 2004— y en Londres —el 7 de julio de 2005—, y que comportarían la adopción urgente de una

---

[31] Cf. Comunicación de la Comisión al Consejo…, doc. cit., punto 6.4.

[32] Ibíd., punto 5.2.

[33] Ibíd.

[34] Ibíd., punto 6 del apartado Tecnologías de la información y la investigación y la acción penal contra la delincuencia organizada. Hemos de recordar que el considerando séptimo, DCD, se remite a este documento para justificar la adopción de la directiva, advirtiendo que "las conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002 destacan que, a causa del crecimiento significativo de las posibilidades de las comunicaciones electrónicas, los datos relativos al uso de comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en la prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada".

[35] Ibíd.

abultada agenda de medidas políticas y legales para luchar contra el terrorismo internacional. Entre ellas, la aprobación de una regulación comunitaria sobre conservación de datos por los prestadores de servicios de comunicaciones electrónicas pasó a formar parte de las prioridades de la Unión Europea.

La primera línea de actuación al respecto se contiene en un documento de 25 de marzo de 2004 que, bajo el título Declaración del Consejo Europeo sobre la lucha contra el terrorismo[36], fue aprobado en Bruselas como reacción a los atentados terroristas acontecidos en la capital de España apenas diez días antes, frente a los que el Consejo Europeo mostraba tanto su profunda conmoción como "su solidaridad con las víctimas, sus familias y el pueblo español"[37]. La Declaración —que se estructura en quince puntos más un anexo con los Objetivos Estratégicos de la Unión Europea en la Lucha contra el Terrorismo y una Declaración sobre la Solidaridad contra el Terrorismo[38]—. sentó las bases de lo que sería desde entonces la agenda de la Unión Europea en materia de cooperación policial y judicial, y de la que la lucha contra el terrorismo sería uno de los objetivos principales.

Por un lado, la Unión justificaba su interés en esta nueva línea de actuación con el argumento de que la amenaza del terrorismo concernía a los intereses de la Unión Europea en tanto que "los actos de terrorismo atentan contra los valores en que se basa la Unión"[39]. Frente a la misma, la Unión y sus Estados miembros se comprometían desde aquel mismo instante a hacer cuanto estuviera a su alcance para combatir todas

---

[36] El texto íntegro oficial es de difícil acceso, pero puede encontrarse en: http://www.realinstitutoelcano.org/especiales/atentados/docs/declaracterrorUE25304.pdf

[37] Cf. Declaración del Consejo Europeo…, doc. cit., p. 1.

[38] Transcribimos aquí los títulos de estos puntos para dar una cabal idea de su alcance: 1. Introducción; 2. Cláusula de solidaridad; 3. Estrategia Europea de Seguridad; 4. Asistencia a las víctimas; 5. Afianzar la cooperación existente; 6. Reforzar los controles en las fronteras y la seguridad de los documentos; 7. Directrices de la UE para un enfoque común de la lucha contra el terrorismo; 8. Objetivos estratégicos de un plan de acción revisado de la UE para la lucha contra el terrorismo; 9. Intercambio de información; 10. Impedir la financiación del terrorismo; 11. Medidas para la protección del transporte y de la población; 12. Cooperación internacional; 13. Cooperación con los Estados Unidos y otros interlocutores; 14. Creación del cargo de coordinador de la lucha contra el terrorismo; 15. Acciones futuras.

[39] Cf. Declaración del Consejo Europeo…, doc. cit., p. 1.

las formas de terrorismo con arreglo a los principios fundamentales de la Unión, las disposiciones de la Carta de las Naciones Unidas y las obligaciones establecidas por la Resolución 1373 (2001) del Consejo de Seguridad de las Naciones Unidas[40].

Aunque años atrás el Consejo Europeo había adoptado en su reunión de 21 de septiembre de 2001 —esto es, diez días después del atentado de Nueva York— un Plan de acción para la Lucha contra el Terrorismo, que había sido desde entonces completado con diversas iniciativas[41], los ataques en territorio europeo hicieron que estas políticas antiterroristas pasaran a ser, en brevísimo tiempo, una absoluta prioridad[42]. Así queda bien reflejado en la Declaración, que en su quinto punto abordó

---

[40] Ibid.

[41] El texto del Plan está disponible —en lengua inglesa— en: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33275_es.htm

[42] No sólo para la Unión Europea, sino para otros muchos países occidentales. Los efectos legales y constitucionales de las nuevas políticas antiterroristas han sido exhaustivamente examinadas y discutidas en todos los países desarrollados. Entre los estudios españoles y extranjeros más destacables, cabe citar los siguientes: ASHBY WILSON, Richard, Human rights in the "war on terror", Cambridge (Massachussetts), Cambridge University Press, 2005; BALDINI, V., Sicurezza e libertà nello Stato di diritto in trasformazione, Torino, 2005; BENVENISTI, Eyal, "National Courts and the 'War on Terrorism'", en BIANCHI, A., (a cura di), Enforcing International Law Norms Against Terrorism, Oxford, Hart Publishing, 2004, pp. 307 y ss.; HEYMANN, Philip B., "Protecting liberty in an age of terror", Cambridge (Massachussetts), The MIT Press, 2005, pp. 194 y ss.; HOL, Antoine M., VERVAELE, John A.E. (editores), Security and civil liberties: the case of terrorism, Antwerpen, Intersentia, cop. 2005.; HUSABO, Erling / BRUCE, Ingvild, Fighting Terrorism through Multilevel Criminal Legislation, Security Council Resolution 1371, the EU Framework Decision on Combating Terrorism and their Implementation in Nordic, Duthc and German Criminal Law, M. Nijhoff Publishers, Leiden, 2009; MARTÍNEZ CUEVAS, "La suspensión de derechos y libertades por terrorismo en el Reino Unido, Italia, Alemania, Francia y España: su incorporación a la legislación ordinaria con carácter permanente", en Libro homenaje a Luis Portero, Granada, 2001, pp. 515 y ss.; POSNER, Eric / VERMEULE, Adrian, Terror in the Balance: Security, Liberty and the Courts, Oxford University Press, Oxford, 2007; REVENGA SÁNCHEZ, Miguel, "Garantizando la libertad y la seguridad de los ciudadanos en Europa: nobles sueños y pesadillas en la lucha contra el terrorismo", Parlamento y Constitución, Cortes de Castilla la Mancha y Universidad de Castilla la Mancha, n. 10, 2006-2007, pp. 3 y ss.; "The post 9/11 Migration of Britain's Terrorism Act, 2000", en Choudhry, Sujit (editor), The Migration of Constitutional Ideas, Cambridge University Press, Cambridge, 2006, pp. 374 y ss.; "Sources and Trends in Post 9/11 Anti-Terrorism Laws", en Lazurus / Goold (editores), Human Rights and Security, Hart Publishing, Oxford, 2007, p. 227 y ss.; SERRANO-PIEDECASAS FERNÁNDEZ, José

el afianzamiento de la cooperación ya existente indicando que el marco legislativo creado por la Unión para luchar contra el terrorismo, la mejora de la cooperación judicial y la necesidad de que los Estados miembros aplicasen "en su totalidad y de modo eficaz las medidas adoptadas por el Consejo" [43] en los años anteriores desempeñaban un papel decisivo en la lucha contra las actividades terroristas.

Con el objeto de seguir desarrollando tal marco legislativo, el Consejo Europeo encargó al Consejo que estudiara medidas a adoptar en otros sectores, siendo la primera de ellas las "propuestas destinadas a establecer normas sobre la conservación de datos de tráfico de comunicaciones por parte de los proveedores de servicios"[44]. Esta misma es de

---

Ramón, y Demetrio Crespo, Eduardo, "Del Estado de derecho al Estado preventivo", en El cronista del Estado social y democrático de derecho, Iustel, n. 8, noviembre 2009, pp. 24 y ss.; SITAROPOULOS, Nikolaos, "The Role and Limits of the European Court of Human Rights in supervising State Security and anti terrorism measures Affecting alliens' rights", en Elspeth Guild and Anneliesee Baldaccini Editores, Terrorism and the Foreigner, Amsterdam, 2007; SOTTIAUX, Stefan, Terrorism and the limitations of rights: the ECHR and the US Constitution, Oxford, Hart Publishing, 2008; SPITZ, Pierre-Éric, "À propos de la décision du Conseil constitutionnel nº 96-377 DC du 16 juillet 1996 sur la loi tendant à renfoncer la répression du terrorisme", en Revue Française de Droit Administratif (Rfda), nº 3, 1997, pp. 538 y ss.; TORRES DEL MORAL, Antonio, "Libertades públicas y fuerzas de seguridad", en Constitución y seguridad pública: una reflexión a los veinticinco años, Ministerio del Interior, Madrid, 2005, pp. 25 y ss.; WALKER, Walker, Clive, "Keeping Control of Terrorists Without Loosing Control of Constitutionalism", Stanford Law Review, 2007, p. 1395.; WARBRICK, C., "The European response to terrorism in an age of human rights", European Journal of International Law, 15, 2004, pp. 989 y ss.

[43] Cf. Declaración del Consejo Europeo…, doc. cit., punto 5.

[44] Cf. Declaración del Consejo Europeo…, doc. cit., punto 9. La generalidad de estas medidas previstas por la Declaración, destinadas a avanzar el marco legislativo antiterrorista comunitario, tenían un denominador común: la necesidad de conservar la información relevante y de simplificar su intercambio como herramienta de lucha contra el terrorismo. De hecho, el punto nueve de la Declaración —rubricado "intercambio de información"— enunció lo que a nuestro entender podría considerarse el propósito general y más inmediato de la Declaración. En sus propias palabras, el Consejo Europeo, al tiempo que destacaba "la importancia de una cooperación más eficaz en materia de información analítica y una mejor evaluación de la amenaza", invitaba a los Estados miembros a "mejorar los mecanismos de cooperación y fomentar la colaboración sistemática y efectiva entre los servicios de Policía, de seguridad y de información". Esta preocupación por mejorar la obtención e intercambio de información relevante está presente en otros muchos puntos del documento. Así, bajo la rúbrica de Optimizar la eficacia de los sistemas de información, el apartado c) del punto quinto recogió la petición del Consejo Europeo a la Comisión para que presentara propuestas para aumentar la interoperabilidad entre las bases de datos

hecho la que acaparaba mayor interés por parte del órgano, que advertía explícitamente, en el mismo lugar, que debía "darse prioridad a las propuestas relativas a la conservación de datos de tráfico de comunicaciones y al intercambio de información sobre condenas, con vistas a que estén adoptadas en junio de 2005" [45].

El hecho de que el texto se refiera en todo momento a "propuestas relativas a la conservación" o a "propuestas destinadas a establecer normas sobre la conservación", sin mencionar qué tipo de norma habría de emplearse, pone de manifiesto que, al tiempo de redactar la Declaración, el Consejo no tenía aún claro cuál había de ser el concreto instrumento jurídico a través del cual materializar la medida de conservación.

No obstante, la previsión expuesta se materializó en un primer pero malogrado intento. El 28 de abril de 2004 cuatro Estados miembros —Francia, Irlanda, Reino Unido y Suecia— firmaron un Proyecto de Iniciativa con vistas a la adopción por el Consejo de una Decisión marco sobre la conservación de los datos tratados y almacenados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o el suministro de datos en redes públicas de comunicaciones a efectos de la prevención, investigación, descubrimiento y represión de la delincuencia y de las infracciones penales, con inclusión del terrorismo[46]. La Propuesta fue rechazada por el Parlamento Europeo, que en aquel momento manifestó serias dudas sobre el

---

europeas y estudiara la creación de sinergias entre sistemas de información existentes y futuros para aprovechar el valor añadido que aportan, en sus respectivos marcos jurídicos y técnicos, a la prevención y lucha contra el terrorismo. El Consejo Europeo invitaba asimismo a la Comisión a presentar al Consejo Europeo de junio propuestas relativas al intercambio de información personal —nominatim, ADN, impresiones dactilares y datos de visados— a efectos de la lucha contra el terrorismo . Las propuestas de la Comisión también debían incluir disposiciones para facilitar el acceso de los servicios policiales nacionales a los sistemas de la Unión Europea.

[45] Cf. Declaración del Consejo Europeo…, doc. cit., punto 5.

[46] El título completo del documento era Proyecto de Decisión marco sobre la conservación de los datos tratados y almacenados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o el suministro de datos en redes públicas de comunicaciones a efectos de la prevención, investigación, descubrimiento y represión de la delincuencia y de las infracciones penales, con inclusión del terrorismo, presentada por la República Francesa, Irlanda, el Reino de Suecia y el Reino Unido el 28 de abril de 2004 (CNS/2004/0813). El texto íntegro en su publicación oficial es accesible en el siguiente enlace: http://register.consilium.eu.int/pdf/es/04/st08/st08958.es04.pdf

fundamento jurídico, la proporcionalidad de la disposición y la eventual vulneración del art. 8 CEDH[47].

El fracaso de este primer intento no disminuyó el interés del Consejo por adoptar la medida de conservación, como demuestra el que, pocos meses después, el 14 de junio de 2004, el asunto fuera estudiado por una mesa redonda *ad hoc*, bajo los auspicios del Foro para la prevención de la delincuencia organizada, en la que participaron representantes de las autoridades policiales, de la industria y de las organizaciones de protección de datos. Asimismo, el 30 de julio de 2004, la Dirección General de Sociedad de la Información y Medios de Comunicación y la Dirección General de Justicia, Libertad y Seguridad presentaron conjuntamente un documento sobre la conservación de los datos de tráfico como preparación a un taller público sobre la materia, que fue celebrado el 21 de septiembre de 2004 y, con motivo del cual la Comisión recibió diversas aportaciones, en especial, de la industria y de asociaciones de derechos civiles[48].

Pese a todo, lo cierto es que a la vuelta de un año la normativa sobre conservación de datos aún no había sido aprobada. No es de extrañar, por tanto, que en una posterior reunión del Consejo Europeo —celebrada en Bruselas el 16 y 17 de junio de 2005[49]—, el órgano se viera obligado a otorgar a tales políticas atención especial y renovado impulso, como puede comprobarse en las Conclusiones emitidas por la Presidencia con ocasión de esta reunión[50]. Si bien en su Bloque III el Consejo acogía "con satisfacción los avances legislativos realizados en los ámbitos del intercambio de información

---

[47] Cf. Dictamen del CESE…, doc. cit., punto 2.1.6.

[48] Sobre todas estas iniciativas y sus resultados, cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 4.

[49] Puede accederse al texto íntegro oficial de esta Declaración en el siguiente enlace: http://ue.eu.int/ueDocs/cms_Data/docs/pressData/es/ec/85347.pdf

[50] Las materias de la Declaración se agrupaban en los siguientes cinco bloques: I. Perspectivas financieras, II. Cuestiones económicas, sociales y medioambientales (estrategia de Lisboa; desarrollo sostenible), III. Espacio de libertad, seguridad y justicia, IV. Relaciones exteriores, y V. Varios. Conclusiones de la Presidencia con motivo del Consejo Europeo de Bruselas, de 16 y 17 de junio de 2005, punto 2.

judicial y policial"[51], no dejaba de insistir en la urgencia de que se realizaran avances en todos los ámbitos del Plan de Acción para la lucha contra el terrorismo, en particular por lo que se refería a los plazos de entrada en vigor de aquellas medidas consideradas prioritarias para la eficacia de la lucha contra el terrorismo que había aprobado el Consejo Europeo de marzo de 2004[52], en los términos ya expuestos. Quizás para acentuar su importancia, el Consejo decidió recoger en el punto 19 aquellos aspectos que en concreto deseaba se abordasen *con carácter prioritario* durante el segundo semestre de 2005. Entre todos los trabajos legislativos pendientes destinados a reforzar la cooperación policial y judicial —cooperación aduanera, intercambio de informaciones entre autoridades policiales, al exhorto de obtención de pruebas, etc.— el documento hacía expresa referencia a la "retención de datos sobre tráfico de telecomunicaciones"[53].

El llamamiento a acelerar la tramitación de toda la panoplia de propuestas legislativas y políticas de seguridad que había empezado a rodar un año antes se vio dramáticamente impulsado como consecuencia de los atentados ocurridos en Londres el 7 de julio de 2005. La respuesta europea a los mismos se condensa en el documento emitido en su Sesión Extraordinaria por el Consejo, Justicia y Asuntos de Interior, que tuvo lugar en Bruselas el 13 de julio de 2005, y que llevó por título Declaración del Consejo Europeo sobre la Respuesta de la Unión Europea a los Atentados de Londres, de 13 de julio de 2005[54]. La declaración expresaba que la "prioridad inmediata" del Consejo era "mejorar el sólido marco ya existente en la UE para perseguir e investigar a los terroristas a través de las fronteras, con objeto de impedir sus planes, desmantelar sus

---

[51] Cf. Declaración del Consejo Europeo (junio 2005)…, doc. cit., punto 17.

[52] Ibíd., punto 18.

[53] Ibíd., punto 19. En segundo lugar —y como consecuencia de lo anterior—, la prosecución de los esfuerzos por compartir mejor "la información estratégica y operativa entre los Estados miembros y entre éstos y las agencias y servicios competentes de la Unión, de conformidad con el Programa de La Haya.

[54] La Declaración se desglosa en diez puntos, y encabezados por la condena por parte del Consejo de la Unión Europea, de los atentados terroristas acaecidos, remarcando que el órgano reforzaba "su compromiso de lucha contra el terrorismo y defensa de los principios fundamentales de libertad, seguridad y justicia. El texto íntegro oficial fue publicado mediante comunicado de prensa (11116/05, Presse 187) y está disponible en http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/es/jha/85826.pdf.

redes de apoyo, suprimir toda financiación y llevarlos ante la justicia"[55], incluyendo seguidamente un conjunto de medidas en materia de recogida e intercambio de información que el Consejo de la Unión Europea y los Estados miembros habían de aprobar[56]. Entre las primeras, el Consejo se comprometía concretamente a adoptar una decisión marco sobre la retención de datos de telecomunicaciones antes de octubre de 2005[57]. Como puede apreciarse, el Consejo optaba ya expresamente por el empleo de una decisión marco, a pesar de que un año antes la propuesta presentada por Francia, Irlanda, Reino Unido y Suecia no había prosperado.

En cualquier caso, la tensión acumulada en el seno de la Unión, la alarma generada en la opinión pública y los trabajos precedentes en este marco de declaraciones políticas y medidas legislativas antiterroristas, hicieron que pocos meses después —el 21 de septiembre de 2005— la Comisión tomara la iniciativa y presentara una Propuesta de Directiva de la Comisión Europea sobre conservación de datos del tráfico[58]. El texto

---

[55] Cf. Declaración del Consejo Europeo (junio 2005)…, doc. cit., punto 4.

[56] A saber: intensificar el intercambio de información policial y judicial, en particular por medio de Europol —y su Unidad Operativa de Lucha Antiterrorista— y de Eurojust, así como mejorar el intercambio de información sobre explosivos perdidos y robados, entre otros puntos.

[57] Cf. Declaración del Consejo Europeo (julio 2005)…, doc. cit., punto 4. Las otras decisiones marco a adoptar eran las siguientes: el exhorto europeo de obtención de pruebas —diciembre de 2005 —; tomó forma años después, a través de la Decisión Marco 2008/978/JAI del Consejo, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal (DO L 350 de 30.12.08). el intercambio de información entre los cuerpos de seguridad —diciembre de 2005 —; y, La medida fue concretada a través de la Decisión Marco 2006/960/JAI, de 18 de diciembre, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (DO L 386, 29/12/2006), incorporada al Derecho español a través de la Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (BOE núm. 182 de 28 de julio de 2010).- el intercambio de información relativa a delitos de terrorismo —septiembre de 2005—. La previsión fue provista a través de la Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (DO L 386, 29/12/2006).

[58] El título oficial y completo del documento es Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de

propuesto —cuyo responsable y ponente fue Franco FRATTINI[59]— constaba de trece artículos más un anexo en el que se listaban las categorías de datos electrónicos susceptibles de ser conservados, y que posteriormente pasó a integrarse en el articulado. A pesar de que, como hemos visto, una directiva no era el instrumento que se había previsto en la Declaración en respuesta a los atentados de Londres, el Consejo abrazó la iniciativa en su sesión de los días 1 y 2 de diciembre de 2005, abandonando la idea de la decisión marco. Por su parte, el 14 de diciembre de 2005 el Parlamento emitió su dictamen con arreglo al procedimiento de codecisión establecido en el artículo 251 TCE. Dos meses más tarde, en su sesión de 21 de febrero de 2006, el Consejo adoptó por mayoría cualificada la Propuesta[60] que, tras una difícil tramitación, fue finalmente aprobada el 15 de marzo de 2006. Se trata de la hoy vigente Directiva 2006/24/CE del Parlamento europeo 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 comunicaciones y por la que se modifica la Directiva 2002/58/CE[61].

Al estudio de esta norma dedicaremos la Primera Parte de esta Tesis, empezando por analizar su base jurídica en el siguiente apartado.

---

comunicación electrónica y por la que se modifica la Directiva 2002/58/CE. {SEC(2005) 1131}. Bruselas, 21.9.2005, COM(2005) 438 final 2005/0182 (COD).

[59] Franco Frattini (Roma, 1957) fue Vicepresidente de la Comisión Europea y Comisario de Seguridad, Libertad y Justicia desde 2004 a 2008. Entre 2008 y 2011 desempeñó el cargo de Ministro de Asuntos Exteriores de Italia con el Gobierno de Silvio Berlusconi. En la actualidad ejerce como Diputado de la República en la *Camera dei Deputati*. Acerca de su currículum y actividad en la actualidad puede consultarse: http://www.francofrattinidiarioitaliano.blogspot.com/ (página web oficial).

[60] Irlanda y la República Eslovaca votaron en contra de su adopción.

[61] Publicada oficialmente en DO L 105 de 13.4.2006, pág. 54. Accesible en: http://eur-lex.europa.eu/LexUriServ/site/es/oj/2006/l_105/l_10520060413es00540063.pdf

2 Base jurídica de la DCD

En el momento histórico en que la Unión Europea se decide a introducir una normativa a nivel comunitario de la medida de conservación de datos de las comunicaciones electrónicas con fines penales, una regulación eficiente de la materia comprendía la armonización de seis concretos aspectos:

- — determinación de las categorías de datos que debían conservarse;
- — determinación de los períodos de conservación de los datos;
- — establecimiento de normas de protección y seguridad de los datos almacenados;
- — designación de las autoridades nacionales con competencia para acceder a los datos;
- — delimitación de los delitos cuya represión justificaba tal acceso; y,
- — establecimiento de normas sobre el intercambio de estos datos entre las autoridades nacionales.

Por los motivos que a continuación expondremos, la distribución de competencias en el seno de las Comunidades de acuerdo con la legislación entonces vigente hacía imposible armonizar todos estos elementos en un único instrumento jurídico.

Por un lado, los tres primeros elementos mencionados —categorías de datos a conservar, períodos de conservación y normas de protección y seguridad de los datos almacenados—- son aspectos que afectan directamente a la actividad de los proveedores de servicios. Tales elementos sólo podían ser regulados mediante un instrumento basado en el Primer Pilar —o sea, del TCE, como vg. una directiva o un reglamento—, pues éste otorgaba competencias a la Comunidad Europea para legislar sobre la protección de datos personales y los servicios de telecomunicaciones para garantizar el funcionamiento del mercado único.

Sin embargo, por otra parte, la determinación de las autoridades que podían acceder a los datos conservados, de los delitos cuya persecución justificaba el acceso, y de las condiciones de intercambio de información entre autoridades son cuestiones que sólo podían regularse mediante un instrumento basado en el TUE, es decir, en el Tercer Pilar —como vg. una decisión marco—, pues suponía establecer normas acerca de la

actividad y competencias de las autoridades represivas de los Estados miembros, una categoría que caía dentro de la cooperación policial y judicial comprendida en este Pilar.

Concretamente, la competencia de la Comunidad Europea para regular los tres primeros aspectos venía dada por el art. 95 TCE, conforme al cual el Consejo podía adoptar medidas relativas a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que tuvieran por objeto el establecimiento y el funcionamiento del mercado interior —cf. art. 95.1 TCE—. El legislador comunitario estaba así facultado para recurrir a una directiva o a un reglamento con el fin de eliminar las disparidades entre las regulaciones nacionales, cuando tales disparidades pudieran obstaculizar el ejercicio de las libertades fundamentales o crear distorsiones de la competencia, afectando por ello directamente al funcionamiento del mercado interior[62], o bien para evitar la aparición de futuros obstáculos a los intercambios comerciales derivados de la evolución heterogénea de las legislaciones nacionales, siempre que la aparición de tales obstáculos fuera probable y la medida de que se tratase tuviera por objeto su prevención[63]. Éste era el caso de las categorías de datos que debían conservarse, el período de conservación de esos datos, y las normas de protección y seguridad de los datos almacenados —los tres primeros elementos listados—.

Como explican los considerandos quinto y sexto de la DCD, a consecuencia de los atentados terroristas, varios Estados miembros, entendiendo que los datos sobre las comunicaciones electrónicas eran un medio eficaz para detectar y reprimir las infracciones penales, incluido el terrorismo, habían adoptado unilateralmente medidas para imponer a los prestadores de servicios obligaciones relativas a la conservación de tales datos. Tales normativas habían dado lugar a importantes diferencias legales y técnicas entre las disposiciones nacionales sobre conservación de datos por los prestadores de servicios, especialmente en lo que se refiere a la naturaleza de los datos

[62] Véase, en este sentido, la sentencia de 12 de diciembre de 2006, Alemania/Parlamento y Consejo, C 380/03, Rec. p. I 11573, apartado 37 y jurisprudencia citada

[63] Sentencia Alemania/Parlamento y Consejo, antes citada, apartado 38 y jurisprudencia citada

conservados y a su período de conservación. Las obligaciones relativas a la conservación de los datos tenían implicaciones económicas sustanciales para los prestadores de servicios, en la medida en que conllevaban importantes inversiones y costes de explotación. Era previsible además que los Estados miembros que todavía no habían adoptado una normativa en materia de conservación de datos introdujeran en esta materia normas que podrían incrementar aún más las disparidades entre las distintas medidas nacionales existentes. Todas estas diferencias entre las distintas legislaciones nacionales reguladoras de la conservación de los datos de las comunicaciones electrónicas afectaban directamente al funcionamiento del mercado interior. Era además previsible que esta situación se fuera agravando.

A la vista de estos argumentos, el legislador comunitario estaba legitimado para adoptar normas armonizadoras con objeto de proteger el buen funcionamiento del mercado interior. La armonización podía extenderse a determinar las categorías de datos que debían conservarse, los períodos de conservación de los datos y la protección y seguridad de los datos almacenados, pues todos estos aspectos se refieren directa y estrictamente a la actividad económica de los proveedores de servicios de comunicaciones electrónicas, un ámbito que la Comunidad podía regular sin problema.

Sin embargo, la determinación de qué delitos justifican el acceso a los datos, qué autoridades nacionales podían acceder a los mismos o bajo qué circunstancias podían intercambiar información sobre ellos comportaba armonizar las legislaciones penales y procesales de los Estados miembros, una competencia que caía fuera del ámbito del art. 95 TCE y, por tanto, del Derecho comunitario. La cooperación policial y judicial en materia penal no se encontraba entre los fines y competencias de la Comunidad Europea, tal como eran descritos en el TCE —arts. 2 y 3.1.h) TCE—, por lo que tales materias no podían en consecuencia ser objeto de una directiva o un reglamento.

De hecho, la política exterior y de seguridad común y la prevención y la lucha contra la delincuencia fueron incluidos entre los objetivos de la Unión Europea por el art. 2 TUE, que introdujo un Título VI sobre *Disposiciones relativas a la cooperación policial y judicial en materia penal*, por el que los Estados miembros se comprometían a la adopción progresiva de medidas que establecieran normas mínimas relativas a los

elementos constitutivos de los delitos y a las penas en los ámbitos de la delincuencia organizada, el terrorismo y el tráfico ilícito de drogas —art. 31 TUE—. A iniciativa de cualquier Estado miembro o de la Comisión, el Consejo podía, por unanimidad, adoptar decisiones marco para la aproximación de las disposiciones legales y reglamentarias de los Estados miembros —art. 32.1.b) TUE—.

Así pues, desde el punto de vista del Tercer Pilar, una decisión-marco del Consejo —basada en el TUE— era adecuada para llevar a cabo una armonización de legislaciones penales y procesales sobre la conservación de datos en todo lo que se refería al acceso y explotación de los datos —delitos, autoridades y las condiciones de intercambio—. Sin embargo, la medida del Tercer Pilar no podía a su vez regular las categorías de datos, su protección o los plazos de conservación. Estos aspectos se refieren a la actividad de los prestadores de servicio, cuya regulación ya había sido tratada por una medida del Primer Pilar, en concreto, la meritada Directiva 2002/58/CE[64] —que se adoptó sobre la base del art. 95 TCE—. Las modificaciones y excepciones que la DCD lleva a cabo sobre la Directiva 2002/58/CE sólo podían efectuarse debidamente mediante un acto comunitario con la misma base jurídica. Conforme con el art. 47 TUE, que regulaba la relación entre el TUE y el TCE, ningún instrumento jurídico adoptado de conformidad con el TUE podía afectar al marco legislativo adoptado con arreglo al TCE[65]. Al establecer que ninguna disposición del TUE afectaría a los Tratados constitutivos de la Comunidad Europea ni a los Tratados y actos subsiguientes que los hayan modificado o completado, el art. 47 TUE pretendía conforme a lo dispuesto en los arts. 2.5 y 3.1 TUE mantener y desarrollar el acervo comunitario[66]. Sólo el legislador comunitario era competente para modificar las obligaciones impuestas por una directiva basada en el TCE. Ni los artículos 30, 31.1.c) y 34.2.b) TUE, ni ningún otro artículo del TUE podían

[64] De hecho —y de acuerdo con el análisis realizado por los documentos preparatorios de la Propuesta— "fue solamente porque no pudo alcanzarse ningún acuerdo político sobre el alcance efectivo de la conservación que esta cuestión no había sido objeto de mayor armonización ya en la Directiva 2002/58/CE". Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 8.

[65] Esta exigencia figuraba también en el párrafo primero del art. 29 TUE, que introduce el Título VI de este último Tratado, bajo el epígrafe de "Disposiciones relativas a la cooperación policial y judicial en materia penal".

[66] Sentencia de 20 de mayo de 2008, Comisión/Consejo, C-91/05, Rec. p. I-0000, apartado 59

servir de fundamento a una normativa que, en relación con las categorías de datos que han de conservarse por los prestadores de servicios y el período de conservación de estos datos, modificase las obligaciones impuestas al ejercicio de las actividades de los prestadores de servicios por la Directiva 2002/58 o estableciera —como hace la DCD— no aplicarles el régimen establecido por la Directiva 2002/58. Puesto que la modificación de la Directiva 2002/58 era competencia de la Comunidad, la regulación de estos aspectos no podía basarse en una disposición del TUE sin vulnerar su art. 47[67].

En consecuencia, el intento de regular la conservación de datos a través de una medida del Tercer Pilar debe reputarse a nuestro entender como ilegal. La iniciativa presentada al Consejo el 28 de abril de 2004 por Francia, Irlanda, Suecia y Reino Unido con vistas a la adopción de una decisión marco[68] tenía su base en el artículo 31.1.c) TUE, pero contenía disposiciones complementarias tanto sobre el acceso a los datos retenidos como sobre peticiones de acceso de otros Estados miembros[69]. Obviamente, el art. 47 TUE no permitía que un acto fundado en el mismo modificara el acervo

---

[67] Ibíd., apartado 33 y jurisprudencia citada. De hecho, corresponde al Tribunal de Justicia de la Unión velar por que los actos que, según una de las partes, están comprendidos en el ámbito de aplicación del Título VI del TUE y que, por su naturaleza, pueden producir efectos jurídicos no invadan las competencias que las disposiciones del TCE atribuyen a la Comunidad.

[68] La base jurídica de la norma se fundaba, por un lado, en el art. 31.1.c) TUE, que establece que la acción en común sobre cooperación judicial en materia penal incluirá -entre otras- la consecución de la compatibilidad de las normas aplicables en los Estados miembros, en la medida necesaria para mejorar dicha cooperación, y por otro, en el art. 34.2.b) TUE, conforme al cual, a iniciativa de cualquier Estado miembro o de la Comisión, el Consejo podrá, por unanimidad adoptar decisiones marco para la aproximación de las disposiciones legales y reglamentarias de los Estados miembros. Indicaba a renglón seguido el epígrafe que las decisiones marco no tendrán efecto directo y obligarán a los Estados miembros en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios.

[69] Como explica el punto 3 de la Exposición de Motivos de la Propuesta de Directiva, doc. cit., la propuesta se limita a lo que los Estados miembros "no pueden lograr satisfactoriamente y lo que la Unión hace mejor, y restringe el alcance de las obligaciones de conservación de los proveedores de servicios de comunicaciones electrónicas o de una red de comunicaciones de acceso público. La propuesta deja a los Estados miembros la elección de las autoridades que deben tener acceso a los datos conservados y en qué condiciones". El acceso a la información y su intercambio entre las autoridades represivas correspondientes es una cuestión que queda fuera del ámbito del TCE.

comunitario, en este caso, a las Directivas 95/46/CE y 2002/58. Así, al determinar en una decisión marco las categorías de datos que debían conservarse y la duración de los períodos de conservación, el Consejo se estaba arrogando la regulación de materias que eran competencia del legislador comunitario. Así lo apreció la propia Comisión, que respondiendo a la presentación de esta iniciativa, advirtió que se reservaba el derecho de presentar una propuesta de directiva fundada en estos argumentos, cosa que hizo el 21 de septiembre de 2005 y que, finalmente, daría lugar a la vigente DCD[70].

Así las cosas, la Unión se encontraba en una disyuntiva: o bien optaba por aprobar una medida del Primer Pilar —renunciando a regular el acceso y explotación de los datos— o bien una medida del Tercer Pilar —renunciando a armonizar las condiciones de conservación para los proveedores—. La acción de la UE se inclinó finalmente por una medida del Primer Pilar, lo que a su vez exigía elegir entre el empleo o de una directiva o de un reglamento. Entre ambos instrumentos, la Comisión se inclinó por la directiva ya que, en sus propias palabras, "comparada con un reglamento, [la directiva deja] en un área sensible un cierto margen de maniobra a los Estados miembros en la aplicación. Un reglamento sería demasiado riguroso, especialmente teniendo en cuenta las diversas arquitecturas técnicas utilizadas por los distintos operadores en los diferentes países. La directiva dejará suficiente margen a los Estados miembros para adaptarse a las exigencias nacionales"[71].

En todo caso, el optar por un instrumento del Primer Pilar supuso que sus disposiciones necesariamente tuvieron que limitarse a armonizar las actividades de los prestadores de servicios, de manera que las disposiciones de la DCD abordan la aproximación de las legislaciones nacionales respecto esencialmente a las actividades de los prestadores de servicios en el sector afectado del mercado interior, en concreto: la obligación de conservar datos —art. 3 DCD—, las categorías de datos que deben conservarse —art. 5 DCD—, los períodos de conservación de los datos —art. 6—, la protección y seguridad

[70] El Consejo, en lugar de seguir adelante con la adopción de una decisión marco, adoptó la Propuesta de Directiva en su sesión de 1 y 2 de diciembre de 2005.

[71] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 5.

de los datos —art. 7 DCD—, y los requisitos de almacenamiento de éstos —art. 8 DCD—.

De este modo, "la presente Directiva —advierte el considerando vigésimo quinto de la DCD— se entiende sin perjuicio de la facultad de los Estados miembros para adoptar medidas legislativas relativas al derecho de acceso y de utilización de los datos por parte de las autoridades nacionales tal como determinen los mismos". Además, el art. 3 DCD prevé que los prestadores de servicios sólo deben conservar los datos generados o tratados durante la prestación de los servicios de comunicación de que se trate. Estos datos son tan sólo los que están estrechamente ligados al ejercicio de la actividad comercial de estos prestadores. La DCD regula operaciones que son independientes de la aplicación de toda posible acción de cooperación policial y judicial en materia penal. Tales acciones, como son el acceso a los datos, la explotación de éstos por las autoridades policiales o judiciales de los Estados miembros y el intercambio de información entre las autoridades represivas, son cuestiones que quedaban comprendidas, en principio, en el ámbito de aplicación del título VI del TUE y fuera del ámbito del TCE[72], y, por tanto, no podían armonizarse, como advierte el vigésimo quinto considerando y el art. 4 DCD.

De todos modos, y a pesar de estas limitaciones, la acción comunitaria lograría la parte más importante de sus objetivos, asegurando que los datos de tráfico se conservasen en toda la Unión Europea y pudieran ponerse a disposición de las autoridades represivas en igualdad de condiciones. Esto, simultáneamente, beneficiaría también a la industria de las comunicaciones electrónicas, especialmente para aquellas empresas que ofreciesen servicios en múltiples Estados miembros[73].

Tras la adopción de la DCD su base jurídica fue recurrida ante el Tribunal de Justicia por la República de Irlanda, recurso que dio lugar a la Sentencia del Tribunal de

[72] En este contexto, no puede dejar de señalarse que, al tiempo de la tramitación de la Directiva, la Comisión estaba preparando proyectos de propuestas legislativas basadas en el Tratado de la Unión Europea relativas al principio de disponibilidad de la información con el fin de reprimir actividades ilícitas y al establecimiento de principios de protección de los datos en el marco del Tercer Pilar.

[73] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 7.

Justicia (Gran Sala) de 10 de febrero de 2009, Irlanda contra Parlamento Europeo y Consejo de la Unión Europea, asunto C-301/06[74].

De acuerdo con el planteamineto del recurrente, para que una medida fundada en el art. 95 TCE sea válida, debe tener por "centro de gravedad" la aproximación de las legislaciones nacionales con objeto de mejorar el funcionamiento del mercado interior[75]. Irlanda alegó que ni el art. 95 TCE ni ninguna otra de las disposiciones del TCE podían proporcionar una base jurídica apropiada para una Directiva cuyo "único objetivo o, al menos, el objetivo principal o predominante de dicha Directiva es facilitar la investigación, detección y enjuiciamiento de infracciones penales"[76]. Tal norma no podía ser adoptada en el marco de las competencias de la Comunidad, ya que la prevención de las distorsiones o de los obstáculos al mercado interior en el caso de la DCD era un objetivo meramente secundario respecto del objetivo principal o predominante, que consiste en la represión de la delincuencia. La Directiva tiene por objeto armonizar la conservación de los datos más allá de los objetivos comerciales, con el fin de facilitar la acción de los Estados miembros para la represión de las infracciones penales, como demuestra el examen de los considerandos, particularmente del séptimo al undécimo y del vigésimo primero, y de las disposiciones fundamentales de la Directiva 2006/24, en particular de su art. 1.1[77].

Refutando estos argumentos, el Tribunal de Justicia de la Unión Europea basó su fallo favorable a la legalidad de la Directiva 2006/24/CE en diversos argumentos, empezando por advertir que, aun cuando la necesidad de reprimir la delincuencia, incluido el terrorismo, fue un factor determinante en la decisión de adoptar una directiva que modifica el alcance de los derechos y obligaciones establecidos en los artículos 5, 6 y 9 de la Directiva 2002/58, la importancia concedida a la represión de la

---

[74] Texto completo de la Sentencia disponible en la base de datos oficial del Tribunal de Justicia: http://curia.europa.eu/juris/liste.jsf?language=es&num=C-301/06.

[75] Véase, en particular, la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión, C 317/04 y C 318/04, Rec. I 4721

[76] Cf. Sentencia del Tribunal de Justicia (Gran Sala) de 10 de febrero de 2009, asunto C- 301/06, p. 28.

[77] Ibíd., p. 29.

delincuencia no desvirtúa la elección del artículo 95 TCE[78]. El objetivo de la represión de las infracciones penales no es ni el único objetivo de dicha directiva ni tan siquiera su objetivo preponderante.

El Tribunal se fijó en la existencia de una previa normativa interna de algunos Estados miembros sobre la materia que podía hacer peligrar la unidad y estabilidad del mercado único de las comunicaciones electrónicas, así como que la posibilidad de que otros Estados procedieran igualmente a su regulación interna acrecentaba aún más dicho riesgo de dispersión normativa, que ya alcanzaba a los datos objeto de previa conservación y a los períodos de duración. Esto hacía que, lo que otrora pudiera plantearse como cuestión de oportunidad, se considerase ahora una cuestión de auténtica necesidad[79]. En este sentido, era evidente para el Tribunal que la directiva tenía una incidencia directa sobre las actividades económicas de los prestadores de servicios y podía, por tanto, contribuir al establecimiento y funcionamiento del mercado interior. De hecho, la Directiva armoniza las disposiciones nacionales relativas a la conservación de ciertos datos por las empresas privadas, en el ámbito de su actividad económica ordinaria. Si el legislador comunitario no hubiera intervenido podría haberse producido una distorsión de la competencia en ese mercado interior[80].

A este argumento se unía la constatación de que la Directiva no hacía sino desarrollar una directiva previa, la 2002/58/CE, plenamente asentada en el art. 95 del Tratado, al centrarse en la protección de la privacidad en el ámbito de las comunicaciones electrónicas; así como en que los destinatarios directos de la norma no eran tanto las autoridades públicas que pudieran hacer uso de las informaciones contenidas en las bases de datos como las operadoras de telecomunicaciones sometidas al deber de conservación[81].

El Tribunal sostuvo, además, que la DCD regula operaciones que son independientes de la ejecución de cualquier cooperación policial y judicial en materia penal, y que no

[78] Ibíd., p. 37.

[79] Ibíd., p. 67.

[80] Ibíd., p. 72.

[81] Ibíd., p. 80.

armonizaba ni el acceso a los datos por parte de las autoridades nacionales competentes, ni la utilización y el intercambio de esos datos entre dichas autoridades[82]. Teniendo en cuenta además que la norma se dirige esencialmente a las actividades de los operadores en el sector pertinente del mercado interior, la conclusión no podía ser otra para el Tribunal que el que la base jurídica de la Directiva resultaba legal y conforme al Derecho de la Unión[83].

No obstante este resultado, es fácil colegir cómo la intención del legislador comunitario iba más allá de imponer unas normas de mínimos sobre las que garantizar la igualdad de condiciones en el establecimiento de un operador de telecomunicaciones en el espacio económico europeo. Como ha señalado RODRÍGUEZ LAINZ, aunque "era cierto que se hacía precisa una previa armonización en lo referente a la unidad en el mercado de las telecomunicaciones, para así evitar que en unos Estados se sometiera a las operadoras de telecomunicaciones a costosísimos deberes de conservación de datos no exigidos en otros […], la Directiva no pudo evitar la tentación de inmiscuirse indirectamente en el tercer pilar, al forzar a sus destinatarios a regular sobre una materia tan delicada sobre la que en no pocos Estados no había aún una decidida voluntad de regulación"[84].

La definitiva entrada en vigor del Tratado de Lisboa podría hacernos pensar que al menos esta segunda dimensión de la normativa común sobre conservación de datos podría salvar el difícil escollo de los instrumentos normativos del ya desaparecido tercer pilar. La materia referente al llamado Espacio Europeo de libertad, seguridad y justicia —arts. 82 a 86 del Tratado de Funcionamiento de la Unión Europea— pasa a tener como instrumentos normativos los correspondientes al procedimiento ordinario; en concreto, se prevé que por simples directivas puedan regularse acercamientos de legislaciones internas en materia de proceso penal y la admisibilidad mutua de pruebas, aunque con posibilidad de dar lugar a una cooperación reforzada en caso de reticencias

[82] Ibíd., p. 83.

[83] Ibíd. , p. 84.

[84] Cf. Rodríguez Lainz, J. L., Reflexiones en torno al informe de evaluación sobre la Directiva de conservación de datos, Diario La Ley, Nº 7706, Sección Doctrina, 30 Sep. 2011, Año XXXII, Ref. D-362, Editorial La Ley, p. 3.

por parte de algún Estado miembro. Sin embargo, la línea apuntada por el Informe de Evaluación de la Comisión —del que hablaremos ampliamente en posteriores capítulos— se ha mantenido dentro de la misma esfera del mercado único y de la protección de los consumidores.

3 Elaboración y tramitación de la DCD

La elaboración de la proyecto de directiva por la Comisión se basó en gran medida —como no podía ser de otra manera— en el amplio debate que había ido desarrollándose en los años anteriores sobre la cuestión, buena parte de cuyos aspectos hemos dado ya cuenta en el anterior apartado.

Con anterioridad a la redacción de la PDCD, la Comisión llevó a cabo un largo proceso de consultas entre los sujetos directamente afectados por la norma, con particular atención a las autoridades represivas, las compañías de telecomunicaciones y las agencias de protección de datos[85]. Ya en esta primera fase quedaron patentes los tres intereses en liza que, desde entonces, rodean el debate en torno a la DCD, a saber: la eficacia policial, el derecho fundamental a la intimidad y los costes económicos para las compañías de telecomunicaciones.

Siguiendo el relato de hechos que hace la Exposición de Motivos de la PDCD acerca de este período, estas primeras consultas pusieron de manifiesto, en primer lugar, el gran interés de las fuerzas y cuerpos policiales en la aprobación de la normativa, en tanto que la conservación de los datos de las comunicaciones se presentaba como una "una herramienta esencial para que las autoridades represivas prevengan y combatan la delincuencia y el terrorismo"[86]. A mayor abundamiento, las autoridades policiales insistieron en la necesidad de que la conservación se extendiera por el tiempo y respecto de los datos necesarios para las investigaciones complejas de delitos graves —que pueden prolongarse durante varios años—, en apoyo de lo cual aportaron ejemplos

[85] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 5.

[86] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 4.

de casos en los que tales datos habían resultado ser esenciales para investigaciones criminales en delitos como atentados con bombas o asesinatos[87].

Por su parte, los portavoces de las organizaciones europeas representativas del sector de las telecomunicaciones y de la industria de internet manifestaron su buena disposición a cooperar con los servicios policiales —como, al parecer, venían haciendo desde antes—, si bien insistieron a la Comisión en que un período de conservación largo generaría costes considerables que habrían de ser afrontados por las propias compañías[88]. Los dos caballos de batalla del sector en los debates posteriores quedaron así perfectamente delineados en esta etapa: por un lado, las empresas abogaban por períodos de conservación no superiores a seis meses, argumentando que, en la práctica, los datos que los servicios represivos solicitaban no sobrepasaban los seis meses de antigüedad; por otro, era de su máximo interés el que se arbitraran por parte de la Unión mecanismos a favor del sector para reemborsarles los costes adicionales generados por la regulación[89].

Finalmente, en una tercera posición, los representantes de las autoridades de protección de datos y las asociaciones de derechos civiles alegaron que la conservación de los datos suponía una interferencia en la vida privada de los ciudadanos, por lo que los períodos de conservación debían ser lo más breves posible. En concreto, cuestionaron la proporcionalidad de los períodos de conservación superiores a seis meses y expresaron su preocupación por la finalidad y los objetivos de la conservación, que a su entender habían de especificarse con total claridad[90].

Estos tres frentes establecidos con ocasión de las consultas previas tendrían ocasión de ser reabiertos tras la fijación del texto de la Propuesta, que se sometió al dictamen de los organismos comunitarios interesados —tal como prevé el procedimiento legislativo europeo—, así como a las alegaciones de otros sujetos implicados.

---

[87] Ibíd.

[88] Ibíd.

[89] Ibíd.

[90] Ibíd.

Conviene advertir que, en atención a todo lo alegado por las distintas partes implicadas, la Propuesta elaborada por la Comisión quiso presentarse por parte de la misma como "un planteamiento equilibrado", que se basaba no sólo en los resultados de las consultas previas, sino también en una "evaluación de impacto" encargada previamente por la propia institución[91].

Lo cierto es que los dictámenes emitidos sobre la Propuesta de Directiva por parte del GT29, el SEPD, el Parlamento Europeo y del CESE pueden en general calificarse como una dura censura al texto proyectado, siendo la principal objeción común el considerar que no tutelaba suficientemente los derechos fundamentales afectados. De hecho, algunas de las observaciones contenidas en estos dictámenes se tradujeron más tarde en enmiendas parlamentarias, que a su vez contribuyeron a modificar en buena medida el texto finalmente aprobado, si bien otra porción de estas críticas fueron obviadas y siguen siendo usadas aún hoy como poderosos argumentos contra la vigente normativa, tal como tendremos ocasión de ver más adelante.

Siguiendo el orden cronológico de su emisión, el primero de estos documentos en ver la luz fue el del SEPD[92], que el 26 de septiembre de 2005 —apenas unos días después de la publicación de la Propuesta— respondió a la solicitud de dictamen recibida de la Comisión el 23 de septiembre de 2005, para evaluar —de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n. 45/2001— el impacto directo que la normativa tendría sobre la protección de datos garantizada por el art. 8 CEDH y el modo en que se respetaban los principios de proporcionalidad y subsidiariedad.

---

[91] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 5. La Comisión llevó a cabo una evaluación de impacto, cuyo d está accesible en http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

[92] Cf. Dictamen del Supervisor Europeo de Protección de Datos sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final] (2005/C 298/01), publicado en el Diario Oficial de la Unión Europea el 29 de noviembre de 2005, C 298/1 a C 298/12. El texto oficial completo es accesible desde http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_ES.pdf

El dictamen se componía de ochenta y ocho puntos agrupados en torno a seis capítulos[93], en los que el SEPD venía a concluir, en términos ciertamente ásperos, que la norma proyectada no aportaba una respuesta adecuada y proporcionada a las necesidades de la sociedad[94]. Asimismo consideraba —ya lo hemos adelantado— que la Propuesta no adoptaba las salvaguardias necesarias para tutelar suficientemente los derechos fundamentales en juego, ya que resultaban insuficientes las medidas concretas respecto el acceso y la utilización posterior de los datos, el ejercicio de los derechos de los titulares de los datos y los incentivos a los proveedores para que invirtieran en una infraestructura técnica adecuada[95].

La principal preocupación del Supervisor se centraba en que la Propuesta respetara los derechos fundamentales, factor que consideraba "esencial"[96]. Una medida legislativa que perjudicara la protección garantizada por el Derecho comunitario y, más concretamente, por la jurisprudencia del TJUE y del TEDH "no sólo era inaceptable, sino que también ilegal"[97].

El SEPD no dudó en reconocer la importancia que tenía para los servicios policiales de los Estados miembros disponer de todos los instrumentos jurídicos necesarios, en especial en la lucha contra el terrorismo y otros tipos de delincuencia grave: "una disponibilidad adecuada de determinados datos de tráfico y de localización de los servicios electrónicos públicos puede ser un instrumento decisivo para dichos servicios policiales y puede contribuir a la seguridad física de las personas". Sin embargo, al mismo tiempo, resultaba evidente que la Propuesta presentaba un impacto considerable en el derecho a la protección de datos personales[98]. De hecho, si la misma se consideraba solamente desde esta perspectiva, recordaba el dictamen que los datos de tráfico y de localización "no debían retenerse en absoluto con fines represivos", pues tal

---

[93] Los seis capítulos son los siguientes: I. Introducción, II. Observaciones generales, III. La base jurídica y el proyecto de Decisión marco, IV. Necesidad de armonización, V. Comentarios sobre los artículos de la propuesta, VI. Conclusiones.

[94] Cf. Dictamen del SEPD…, doc. cit., punto 26.

[95] Cf. Dictamen del SEPD…, doc. cit., puntos 27 y 28.

[96] Cf. Dictamen del SEPD…, doc. cit., punto 8.

[97] Cf. Dictamen del SEPD…, doc. cit., punto 74.

[98] Cf. Dictamen del SEPD…, doc. cit., punto 3.

es el principio establecido con claridad por la Directiva 2002/58/CE, en los términos que ya explicamos en el apartado anterior[99].

Así pues, confirmada la afectación de derechos, resultaba necesario que se demostrara la necesidad y la proporcionalidad de la obligación de retener datos en toda su extensión. En lo que se refiere a la primera, el SEPD reconocía los cambios de circunstancias tras los atentados, pero no se mostraba convencido de que existiera una verdadera necesidad de la retención de los datos de tráfico y de localización a efectos de los servicios policiales, al menos en los términos establecidos en la Propuesta[100]. En cuanto a la proporcionalidad de la medida, el Supervisor estimaba que la Propuesta debía modificarse en tres direcciones.

En primer lugar, los plazos de retención debían limitarse, en tanto que los proyectados no reflejaban las necesidades demostradas de los servicios policiales. En concreto, alegaba el SEPD que el período máximo de dos años de conservación de datos suponía un abuso, ya que en la práctica el plazo de seis meses a un año era el utilizado por la Policía para llevar a cabo investigaciones complejas de delitos graves[101].

En segundo lugar, y con igual razonamiento, el dictamen abogaba por la necesidad de limitar el volumen de datos a almacenar, pues el mismo debía reflejar las necesidades de los servicios policiales[102].

En tercer y último lugar, la Propuesta presentaba para el SEPD numerosos defectos en lo que se refería a las medidas de seguridad de los datos[103]. Debía asegurarse que no fuera posible a este respecto acceder a datos de contenido, así como prevenir el acceso y el uso posterior de la información almacenada, que habría de borrarse adecuadamente al final de un plazo de retención. También debía asegurarse de garantizar el ejercicio de

---

[99] Ibíd. De acuerdo con esta norma, los datos de tráfico deben borrarse cuando el almacenamiento ya no sea necesario a efectos de la propia comunicación en sí —incluso con fines de facturación—. Las excepciones a este principio jurídico están sujetas a condiciones estrictas.

[100] Cf. Dictamen del SEPD…, doc. cit., puntos 14-23.

[101] Cf. Dictamen del SEPD…, doc. cit., punto 16.

[102] Cf. Dictamen del SEPD…, doc. cit., punto 77.

[103] Ibíd.

los derechos de las personas a las que se refieren los datos. En general, el deseo del Supervisor era que se agregaran a la Propuesta otras salvaguardias adicionales para la protección de datos, no una simple referencia a las salvaguardias en la legislación vigente[104].

Adicionalmente, para que la DCD fuera aceptable desde la perspectiva de la protección de datos, el SEPD consideraba conveniente la adición de otros incentivos a los proveedores que inviertan en una infraestructura técnica conveniente, incluidos incentivos financieros[105].

En definitiva, del dictamen se desprende con claridad que el SEPD no estaba convencido en absoluto acerca de la necesidad de la medida de conversación de datos. El hecho es que muchas de sus recomendaciones no encontraron eco en el texto finalmente aprobado. Así, por ejemplo, ni el acceso a los datos ni su destrucción han sido regulados con detalle en la DCD. A pesar de que tratarse de extremos relevantes para la adecuada protección de los datos personales, su concreción finalmente se ha dejado por completo a la implementación por parte de cada Estado.

La siguiente andanada de críticas a la Propuesta vino de la mano del GT29[106], que el 21 de octubre de 2005 adoptó su *Dictamen 4/2005 sobre la Propuesta de Directiva sobre*

---

[104] Cf. Dictamen del SEPD…, doc. cit., punto 79.

[105] Cf. Dictamen del SEPD…, doc. cit., punto 80.

[106] Cabe recordar que el GT29 fue creado por el art. 29 de la Directiva 95/46/CE; su art. 30.1 le atribuyó entre otras la función la de asesorar a la Comisión Europea sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades.
El GT29 se creó al amparo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. Sus dictamenes se adoptan en virtud del el artículo 29 y la letra a) del apartado 1 y el apartado 3 del artículo 30 de dicha Directiva, así como el apartado 3 del artículo 15 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, Su Reglamento interno, y en particular sus artículos 12 y 14.

la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE[107].

Con una extensión de doce páginas precedidas por un Resumen y seguidas por tres apartados[108], el informe comenzaba afirmando que la DCD nos enfrentaba a "una decisión histórica"[109]. El análisis del Grupo partía del hecho de que la conservación de los datos del tráfico interfería "con el derecho fundamental e inviolable a la confidencialidad de las comunicaciones", de tal modo que su primera consideración fue recordar que "toda restricción a este derecho fundamental debe estar justificada por una necesidad apremiante, sólo deberá permitirse en casos excepcionales y deberá contar con las garantías adecuadas"[110].

El tono general del dictamen es de desconfianza hacia la medida, al tiempo que incluye numerosas observaciones para su mejora. Así, aunque el Grupo reconocía que el terrorismo plantea a nuestra sociedad un desafío *real y apremiante*, también advertía

---

Se trata de un organismo consultivo europeo independiente relativo a la protección de datos y de la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. La secretaría corre a cargo de la Dirección C (Justicia Civil, Derechos Fundamentales y Ciudadanía) de la Comisión Europea. Su sitio web es accesible desde http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

Cabe recordar que el GT29 fue creado por el art. 29 de la Directiva 95/46/CE; su art. 30.1 le atribuyó entre otras la función la de asesorar a la Comisión Europea sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades

[107] El Considerando 15, DCD, recuerda la necesidad de someter la Directiva a dictamen del GT29 en los siguientes términos: "La Directiva 95/46/CE y la Directiva 2002/58/CE son plenamente aplicables a los datos conservados de conformidad con la presente Directiva; el artículo 30, apartado 1, letra c), de la Directiva 95/46/CE exige la consulta al Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, establecido de conformidad con el artículo 29 de dicha Directiva".

[108] Estos apartados son los siguientes: I. Antecedentes; II. Evaluación preliminar y condiciones previas generales, y III, Otras garantías especificas.

[109] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 5.

[110] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 3.

que los Gobiernos debían responder a este desafío de una manera que no socavase el derecho a la confidencialidad de los datos. En este sentido, el dictamen hacía hincapié en que la justificación para la conservación obligatoria y general de los datos debía demostrarse claramente y apoyarse "con pruebas", cuestionando a renglón seguido el que la justificación para la conservación obligatoria y general de los datos —alegada por las autoridades competentes de los Estados miembros— se basara en pruebas claras[111]. La conclusión del Grupo era que la iniciativa de la Comisión Europea debía dar lugar a la fijación de períodos de conservación lo más breves posible y a un límite máximo de conservación aplicable a todos los Estados miembros, dándoles libertad para fijar períodos de conservación más cortos[112].

Hay que reconocer que, en algunos puntos, las opiniones del GT29 no hacen sino abundar en lo que las otras instituciones lo harían más tarde, como por ejemplo, la necesidad de determinar claramente qué se entiende por "delitos graves", la prohibición de *data mining* y de procesar los datos retenidos por parte de los proveedores de servicios, o la conveniencia de una mayor delimitación de las medidas de seguridad a adoptar y de las condiciones bajo las que las autoridades competentes pueden acceder y utilizar tales datos para combatir y prevenir el terrorismo[113].

A nuestro entender, no obstante, el mérito y singularidad del dictamen del GT29 descansa en otra parte, en concreto: en haber efectuado un análisis marcadamente más práctico y con miras más amplias que el resto de los órganos dictaminante, pues llegaba a ofrecer interesantes alternativas a la regulación proyectada. En este sentido, es necesario hacer mención a la sugerencia de que se tuviera en cuenta la existencia de "enfoques menos invasores de la intimidad, como por ejemplo, el procedimiento de *quick freeze* o congelación rápida[114]. También es mérito del Grupo haber insistido en

---

[111] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 7.

[112] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 8.

[113] Cf. Dictamen 4/2005, del GT29…, doc. cit., pp. 9-13.

[114] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 7. De acuerdo con este sistema, ni los proveedores de comunicación ni los prestadores de servicios de internet están obligados a almacenar datos relativos al tráfico. En casos justificados, las autoridades policiales consultan a las empresas y piden que se almacenen ciertos datos. Después de que esos datos se hayan almacenado, las autoridades tienen algunas

que las medidas que eventualmente se introdujeran deberían ser objeto de amplia publicidad, así como la propuesta de que las pruebas de la necesidad de estas medidas debían ser "objeto de una evaluación periódica, que deberá realizarse al menos cada dos o tres años y hacerse pública"[115]. Y lo que es más novedoso: además de basarse en una evaluación periódica, las medidas debían ser limitadas en el tiempo de acuerdo con el concepto *sunset legislation* —legislación de vigencia limitada—. Para ser exactos, el Grupo estimaba que un período de tres años debía reputarse como adecuado[116].

El dictamen se cerraba con la propuesta de veinte garantías específicas, con especial atención a los requisitos aplicables a los destinatarios y al tratamiento posterior de los datos, la importancia de las autorizaciones y controles, las medidas aplicables a los prestadores de servicios —también en términos de seguridad y de separación lógica de los datos—, la determinación de las categorías de datos en cuestión y su actualización, y a la necesidad de excluir datos relativos al contenido[117].

Finalmente, hay que indicar que, con posterioridad a la aprobación de la Directiva, el 13 de julio de 2010 el GT29 emitió otro dictamen, el 3/2006, relativo a su aplicación[118]. En el mismo, el Grupo reiteraba su preocupación por las previsiones contempladas en la Directiva y se ratificaba en muchas de las opiniones expuestas en el anterior dictamen, sobre todo, en la necesidad de incluir medidas que aminorasen el fuerte impacto sobre la privacidad de la vigente normativa[119].

---

semanas para recoger pruebas a fin de obtener una orden judicial. Posteriormente, con esta orden, pueden acceder a los datos.

[115] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 13.

[116] Ibíd.

[117] Cf. Dictamen 4/2005, del GT29…, doc. cit., pp. 9-13.

[118] Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, adopted on 13 July 2010 [00068/10/EN WP 172]. El document no ha sido traducido al castellano.

[119] Cf. Report 01/2010 on the second joint…, doc. cit., p. 1.

El siguiente informe sobre la DCD en ver la luz fue el presentado el 16 de noviembre de 2005 por el CESE[120], al que —de conformidad con el artículo 95 TCE— el Consejo de la Unión Europea había solicitado consulta acerca del texto.

El 27 de septiembre de 2005 la Mesa del CESE había encargado a la Sección Especializada de Transportes, Energía, Infraestructuras y Sociedad de la Información la preparación de trabajos sobre el asunto. Con gran celeridad, el Pleno de los días 18 y 19 de enero de 2006 aprobó, por noventa y dos votos a favor, diecisiete en contra y diecisiete abstenciones su *Dictamen sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE"*.

Formalmente, el documento resultante estaba dividido en dos grandes bloques. El primero contenía las *Conclusiones y recomendaciones*; el segundo, su *Motivación*[121]. Acompañaron al texto un anexo con las propuestas de enmienda que habían obtenido más de un cuarto de los votos emitidos en el seno del Comité pero que fueron finalmente rechazadas.

El tono y contenido del dictamen lo convierten en el más negativo de cuantos se emitieron sobre la Propuesta de directiva. Ya su punto 1.1 marcaba el tono crítico presente a lo largo del documento, advirtiendo la "extrañeza y preocupación" del Comité "por la presentación de una propuesta normativa de esta índole, pues su contenido resulta desproporcionado y afecta a los derechos fundamentales", para indicar a renglón seguido que "el tratamiento dado en la propuesta a los derechos

---

[120] Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE» COM(2005) 438 final — 2005/0182 (COD) (2006/C 69/04) Diario Oficial de la Unión Europea de 21 de marzo de 2006 (C 69/16 - C 69/21). El texto oficial puede consultarse en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:069:0016:0021:ES:PDF

[121] Este segundo bloque englobaba a su vez los apartados de *Antecedentes*, *Propuesta de la Comisión*, *Observaciones generales* y *Observaciones específicas*.

humanos, especialmente, el derecho a la intimidad, no se realiza adecuadamente y puede colisionar en determinados aspectos"[122].

Para el CESE, parecía evidente que la proyectada directiva tendría consecuencias muy amplias para la integridad de todos los usuarios de servicios de comunicaciones electrónicas y, sobre todo, corría el riesgo de socavar la confianza de los usuarios de las comunicaciones electrónicas y disminuir su disposición a utilizar las denominadas TICs[123]. Esta pérdida de confianza por parte de los consumidores implicaba a su vez el riesgo de que el desarrollo de la sociedad de la información se viera "frenado a largo plazo"[124].

Por otra parte, el CESE no ocultaba sus dudas acerca que la Propuesta cumpliera *en su totalidad* con los principios de subsidiariedad y proporcionalidad, dada la ausencia de razones que justificasen que un objetivo de la Comunidad pudiera alcanzarse mejor en el plano de ésta. En lo que concierne al cumplimiento del primero —el principio de subsidiariedad— la Propuesta de Directiva convertía las medidas nacionales vigentes en materia de seguridad pública en "medidas de efecto equivalente" —obstáculos al mercado interior de las telecomunicaciones— que debían ser eliminados conforme a lo dispuesto en el artículo 14 TCE[125], para afirmar seguidamente que, dado que hasta la fecha ni el Consejo ni el Parlamento habían sido capaces de acordar un marco de solución a los problemas en cuestión, urgía una acción supranacional en el ámbito del mercado interior desde la cual proceder a su regulación[126]. "Toda esta forma de razonar —observaba el dictaminante— sería lógica si los problemas de seguridad fueran equiparables a otros que afectan al funcionamiento del mercado interior —por ejemplo, de índole estrictamente mercantil, fiscal o laboral—; si existieran plazos perentorios para la adopción de normas o si, finalmente, fuera posible, y necesario, crear un espacio jurídico uniforme al respecto"[127]. Sin embargo, el CESE advertía que la seguridad del Estado no es un bien jurídico previsto en el Derecho comunitario, a diferencia de las

[122] Cf. Dictamen del CESE…, doc. cit., punto 1.2.

[123] Cf. Dictamen del CESE…, doc. cit., punto 2.3.2.

[124] Cf. Dictamen del CESE…, doc. cit., puntos 1.3. y 2.3.3.

[125] Cf. Dictamen del CESE…, doc. cit., punto 2.3.2.

[126] Cf. Dictamen del CESE…, doc. cit., punto 2.3.9.

[127] Cf. Dictamen del CESE…, doc. cit., punto 2.3.10.

nociones de orden público y de la seguridad pública —previstas en los Tratados— para justificar la adopción excepcional de medidas de salvaguardia por los Estados miembros[128]. Tampoco existía en los Tratados, a su entender, una base clara de actuación al respecto, ni plazo alguno que impusiera la inmediatez de su actuación. Finalmente, se apuntaba que las amenazas a la seguridad de los Estados no eran subsumibles en un instrumento de armonización que pretendía dar "un tratamiento idéntico (que no común) a situaciones diferentes"[129].

Aparte de estas críticas, no puede dejar de notarse que fue el CESE el primer órgano que se opuso de plano a que las compañías de telecomunicaciones fueran compensadas económicamente por los gastos que la normativa acarreaba. En su opinión, los costes adicionales en que incurrieran los operadores para cumplir los datos de almacenamiento y transmisión de datos contemplados en la Propuesta habían de ser entendidos "como una carga que los operadores deberían asumir por el mero hecho de estar en el mercado, sin que el erario público, y por ende todos los ciudadanos, tengan que soportarla"[130]. Postura que, como veremos, prevaleció en el texto finalmente aprobado, que omite la cuestión.

Finalmente, el Dictamen culminaba con un último y expresivo párrafo, en el que se afirmaba con contundencia que, por todas las razones expuestas:

> "la Comisión, como «guardiana de los Tratados» y de sus principales esencias, según los artículos 6-1[131] y 6-2[132] del TUE, debería revisar sustancialmente esta

[128] Cf. Dictamen del CESE…, doc. cit., punto 2.3.11.

[129] Cf. Dictamen del CESE…, doc. cit., punto 2.3.12.

[130] Cf. Dictamen del CESE…, doc. cit., punto 1.5.

[131] Establece el artículo 6-1 TUE que "la Unión se basa en los principios de libertad, democracia, respeto de los derechos humanos y de las libertades fundamentales y el Estado de Derecho, principios que son comunes a los Estados miembros".

[132] Conforme al artículo 6-2 TUE, "La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma el 4 de noviembre de 1950, y tal y como resultan de las tradiciones constitucionales comunes a los estados miembros como principios generales del Derecho comunitario".

propuesta, que a juicio del Comité no respeta en su totalidad los derechos fundamentales, ni las reglas de acceso, uso e intercambio de los datos"[133].

Puestas sobre la mesa estas opiniones, y una vez incoada la tramitación parlamentaria, el Parlamento Europeo se mostró también crítico con la Propuesta, lo que tuvo su reflejo en la aprobación de una serie de enmiendas que trataban de tutelar los derechos de los titulares de los datos. Por ejemplo, la enmienda 82, que introdujo un nuevo artículo 7 *bis* —que se convirtió en el art. 7 DCD— enfatizó la necesidad de adoptar medidas de seguridad. O bien la enmienda 88, que añadió un nuevo artículo 11 *ter* —que se convirtió en el art. 13 DCD—, hacía referencia a los recursos judiciales, responsabilidades y sanciones. Además, cabe destacar que, durante el paso por la cámara, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, en un informe de finales de noviembre de 2005, también insistió en la necesidad de reducción de los plazos previstos por la Propuesta, ya que a juicio de la Comisión de Industria e Investigación la persecución de delitos por parte de las autoridades no suponía más de tres meses de antigüedad, debiendo los períodos legales responder a las necesidades efectivas y no aumentarlos desproporcionadamente. El informe también mostraba su preocupación sobre los costes de archivo, almacenamiento, tratamiento y seguridad de los datos, que supondría un coste para las empresas de cientos de millones, sin contar los gastos derivados de la actualización y mantenimiento de los sistemas informáticos desarrollados al efecto[134].

Pese a su esfuerzo por reforzar las garantías de la normativa, lo cierto es que —como apunta VILASAU[135]— el Parlamento Europeo también adoptó algunas enmiendas más discutibles, como la enmienda 85, que suprimió el art. 10 de la Propuesta que hacía referencia a los costes; o la enmienda 87 que proponía la introducción de un nuevo

---

[133] Cf. Dictamen del CESE…, doc. cit., punto 2.4.15. La misma idea se adelantaba en el punto 1.6.

[134] Cf. Dictamen del CESE…, doc. cit., últimos puntos.

[135] VILASAU SOLANA, M., La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad, en *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, n. 3, 2006, p. 5 (edición digital).

artículo 11 *bis*, que se convirtió en el art. 12 del texto definitivo, relativo a las *medidas futuras*, cuyo contenido explicaremos en su momento[136].

La difícil tramitación de la DCD no sirvió para que la norma resultante solventara las cuestiones en liza. El texto finalmente resultante fue aprobado por la cámara el 15 de marzo de 2006 y publicado en el Diario Oficial el 13 de abril, entrando en vigor veinte días más tarde. Al estudio pormenorizado de su articulado dedicaremos los siguientes capítulos.

4 Objetivo de la DCD

4.1 Objetivo de la DCD

El objetivo perseguido por la DCD se expresa con claridad en su primer artículo, que —compuesto por dos apartados bajo la rúbrica de "Objeto y ámbito"— se ocupa de definir el propósito de la norma y los sujetos afectados por la misma[137].

---

[136] Véase respecto todas las enmiendas la resolución legislativa del Parlamento europeo de 14 de diciembre de 2005 sobre la Propuesta de directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)].

[137] Transcribimos aquí, para su examen directo, el tenor literal del precepto:

Artículo 1. Objeto y ámbito.

1. La presente Directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

2. La presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

Conforme a lo dispuesto en el primer apartado, el propósito de la DCD consiste en armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

Con estas palabras, el art. 1.1 DCD resume el contenido esencial de la norma que nos ocupa. Expuesto más llanamente, la Directiva obliga a los Estados miembros a adoptar medidas para garantizar que un determinado conjunto de datos externos[138] de las comunicaciones electrónicas sean conservados y se hallen disponibles durante un plazo de entre seis y veinticuatro meses[139] para los fines de investigación, detección y enjuiciamiento de delitos graves, según lo definido por cada Estado miembro en su Derecho nacional[140]. No indica por tanto qué concretos delitos justifican el uso de los datos, qué autoridades pueden acceder a los mismos y bajo qué condiciones pueden éstas intercambiarlos.

Un ordenado análisis de tan compleja obligación parece más convenientemente abordado si nos ocupamos primero de la materia objeto de regulación *stricto sensu*, para continuar inmediatamente después por la necesidad de armonización comunitaria sobre la misma.

Respecto de la primera, su importancia para la Unión Europea fue sostenida con profusión de argumentos en la Exposición de Motivos de Propuesta. Conforme a este texto, los motivos y objetivos de la DCD se justificaban por el hecho de que "cada vez más ciudadanos realizan diariamente actividades y transacciones a través de redes y servicios de comunicaciones electrónicas"[141]. Estas comunicaciones generan datos de tráfico o datos de localización como, por ejemplo, detalles sobre la localización del autor de la llamada, el número llamado, la hora y la duración de la llamada. Cuando se

[138] Cf. art. 5 DCD.

[139] Cf. art. 6 DCD.

[140] Cf. art. 1 DCD.

[141] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 2.

combinan con datos que permiten la identificación del abonado o usuario del servicio, "la disponibilidad de tales datos de tráfico tiene su importancia para las actividades relacionadas con la represión de actividades ilícitas y la seguridad, como la prevención, investigación, detección y enjuiciamiento de delitos graves, como es el caso del terrorismo y la delincuencia organizada"[142]. Sin embargo —razonaba la Comisión— con los cambios en los modelos empresariales y ofertas de servicios, tales como la proliferación de tarifas planas, servicios de comunicaciones electrónicas pagados por adelantado o gratuitos, los datos de tráfico no siempre podían ser almacenados por todos los operadores en la misma medida que los últimos años, en función de los servicios que ofrecen [143].

Comprobaba también la institución que esta tendencia se veía reforzada por ofertas recientes de servicios de comunicación VoIP[144], o incluso servicios de tarifa plana para comunicaciones telefónicas fijas. Con este tipo de servicios, los operadores ya no tendrían necesidad de almacenar datos de tráfico para facturar, y así, si los datos de tráfico no se almacenaban con fines de facturación u otros fines comerciales, tampoco estarían disponibles para las autoridades públicas cuando sea legítimo acceder a los datos. La conclusión para la Comisión no podía ser otra sino el que estos avances estaban "dificultando a las autoridades públicas el cumplimiento de sus deberes de prevención y lucha contra la delincuencia organizada y el terrorismo, y están facilitando la comunicación entre los delincuentes, que ya no temen que las autoridades represivas puedan utilizar sus datos para frustrar sus actividades"[145]. En consecuencia,

---

[142] Ibíd.

[143] Ibíd.

[144] VoIP (Voice over IP, o voz sobre protocolo de internet) es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

[145] Ibíd.

todas las disposiciones relacionadas con esta problemática debían armonizarse de conformidad con el art. 14 TCE[146].

Expuestas así las razones por las que la Unión Europea consideraba importante aprobar una regulación en materia de conservación de datos de las comunicaciones electrónicas, hemos de considerar seguidamente la necesidad de armonización de la materia concernida a través de una directiva. Como hemos adelantado, tal necesidad venía dada por la urgencia de adoptar en el seno de la Unión disposiciones armonizadas sobre la materia ante la dispersión normativa en determinados casos, o la ausencia de regulación en otros.

Ciertamente, si echamos un vistazo a la situación de las legislaciones internas en materia de conservación de datos al tiempo de la tramitación de la DCD, se constata que, en efecto, un cierto número de Estados miembros había adoptado en los años inmediatamente anteriores medidas nacionales que exigían a los operadores de telecomunicaciones retener determinados tipos de datos para su uso con concretas finalidades penales. Estas normas se enmarcaban —como ya expusimos en su momento— en la corriente político-legislativa surgida en occidente a partir de los atentados terroristas de Nueva York. Al respecto, puede destacarse la aprobación en Reino Unido de las *Regulations of Investigatory Powers*[147], que obligaban a los

---

[146] Ahora consolidado en el art. 26 TFUE, el tenor literal reza así: "1. La Unión adoptará las medidas destinadas a establecer el mercado interior o a garantizar su funcionamiento, de conformidad con las disposiciones pertinentes de los Tratados.

2. El mercado interior implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones de los Tratados.

3. El Consejo, a propuesta de la Comisión, definirá las orientaciones y condiciones necesarias para asegurar un progreso equilibrado en el conjunto de los sectores considerados".

[147] *An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes*,

proveedores de internet a retener datos de tráfico, así como la *Anti-Terrorism Crime and Security Act*[148], que englobó en gran medida la lucha contra el terrorismo y la seguridad nacional dentro de un marco también electrónico. En la misma línea, Italia permitió en su Código de Protección de Datos Personales de 2004 la conservación de datos de tráfico por un período de treinta meses[149]. Asimismo, la legislación belga sobre cibercriminalidad[150] facultó la conservación de datos para la investigación criminal, en tanto que en Dinamarca otra norma hacía lo propio por un período de un año. Dentro del Espacio Económico Europeo, también poseían legislación sobre conservación de datos en Islandia y Liechtenstein[151].

Las grandes diferencias entre las disposiciones legislativas, reglamentarias y técnicas de cada Estado miembro en materia de conservación de datos de tráfico planteaban —al entender del legislador europeo— obstáculos ciertos para el mercado interior de las comunicaciones electrónicas, en la medida en que los prestadores de servicios se enfrentaban a requisitos diferentes en cuanto a los tipos de datos que debían

---

2000, Chapter 23. El texto oficial está publicado en http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

[148] *An Act to amend the Terrorism Act 2000; to make further provision about terrorism and security; to provide for the freezing of assets; to make provision about immigration and asylum; to amend or extend the criminal law and powers for preventing crime and enforcing that law; to make provision about the control of pathogens and toxins; to provide for the retention of communications data; to provide for implementation of Title VI of the Treaty on European Union; and for connected purposes*, 2001, Chapter 24. Puede consultarse la publicación oficial en http://www.legislation.gov.uk/ukpga/2001/24/pdfs/ukpga_20010024_en.pdf

[149] *Decreto Legislativo* n. 196, *Codice in materia di protezione dei dati personali*, publicado el 29 de julio de 2003 en *Gazzetta Ufficiale*, n. 174, *Supplemento Ordinario*, n. 123. El texto de la norma es accesible en: http://www.camera.it/parlam/leggi/deleghe/testi/03196dl.htm

[150] *Wet van 28 november 2000 inzake informaticacriminaliteit, Belgisch Staatsblad*, de 3 de febrero de 2001, p. 2909, modificando el *Strafwetboek* (código de enjuiciamiento criminal), disponible en holandés y francés en http://www.juridat.be/cgi_wet/wetgeving.pl. Cf. Wet houdende de voorafgaande titel van het Wetboek van Strafvordering, que introduce un nuevo título al citado código, disponible en http://www.juridat.be/cgi_wet/wetgeving.pl

[151] La legislación de transposición en Islandia es la Ley de Telecomunicaciones 81/2003 (modificada en abril de 2005); en Liechtenstein es la Ley de Telecomunicaciones de 2006.

conservarse, así como en cuanto a su conservación *stricto sensu*[152]. No puede olvidarse tampoco que —como mencionamos— la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, había establecido años atrás en sus arts. 5, 6 y 9 el principio general de la destrucción de los datos del tráfico cuando ya no se necesitasen para la transmisión. En tales casos, los datos debían borrarse o hacerse anónimos a excepción de los necesarios para la facturación o los pagos por interconexión o previo consentimiento para su tratamiento con fines comerciales o la prestación de servicios de valor añadido. Al tiempo, el art. 15.1 de la misma Directiva abrió la posibilidad de que los Estados miembros prevean excepciones a estos mismos artículos; concretamente, las legislaciones internas pueden prever restricciones al alcance de los artículos 5, 6 y 9 cuando tal limitación constituya "una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y enjuiciamiento de delitos". De hecho, al amparo de este art. 15 se habían dictado varias de las normas de producción interna que con su diversidad en los datos a retener y en los plazos de retención, venían a justificar la necesidad de adoptar una directiva que pusiera fin a las disparidades y eliminara así los consiguientes obstáculos para el mercado interior de comunicaciones electrónicas.

Además de este argumento, habría que añadir otro relativo a los fines de represión penal perseguidos por la DCD. En concreto, parecía evidente que la falta de armonización perjudicaba las necesidades de los servicios policiales en la medida en que las autoridades competentes tenían que adaptar sus esfuerzos investigadores a requisitos legales de variada índole, lo que dificultaba a su vez el intercambio de información entre las autoridades de los Estados miembros —sobre todo teniendo en cuenta que para una gran cantidad de comunicaciones electrónicas es competente la jurisdicción de más de un Estado miembro—. Ejemplos ilustrativos pueden ser, a este respecto, las llamadas telefónicas transfronterizas, la itinerancia de las comunicaciones, el cruce de fronteras durante las comunicaciones móviles o el uso de un proveedor en otro Estado miembro que el país de residencia del individuo.

---

[152] Véase el documento de trabajo sobre la evaluación del impacto de la Propuesta de Directiva [Bruselas, 21.9.2005. SEC (2005) 1131].
Disponible en: http://ec.europa.eu/justice_home/doc_centre/police/doc/sec_2005_1131_en.pdf

En virtud de ambas líneas argumentales, la armonización de los elementos principales incluidos en la DCD debía ser en consecuencia integral, lo que a su vez se entendía —por añadidura— imprescindible para cumplir con el CEDH y los principios de la legislación sobre protección de datos. Tal como el SEPD puso de relieve[153], permitir diferencias esenciales entre las leyes de los Estados miembros no eliminaría las perturbaciones existentes en el mercado interior de las comunicaciones electrónicas, que se debían entre otras cosas a la adopción de medidas legislativas en los Estados miembros en virtud del artículo 15 DPCE. De esta manera, la armonización debía cubrir todos los elementos concernidos y hacerlo "teniendo en cuenta el funcionamiento del mercado interior, las necesidades de los servicios policiales y, en último lugar, pero no por ello menos importante, el CEDH y los principios de protección de datos"[154]. Más concretamente, cualquier medida legislativa que obligase a retener los datos de tráfico y de localización tenía —en opinión del órgano— que delimitar claramente el número de datos a retener, los plazos de retención y los fines de acceso y posterior utilización de los datos, para que fuera aceptable desde la perspectiva de la protección de datos y para cumplir con los requisitos de necesidad y de proporcionalidad[155].

Dentro de esta preocupación por que la armonización fuera integral y, en lo que se refiere concretamente a la necesidad de armonización respecto de los plazos de conservación, es mérito del GT29 el haber advertido que la armonización de la legislación de los Estados miembros debía asegurar que el establecimiento de un período de conservación obligatorio de los datos a nivel europeo estuviera basado en una "evaluación de proporcionalidad efectuada a nivel europeo", que tuviera en cuenta también "el carácter transnacional de la delincuencia organizada, así como los requisitos máximos de seguridad de todos los Estados miembros"[156]. El Grupo también sugirió que se aclarara posteriormente que el período de conservación de datos mencionado en la Directiva debía considerarse como "el límite máximo armonizado

[153] Cf. Dictamen del SEPD…, doc. cit., punto 45.

[154] Cf. Dictamen del SEPD…, doc. cit., punto 44.

[155] Cf. Dictamen del SEPD…, doc. cit., punto 48.

[156] Cf. Dictamen 4/2005, del GT29…, doc. cit., punto 2.

aplicable a todos los Estados miembros"[157], de tal modo que quedara claro que los Estados miembros no podrían establecer períodos de conservación de datos más largos que los previstos en la Directiva, aunque tendrían libertad para establecer períodos de conservación más breves. Como veremos, tan sensata petición no fue atendida por el legislador europeo.

En lo que se refiere a otro elemento relevante afectado por la armonización —la finalidad de la conservación— es de importancia recalcar que el artículo 1.1[158] de la Propuesta de Directiva tenía un contenido ligeramente distinto al finalmente aprobado. La obligación de conservación tenía en la Propuesta la finalidad de asegurar que los datos estuvieran disponibles con fines de "prevención, investigación, detección y enjuiciamiento" de delitos graves, añadiendo seguidamente: "como el terrorismo y la delincuencia organizada"[159]. El texto final eliminó la "prevención", mencionando sólo los fines de "investigación, detección y enjuiciamiento" de delitos graves, al tiempo que sustituyó la concreción ejemplificativa por una remisión a lo que debiera entenderse por tales delitos graves: "tal como se definen en la legislación nacional de cada Estado miembro"[160]. Esta modificación está en el origen de una de las grandes fallas de la DCD, pues ahora los datos pueden conservarse con el fin específico de perseguir otras "infracciones graves" indeterminadas, con los consecuentes problemas que más tarde consideraremos. Además, el Grupo llegó a sugerir, para reforzar esta idea, el que la limitación de la finalidad figurase también en el titulo final de la DCD[161], cuya redacción primigenia llevaba por título "sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la

---

[157] Ibid.

[158] Concretamente, el art. 1 de la Propuesta establecía lo siguiente: "Esta Directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con el tratamiento y la conservación de determinados datos, para asegurar que los datos estén disponibles con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como el terrorismo y la delincuencia organizada".

[159] También realizaba la misma puntualización el art. 11 de la Propuesta.

[160] Cf. art. 1.1 DCD.

[161] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 9.

que se modifica la Directiva 2002/58/CE". Ni una ni otra propuesta tuvieron éxito[162]. No sin fundamento, el GT29 ha seguido proponiendo en los últimos años una transposición de la DCD en la que el término "infracciones graves" quede claramente definido y no sean posibles interpretaciones extensivas[163], opinión que apenas ha encontrado eco ni en los Estados miembros ni en la Comisión, a pesar de los muchos argumentos a favor de este cambio y que hemos de discutir en posteriores apartados.

De hecho, en la práctica, con el paso del tiempo la transposición de la DCD ha revelado cómo lo que se entiende por delitos graves a la hora de legitimar el acceso a los datos varía ampliamente en las legislaciones nacionales de cada país de la Unión. La pretendida armonización ha sido un notable fracaso en este importante aspecto. Así, tal como reconoce la propia Comisión en su Informe de Evaluación de 2011[164], diez Estados miembros —Bulgaria, Estonia Irlanda, Grecia, España, Lituania, Luxemburgo, Hungría, Países Bajos y Finlandia— han definido "delito grave" con referencia a una pena de prisión mínima, a la posibilidad de que se imponga una pena privativa de libertad o a una lista de delitos definidos en otras partes de la legislación nacional. Ocho Estados miembros —Bélgica, Dinamarca, Francia, Italia, Letonia, Polonia, Eslovaquia y Eslovenia— exigen que los datos deben conservarse no sólo para la investigación, detección y enjuiciamiento de delitos graves, sino también en relación con todos los delitos y para la prevención de la delincuencia, o por razones generales de seguridad nacional, estatal o pública. Por su parte, las legislaciones de cuatro Estados miembros —Chipre, Malta, Portugal y Reino Unido— se refieren a las "formas graves de delincuencia" o "delitos graves" sin definirlos[165].

La redacción vigente del art. 1.1 DCD sobre la finalidad que justifica la conservación y cesión de los datos —tal como ha sido desarrollada por las distintas legislaciones internas— ha dado origen a un muestrario de las más diversas posibilidades en cada Derecho interno, a saber:

---

[162] En concreto, el título de la vigente norma reza *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*.

[163] Cf. Report 01/2010 on the second joint…, doc. cit., p. 3.

[164] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 7.

[165] Ibíd.

— Austria: no transpuesta;
— Chipre: investigación de delitos graves, de conformidad con lo dispuesto en el artículo 4, apartado 1, de la Ley 183 (I)/2007;
— Eslovaquia: prevención, investigación, detección y enjuiciamiento de delitos, de conformidad con lo dispuesto en el artículo 59 bis, apartado 6, de la Ley de comunicaciones electrónicas;
— Eslovenia: garantizar la seguridad nacional, las normas constitucionales y los intereses económicos, políticos y de seguridad del Estado… así como para los fines de defensa nacional, de conformidad con lo dispuesto en el artículo 170 bis, apartado 1, de la Ley de comunicaciones electrónicas;
— España: detección, investigación y enjuiciamiento de los delitos graves contemplados en el Código Penal o en las leyes penales especiales, de conformidad con lo dispuesto en el artículo 1, apartado 1, de la Ley 25/2007;
— Finlandia: investigación, detección y enjuiciamiento de delitos graves, según lo establecido en el capítulo 5a, artículo 3, apartado 1, de la Ley de medidas coercitivas. Cf. artículo 14 bis, apartado 1, de la Ley de comunicaciones electrónicas;
— Francia: detección, investigación y enjuiciamiento de delitos, con el único fin de suministrar a las autoridades judiciales la información necesaria, y prevención de actos de terrorismo y protección de la propiedad intelectual. Las leyes que regulan la utilización de los datos conservados, respectivamente, para los delitos, la prevención de actos de terrorismo y la protección de la propiedad intelectual, son los siguientes: artículo L.34-1 (II) del CPCE, Ley nº 2006-64, de 23 de enero de 2006, y Ley nº 2009-669, de 12 de junio de 2009;
— Grecia: detección de delitos especialmente graves. Tales delitos se definen en el artículo 4 de la Ley 2225/1994; artículo 1 de la Ley 3917/2011;
— Hungría: permitir a los organismos de investigación, la Fiscalía, los tribunales y las agencias nacionales de seguridad realizar sus funciones, y a la Policía y las autoridades aduaneras y fiscales investigar delitos dolosos que lleven aparejada una pena de privación de libertad igual o superior a dos años. Para la finalidad general de la conservación de datos, artículo 159/A de la Ley C/2003, modificada por la Ley CLXXIV/2007; para la finalidad del acceso policial,

artículo 68 de la Ley XXXIV/1994; para la finalidad del acceso de la Oficina aduanera y fiscal, artículo 59 de la Ley CXXII/2010;

— Irlanda: prevención de delitos graves [es decir, delitos que lleven aparejada una pena de privación de libertad de 5 años o más, o un delito citado en el anexo de la ley de transposición], mantenimiento de la seguridad del Estado o salvamento de una vida humana, de conformidad con lo dispuesto en el artículo 6 Comunicaciones (Ley de Conservación de Datos) de 2011;

— Italia: detección y represión de delitos, de conformidad con lo dispuesto en el artículo 132, apartado 1, del Código de protección de datos;

— Letonia: protección de la seguridad pública y del Estado, investigación de delitos, enjuiciamiento penal y procedimientos penales, de conformidad con lo dispuesto en el artículo 71, apartado 1, de la Ley de comunicaciones electrónicas;

— Lituania: investigación, detección y enjuiciamiento de delitos graves y muy graves, según lo definido en el Código Penal lituano. Cf. artículo 65 de la Ley X-1835;

— Luxemburgo: detección, investigación y enjuiciamiento de delitos que lleven aparejada una condena penal máxima de un año o más, de conformidad con lo dispuesto en el artículo 1, apartado 1, de la Ley de 24 de julio de 2010;

— Malta: investigación, detección o enjuiciamiento de delitos graves, de conformidad con lo dispuesto en el artículo 20, apartado 1, Anuncio oficial 198/2008;

— Países Bajos: investigación y enjuiciamiento de delitos graves para los que puedan imponerse penas privativas de libertad, de conformidad con lo dispuesto en el artículo 126 del Código de enjuiciamiento penal;

— Polonia: prevención o detección de delitos, prevención y detección de delitos fiscales, uso por los fiscales y jueces en caso de que sea relevante para procedimientos judiciales, así como para los efectos de la Agencia de Seguridad Interior, la Agencia de Inteligencia Exterior, los Servicios Centrales de lucha contra la Corrupción, los Servicios de contrainteligencia militar y los Servicios de inteligencia militar. Cf. artículo 180 bis, Ley de telecomunicaciones de 16 de julio de 2004, modificado por el artículo 1 de la Ley de 24 de abril de 2009;

— Portugal: investigación, detección y enjuiciamiento de delitos graves, de conformidad con lo dispuesto en el artículo 1, 3 (1), de la Ley 32/2008;
— Reino Unido: investigación, detección y enjuiciamiento de delitos graves, según el Reglamento sobre la conservación de datos (Directiva CE) de 2009 (2009 nº 859);
— Rumanía: no transpuesta
— Suecia: no transpuesta.

Del examen de toda esta relación se concluye que, en la actualidad, la mayoría de los Estados miembros permiten el acceso y uso de los datos conservados con fines que van más allá de los cubiertos y pretendidos por la DCD, incluida la prevención y la lucha contra la delincuencia en general y el riesgo para la vida y la integridad física. Se reafirma de esta manera la conclusión que adelantamos unas páginas antes. Si bien el objetivo de la DCD era armonizar las regulaciones sobre conservación de datos aprobadas por iniciativa de algunos Estados o surgidas al amparo de la Directiva 2002/58/CE —la Directiva sobre la privacidad y las comunicaciones electrónicas—, el resultado final ha sido el diametralmente opuesto. En los momentos actuales, cada país permite la cesión de datos de acuerdo con finalidades penales completamente divergentes.

Como es natural, tales contrastes han perjudicado el volumen y la frecuencia de las solicitudes de cesión de datos entre Estados miembros —un objetivo también perseguido por la Comisión— y quizás, incluso, incrementado los costes generados para las compañías de telecomunicaciones por el cumplimiento de las obligaciones establecidas en la DCD. Si a esto le añadimos que tal situación puede considerarse que no ofrece la previsibilidad suficiente que se exige en el contexto del CEDH a cualquier medida legislativa que restrinja el derecho a la intimidad[166], no cabe sorprenderse de que la propia Comisión Europea no haya podido menos que expresar su "voluntad" de

[166] Al respecto, puede consultarse, entre otras, la Sentencia del Tribunal de Justicia de la Unión Europea de 20 de mayo de 2003, en los asuntos acumulados C-465/00, C-138/01 y C-139/01 (Petición de decisión prejudicial: Verfassungsgerichtshof y Oberster Gerichtshof): Rechnungshof (C-465/00) contra Österreichischer Rundfunk y otros, y entre Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) y Österreichischer Rundfunk (sobre divulgación de datos sobre los ingresos de empleados de entidades sujetas al control del Rechnungshof).

evaluar "la necesidad y las opciones para lograr un mayor grado de armonización en este ámbito"[167].

4.2 Sujetos obligados

La determinación del ámbito subjetivo de la DCD tampoco es satisfactoria. El art. 1.1 DCD se ocupa de indicar quiénes son los sujetos obligados por la norma, esto es, qué operadores deben cumplir la obligación de conservación de datos, describiéndolos como "los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones". A la hora de transponer la Directiva en los ordenamientos nacionales, la concreción de esta previsión ha dado lugar a una indeseable disparidad de criterios sobre cuáles son los proveedores afectados por la norma. Así, por ejemplo, y de acuerdo con lo observado por la Comisión Europea en su Informe de Evaluación[168], dos Estados miembros —Finlandia y Reino Unido— no exigen a los pequeños operadores que conserven datos, ya que, a su entender, los costes tanto para el proveedor como para el Estado superarían las ventajas que se obtendrían para los sistemas de justicia penal y policial, mientras cuatro Estados miembros —Letonia, Luxemburgo, Países Bajos y Polonia— han establecido disposiciones administrativas dispares[169].

La falta de una definición realmente armonizadora de los sujetos obligados no sólo distorsiona el mercado a través de la imposición de la conservación y el correlativo gasto de almacenamiento, sino que, indirectamente, las disparidades entre las legislaciones nacionales sobre qué operadores están o no obligados conlleva

---

[167] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 10. Conviene añadir que la Comisión realizó una declaración sugiriendo que se considerara la lista de delitos en la orden de detención europea. Se trata de la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros.

[168] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 10.

[169] Ibíd.

necesariamente discriminaciones en el marco del mercado único. Mientras que los grandes operadores presentes en varios Estados miembros se benefician de economías de escala en términos de costes, los operadores más pequeños de algunos Estados miembros tienden a crear empresas conjuntas o subcontratan a empresas que se especializan en funciones de conservación y recuperación de datos para reducir costes. Esta externalización de funciones técnicas no afecta, evidentemente, a la obligación de los proveedores de supervisar adecuadamente las operaciones de tratamiento de datos y garantizar que se cuenta con las medidas de seguridad necesarias, lo que puede ser problemático especialmente para los pequeños operadores. De hecho, estas circunstancias, constatadas por la propia Comisión, le han llevado a tomar la decisión a futuro de "examinar las cuestiones de seguridad de los datos y su impacto en las pequeñas y medianas empresas, por lo que respecta a las opciones para modificar el marco de la conservación de datos"[170]. Estamos, en conclusión, ante uno de los resultados insatisfactorios de la DCD, que debería ser revisado sin demora.

4.3 Sujetos afectados

Distintos de los sujetos *obligados* son los sujetos *afectados*, de cuya regulación se ocupa el art. 1.2 DCD[171]. Según el precepto, la Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. Además, el texto aclara seguidamente que no se aplicará al *contenido de las comunicaciones* electrónicas, "lo que incluye la información consultada utilizando una red de comunicaciones electrónicas"[172].

---

[170] Ibíd.

[171] Dispone el precepto literalmente que "2. La presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas".

[172] El artículo 1.2 de la Propuesta presentaba una redacción prácticamente idéntica, habiéndose producido tan sólo unos mínimos retoques estilísticos.

La Directiva entiende concretamente por *dato* —según la definición del art. 2.2.a) de la propia DCD— los "de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario", que es lo que ha de servir de referente al interpretar la norma. Por otra parte, respecto a qué ha de entenderse por *usuario*, baste remitirse al art. 2.2.b) DCD, que define "usuario" incluyendo a "toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público, con fines privados o comerciales, sin haberse por tanto necesariamente abonado a dicho servicio".

Aunque la determinación de estos elementos no parece suscitar dudas relevantes, vale la pena hacer constar en relación con la última definición y respecto de la referencia a *fines privados o comerciales*, la pregunta planteada por VILASAU[173] acerca de si acaso la misma comporta que se excluya del concepto de usuario para la aplicación de la DCD a las Administraciones Públicas. En su opinión, en el art. 1.2 DCD no parece contemplarse esta exclusión[174]. Aunque el interrogante sigue planteado a tenor del art. 2.2.b) DCD, no puede dejar de notarse, sin embargo, que esta exclusión no tendría mucho sentido, pues entre los datos del tráfico que se retienen se hallan los necesarios para "identificar el destino de una comunicación" —cf. art. 5.1.b) DCD—. En el caso de excluir de la obligación de retener los datos del tráfico relativos a las Administraciones, ello afectaría no sólo a los datos que generan las mismas en las comunicaciones entre sus órganos o con otras entes públicos, sino también aquellos otros supuestos en que una Administración se relaciona con terceros —como receptora u origen de una comunicación—[175].

---

[173] Cf. Vilasau Solana, M., La Directiva 2006/24/CE sobre conservación…, op. cit., p. 7.

[174] Ibíd.

[175] Por lo tanto, si se considera tan importante retener los datos respecto de un hipotético criminal, se desconocerían aquellos datos en los que el sujeto en cuestión se ha relacionado con la Administración. Si se predica que es tan indispensable poder retener los datos, no se justifica suficientemente que este supuesto quede excluido. Además respecto a las Administraciones, una parte de las comunicaciones que realizan los funcionarios y resto de personal (telefonía, acceso a internet), afecta a la esfera privada. ¿Cómo se podría separar y controlar esta actividad distinta de la propia de la Administración?

5 Definiciones

Aunque en el apartado anterior acabamos de adelantar parte de su contenido, el art. 2 DCD —bajo la rúbrica de "definiciones" y compuesto por dos apartados— incluye un breve glosario con algunos de los términos empleados en la norma y se remite, a efectos de interpretar los restantes a la batería de definiciones recogidas en directivas anteriores sobre materias conexas[176].

El hecho de que la DCD contenga un precepto donde se exponen interpretaciones auténticas de los términos técnicos empleados no es en absoluto novedoso en la normativa europea, pues también lo hacen otras directivas o reglamentos, elaborados

[176] Transcribimos aquí, para su examen directo por el lector, el tenor literal del artículo:

"Artículo 2. Definiciones.

1. A efectos de la presente Directiva, se aplicarán las definiciones de la Directiva 95/46/CE, de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco), y de la Directiva 2002/58/CE.

2. A efectos de la presente Directiva, se entenderá por:

a) «datos»: los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario;

b) «usuario»: toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público, con fines privados o comerciales, sin haberse necesariamente abonado a dicho servicio;

c) «servicio telefónico»: las llamadas (incluida la transmisión de voz, buzones vocales, conferencias y datos), los servicios suplementarios (incluido el reenvío o transferencia de llamadas) y los servicios de mensajería y servicios multimedia (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia);

d) «identificador de usuario»: un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a internet o a un servicio de comunicaciones por internet, o de su registro en uno de dichos servicios;

e) «identificador de celda»: la identidad de la celda desde la que se origina o termina una llamada de teléfono móvil;

f) «llamada telefónica infructuosa»: una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación o en la que ha habido una intervención por parte del gestor de la red".

sobre los modelos propuestos por UNCITRAL[177]. Debe valorarse positivamente que el legislador comunitario ofrezca tales clarificaciones, sobre todo cuando se trata de términos procedentes de una rama ajena al Derecho, como es el caso de la ingeniería de las telecomunicaciones. En algunas ocasiones, la definición sirve además para armonizar las divergentes interpretaciones que un mismo vocablo pueda encontrar en la legislación de los Estados miembros.

En el caso de nuestra norma, y respecto del contenido expresado en el art. 2 DCD, cabe señalar que su glosario recoge los siguientes términos. A efectos de la DCD, se entenderá por:

a) *datos*: los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario;

b) *usuario*: toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público, con fines privados o comerciales, sin haberse necesariamente abonado a dicho servicio;

c) *servicio telefónico*: las llamadas —incluida la transmisión de voz, buzones vocales, conferencias y datos—, los servicios suplementarios —incluido el reenvío o transferencia de llamadas— y los servicios de mensajería y servicios multimedia —incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia—;

---

[177] La Comisión de las Naciones Unidas para el derecho mercantil internacional, CNUDMI (o UNCITRAL, por su siglas en inglés *United Nations Commission for the Unification of International Trade Law*) fue creada por la Asamblea General de las Naciones Unidas mediante la Resolución 2205 (XXI) del 17 de diciembre de 1966 "para promover la progresiva armonización y unificación del derecho mercantil internacional". La CNUDMI lleva a cabo su función mediante sesiones anuales celebradas alternativamente en Nueva York y Viena.
La mayoría de las relaciones comerciales internacionales que se llevan a cabo hoy en día se basa en consultas efectuadas a la CNUDMI. Su finalidad es reducir los obstáculos legales que impiden el flujo del comercio internacional y armonizar las leyes mercantiles. Sobre la actividad de este órgano en la actualidad, puede consultarse su página web oficial, que contiene abundantísima información: http://www.uncitral.org/.

d) *identificador de usuario*: un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a internet o a un servicio de comunicaciones por internet, o de su registro en uno de dichos servicios;

e) *identificador de celda*: la identidad de la celda desde la que se origina o termina una llamada de teléfono móvil;

f) *llamada telefónica infructuosa*: una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación o en la que ha habido una intervención por parte del gestor de la red.

Estos seis términos deben unirse a todos los recogidos en las directivas a las que se remite expresamente el art. 2 DCD, a saber:

—la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Cf. articulo 2 —*Definiciones*—.

—la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas. Cf. artículo 2 —*Definiciones*—.

—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—. Cf. artículo 2 —*Definiciones*—.

Las definiciones recogidas en todas estas directivas constituyen el lexicón propio de la normativa europea sobre comunicaciones electrónicas. Por la utilidad que para el estudio e interpretación de nuestra normativa pueda representar tenerlos sistematizados y alfabetizados, hemos recopilado todos estos términos en un único documento que se puede consultar en uno de los Anexos de la presente Tesis.

Para finalizar este apartado, conviene reseñar que el artículo 2 de la Propuesta de Directiva coincidía sustancialmente, bajo similar rúbrica y estructura, con el artículo finalmente aprobado, y que acabamos de exponer. No obstante, aunque también se

remitía a las definiciones de las Directivas 95/46/CE, 2002/21/CE y 2002/58/CE, su glosario se limitaba a sólo dos términos: datos y usuario. Tales definiciones pasaron indemnes al texto en vigor pero vieron anadírseles las otras cuatro que hemos transcrito: servicio telefónico, identificador de usuario, identificador de celda y llamada telefónica infructuosa.

6 Obligación de conservar datos

La obligación de conservar los datos externos de las comunicaciones electrónicas constituye uno de los aspectos centrales de la normativa. El art. 3 DCD[178] —compuesto por dos apartados agrupados bajo la rúbrica *Obligación de conservar datos*— establece el deber de los Estados miembros de adoptar medidas que garanticen que los datos son conservados de conformidad con lo dispuesto en la DCD y en la medida en que sean *generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción* —art. 3.1) DCD—.

El contenido dispositivo del art. 3.1 se presenta, según sus propios términos, como una clara excepción a los arts. 5, 6 y 9 DPCE sobre la privacidad y las comunicaciones

[178] El tenor literal del artículo establece lo siguiente:

Artículo 3. Obligación de conservar datos.

1. Como excepción a los artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.

2. La obligación de conservar datos mencionada en el apartado 1 incluirá la conservación de los datos especificados en el artículo 5 en relación con las llamadas telefónicas infructuosas en las que los datos los generan o tratan, y conservan (en lo que a los datos telefónicos se refiere) o registran (en lo que a los datos de internet se refiere), proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo la jurisdicción del Estado miembro de que se trate en el marco de la prestación de los servicios de comunicaciones en cuestión. La conservación de datos en relación con las llamadas no conectadas no será obligatoria con arreglo a la presente Directiva.

electrónicas. Como ya vimos, estos artículos consagraron unas firmes garantías de privacidad a favor de los usuarios de las comunicaciones electrónicas, que la DCD viene ahora a excepcionar. Así, el art. 5.1 de dicha norma garantiza:

> "la confidencialidad de las comunicaciones y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados".

Además, por su parte, el art. 6 dispone que los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deben "eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación".

Finalmente, el art. 9.1 establece que en caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, "sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido".

Como se echa de ver, la obligación de conservación establecida por el art. 3.1 DCD se presenta como una amplísima excepción de los principios generales que rigen la materia, que son los establecidos en la Directiva 2002/58/CE. O mejor dicho, más que suponer una excepción a unos principios, el resultado es la inversión de la situación legislativa: en la práctica, la excepción pasa a ser la regla general. Los numerosos datos señalados por la DCD pasarán a conservarse, en tanto que los pocos que caen fuera de la obligación de conservación, deberán regirse por los artículos de la directiva. En el mejor de los casos, puede decirse que ambas legislaciones conviven en un paradójico régimen.

Tan compleja situación se agrava si la contemplamos desde la perspectiva de los derechos fundamentales implicados, en especial, el derecho a la protección de datos de carácter personal. Como los órganos dictaminantes ya pusieron de manifiesto durante la

tramitación de la norma, el art. 3.1 DCD[179] constituía la "disposición clave" de la misma al introducir la obligación de retener datos de tráfico y datos de localización, así como al dar efecto al principio de restricción de la finalidad[180]. Sin embargo, y a pesar de su relevancia, el precepto se limitaba únicamente a indicar que los datos se conservasen "de conformidad con lo dispuesto en la presente Directiva", sin incluir ulteriores referencias a las garantías de los titulares de los datos en otros artículos[181]. La ausencia de otras garantía en el texto llevó al GT29 a proponer al legislador medidas concretas cuya inclusión resultaba, a su entender aconsejable. Así, sugirió, entre otras garantías específicas, la separación de sistemas para la conservación, y que se obligara a que los sistemas de almacenamiento de datos a efectos de orden público estuvieran separados de los sistemas que los proveedores utilizan a efectos empresariales y protegidos por medidas de seguridad más rigurosas —por ejemplo, mediante encriptación— para impedir el acceso y el uso no autorizados[182]. Además, las medidas comunitarias deberían prever normas mínimas sobre medidas de seguridad técnicas y organizativas que deberían adoptar los proveedores, especificando los requisitos generales relativos a las medidas de seguridad establecidas en la Directiva CE/2002/58[183].

Estas propuestas y la denuncia generalizada de tan clamorosa carencia en materia de protección de la privacidad dio lugar a que finalmente se introdujera en el texto de la DCD un precepto que —si bien de forma muy genérica— se refiere a la protección y seguridad de los datos. El art. 7 DCD se ocupa de las garantías de los titulares de los

---

[179] La Propuesta de Directiva se ocupaba en su art. 3.1 de esta obligación de conservar datos, expresándose en términos sustancialmente parecidos. La redacción final sólo incluye ciertas mejoras técnicas en el tenor literal del precepto. Por su parte, el art. 3.2 de la Propuesta regulaba los aspectos relativos al acceso a los datos. Su contenido pasó a formar parte del vigente art. 4 DCD.

[180] Cf., vg., Dictamen del SEPD…, doc. cit., punto 49.

[181] Esta falta de concreción fue criticada por las autoridades de protección de datos. Así, vg. el GT29 consideraba que las medidas comunitarias debían prever normas mínimas sobre medidas de seguridad técnicas y organizativas que deberán adoptar los proveedores, especificando los requisitos generales relativos a las medidas de seguridad establecidas en la Directiva CE/2002/58. Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 10.

[182] Ibíd., nota anterior.

[183] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 11.

datos —calidad, normas de seguridad, acceso y destrucción— en los términos que analizaremos en posteriores apartados.

En todo caso, el periplo parlamentario de la DCD en este punto pone de manifiesto —como ha señalado VILASAU[184]— que el interés prioritario de la Directiva y de sus redactores no se focaliza en la protección de la intimidad o la protección de datos, sino más bien en tutelar y garantizar el interés de las autoridades receptoras de los datos. Así queda reflejado, por ejemplo, en el art. 8 DCD, donde se indica que los datos deben conservarse de tal forma que puedan transmitirse sin demora cuando las autoridades competentes así lo soliciten. "Resulta preocupante —remarca la misma autora— que el principal objetivo de la conservación adecuada fuera facilitar el acceso a los datos a las autoridades y no el de garantizar los derechos de los afectados" [185]. Si bien este aspecto se ha mejorado ligeramente en el texto definitivo, es sin duda revelador de las prioridades latentes en la aprobación de la DCD.

Finalmente, no podemos concluir este apartado sin hacer mención a dos categorías de datos que reciben un tratamiento específico por el art. 3 DCD, que los menciona expresamente con el fin de despejar posibles dudas de interpretación. Así, por un lado, el art. 3.2 DCD establece que la obligación de conservar datos incluye también la conservación de los datos especificados en el art. 5 DCD en relación con las *llamadas telefónicas infructuosas* en las que los datos los generan o tratan, y conservan —en lo que a los datos telefónicos se refiere— o registran —en lo que a los datos de internet se refiere— por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo la jurisdicción del Estado miembro de que se trate en el marco de la prestación de los servicios de comunicaciones en cuestión. Por otra parte, el mismo artículo concluye advirtiendo que la conservación de datos en relación con las *llamadas no conectadas* "no es obligatoria" con arreglo a la Directiva.

[184] Cf. VILASAU SOLANA, M., La Directiva 2006/24/CE sobre conservación…, op. cit., p. 9.

[185] Ibíd.

7 Categorías de datos que deben conservarse

Bajo la rúbrica de "categorías de datos que deben conservarse" y dividido en dos apartados, el art. 5 DCD[186] destaca como el más extenso del articulado y uno de los más

---

[186] A pesar de su extensión, parece conveniente ofrecer al lector el tenor literal del vigente artículo, de modo que pueda servir de guía durante el posterior comentario. El precepto dice así:

"Artículo 5. Categorías de datos que deben conservarse.

1. Los Estados miembros garantizarán que las siguientes categorías de datos se conserven de conformidad con la presente Directiva:

a) datos necesarios para rastrear e identificar el origen de una comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil:

i) el número de teléfono de llamada,

ii) el nombre y la dirección del abonado o usuario registrado;

2) con respecto al acceso a internet, correo electrónico por internet y telefonía por internet:

i) la identificación de usuario asignada,

ii) la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía,

iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo internet (IP), una identificación de usuario o un número de teléfono;

b) datos necesarios para identificar el destino de una comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil:

i) el número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas,

ii) los nombres y las direcciones de los abonados o usuarios registrados;

2) con respecto al correo electrónico por internet y a la telefonía por internet:

i) la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por internet,

ii) los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación;

c) datos necesarios para identificar la fecha, hora y duración de una comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la comunicación,

2) con respecto al acceso a internet, correo electrónico por internet y telefonía por internet:

relevantes de nuestra Directiva, en cuanto que delimita su alcance material. Mientras el

---

i) la fecha y hora de la conexión y desconexión del servicio de acceso a internet, basadas en un determinado huso horario, así como la dirección del Protocolo internet, ya sea dinámica o estática, asignada por el proveedor de acceso a internet a una comunicación, así como la identificación de usuario del abonado o del usuario registrado,

ii) la fecha y hora de la conexión y desconexión del servicio de correo electrónico por internet o del servicio de telefonía por internet, basadas en un determinado huso horario;

d) datos necesarios para identificar el tipo de comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado,

2) con respecto al correo electrónico por internet y a la telefonía por internet: el servicio de internet utilizado;

e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1) con respecto a la telefonía de red fija: los números de teléfono de origen y destino,

2) con respecto a la telefonía móvil:

i) los números de teléfono de origen y destino,

ii) la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada,

iii) la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada,

iv) la IMSI de la parte que recibe la llamada,

v) la IMEI de la parte que recibe la llamada,

vi) en el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio;

3) con respecto al acceso a internet, correo electrónico por internet y telefonía por internet:

i) el número de teléfono de origen en caso de acceso mediante marcado de números,

ii) la línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación;

f) datos necesarios para identificar la localización del equipo de comunicación móvil:

1) la etiqueta de localización (identificador de celda) al comienzo de la comunicación,

2) los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación".

segundo apartado se limita a especificar que de conformidad con la Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación[187], el apartado primero enumera las categorías de datos cuya conservación los Estados miembros deben garantizar. Concretamente, el apartado agrupa los datos en seis categorías, dentro de cada cual se especifican los datos que deben ser retenidos con respecto a: 1) la telefonía de red fija, 2) la telefonía móvil, y 3) el acceso a internet, correo electrónico por internet y telefonía por internet:

> a) datos necesarios para rastrear e identificar el origen de una comunicación:
>
> b) datos necesarios para identificar el destino de una comunicación:
>
> c) datos necesarios para identificar la fecha, hora y duración de una comunicación:
>
> d) datos necesarios para identificar el tipo de comunicación:
>
> e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:
>
> f) datos necesarios para identificar la localización del equipo de comunicación móvil:

Las circunstancias de la elaboración y tramitación de este artículo constituyen prueba irrefutable de cómo la Comisión Europea, al proyectar la presente normativa, se guió fundamentalmente por intereses de eficacia policial. Así, el art. 4 PDCD recogía una relación de categorías similar a la finalmente aprobada, pero se remitía a un anexo que desgranaba todos y cada uno de los datos a retener dentro de las categorías que previamente habían sido establecidas en el proyectado artículo 4. Dicho anexo había de ser objeto de revisión regularmente —"en la medida que fuera necesario"— de acuerdo

[187] Literalmente, el art. 5.2 DCD dispone que: "De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación".

con el procedimiento establecido en el art. 6 PDCD. Concretamente, una comisión se ocuparía de su revisión[188].

Las contundentes críticas a esta fórmula provocaron que finalmente el listado detallado de datos fuera incluido en el articulado, en cuya conveniencia coincidieron todos los organismos que tuvieron que dictaminar sobre la Propuesta. Así, el CESE consideró inadecuado que —mediando la limitación del derecho fundamental al secreto de las comunicaciones— no interviniera el Parlamento Europeo para la ampliación o reducción de las categorías de datos que debían conservarse y se recurriera a esta metodología propia de la ejecución de normas técnicas y de carácter neutro, lo que las normas de conservación de datos distan mucho de ser[189]. Las mismas razones fueron sostenidas por el GT29, para el que la propia DCD debía especificar directamente en su articulado la lista de datos personales a conservar, puesto que tal determinación resultaba importante para calibrar exactamente el impacto en los derechos y libertades fundamentales de los ciudadanos afectados "teniendo en cuenta los riesgos para su esfera personal y teniendo en cuenta también las cuestiones relativas a la garantía de la exactitud y la actualización de los datos conservados" [190]. A mayor abundamiento, consideraba el Grupo que toda propuesta de cambios en la lista de los tipos de datos a conservar debía someterse a una prueba de estricta necesidad, y que la revisión de dicha lista debía realizarse sólo con la aprobación del Parlamento Europeo y con la participación de las autoridades responsables de protección de datos, los representantes de asociaciones de consumidores y usuarios, otros órganos no gubernamentales pertinentes y las asociaciones europeas del sector de las comunicaciones electrónicas[191]. El propio Parlamento Europeo —como era de esperar— se pronunció en un sentido similar, señalando que no era correcto establecer en un anexo los datos a

[188] El proyectado precepto no incluía un segundo apartado —como el vigente art. 5 DCD— que especificara que no se podría conservar dato alguno que revelase el contenido de la comunicación.

[189] Cf. Dictamen del CESE…, doc. cit., punto 2.4.6.

[190] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 14.

[191] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 10-11.

retener, pues se trataba de un punto sobre el que necesariamente debía pronunciarse el propio Parlamento sin que pudiera dejarse a la mera voluntad de la Comisión[192].

En una posición más moderada, el SEPD acogió el artículo alabando la técnica legislativa elegida, con descripciones funcionales en el articulado de la Directiva y con detalles técnicos en un anexo, lo que consideraba suficientemente flexible para responder de forma adecuada a los progresos tecnológicos y da seguridad jurídica al ciudadano [193]. No obstante, respecto de la posibilidad de revisión del Anexo por una "directiva de la Comisión", el Supervisor no dudó en aconsejar que aquellas revisiones que tuvieran un impacto significativo en la protección de datos se hicieran de preferencia a través de una directiva mediante el procedimiento de codecisión[194].

En definitiva, como resultado de esta concurrencia de opiniones negativas por parte de los órganos dictaminantes contra el proyectado anexo y su posible revisión vía el procedimiento de "comitología", el texto definitivo finalmente pasó a fijar en el art. 5 DCD la relación completa y detallada de todos los datos a conservar, cuya conveniencia es manifiesta a la luz de los argumentos que acabamos de exponer.

---

[192] Según su parecer, no podía aceptarse el procedimiento de comitología propuesto por la Comisión, en cuyo seno "los representantes de la Comisión y de los Estados miembros podrán modificar la lista de los datos que deben conservarse sin la participación del Parlamento europeo y las empresas concernidas. Cada ampliación de los tipos de datos que deben conservarse tiene una incidencia clara en los derechos fundamentales y debe someterse a la consideración del Parlamento". Por tanto, concluía que el artículo debía suprimirse. Cf. Informe sobre sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)), elaborada por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior. En concreto, la Comisión de Industria, Investigación y Energía propuso sumprimir en las enmiendas n. 18, 19 y 20 los arts. 4.2, 5 y 6 de la Propuesta. Puede consultarse el documento en su edic. oficial http://www.europarl.europa.eu/omk/sipade3?PUBREF=-//EP//NONSGML+REPORT+A6-2005-0365+0+DOC+PDF+V0//ES&L=ES&LEVEL=2&NAV=S&LSTDOC=Y, pp. 40-41 y 50-51.

[193] Cf. Dictamen del SEPD…, doc. cit., punto 59.

[194] Cf. Dictamen del SEPD…, doc. cit., punto 60. Véase, en el mismo sentido, el Dictamen del SEPD de 23 de marzo de 2005 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el sistema de información de visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros, punto 3.12.

Más allá de las particulares vicisitudes de la redacción del art. 5 DCD, debemos ahora centrarnos en el análisis del resultado final.

Un comentario completo del art. 5 DCD nos invita a exponer ahora tres relevantes distinciones en esta materia: la primera, la diferencia entre datos externos y datos internos de las comunicaciones electrónicas; la segunda, las distintas clases de datos externos de las comunicaciones electrónicas; y la tercera, la selección y clasificación de los datos externos a conservar llevada a cabo por el art. 5 DCD.

En cuanto a la primera distinción, hemos de indicar que, dentro de cualquier comunicación electrónica, podemos distinguir una vertiente material —lo que normalmente denominaríamos *contenido* o *mensaje*— y otra formal —los *datos externos* o *de tráfico*, que hacen posible la comunicación electrónica y a veces simplemente la acompañan[195]—. Estos datos son definidos en el art. 2.b) DPCE como "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de facturación de las mismas"[196].

Tanto la vertiente material como la formal de las comunicaciones electrónicas pueden tener información relevante. En cuanto a los datos de tráfico, su trascendencia radica precisamente en que también aportan información indirectamente acerca del contenido o de los comunicantes, ya sea como consecuencia de que se trataron para hacer posible la comunicación o porque se transmitieron accesoriamente al contenido material. Por su parte, el contenido o mensaje tiene importancia por sí mismo, ya que es la información que el emisor desea transmitir al receptor. Como hemos señalado, el art. 1.2 DCD excluye la conservación de la vertiente material de las comunicaciones electrónicas, al indicar que sus disposiciones no se aplicarán al contenido de las comunicaciones electrónicas, "lo que incluye la información consultada utilizando una red de comunicaciones electrónicas" —léase: internet—. El art. 5.2 DCD abunda en la misma idea de excluir la vertiente material de la comunicación, estableciendo que de

[195] Al respecto, González López, J. J., Los datos..., op. cit., pág. 138 y ss.

[196] GONZÁLEZ LÓPEZ ha criticado esta distinción en *González López, J. J., Los datos de tráfico de las comunicaciones electrónicas en el proceso penal*, La Ley, Madrid, 2007, pág. 29 y ss.

conformidad con la norma, no podrá conservarse ningún dato que revele el contenido de la comunicación[197].

En cuanto a las distintas clases de datos externos de las comunicaciones electrónicas, es posible diferenciar tres categorías principales de datos vinculados a las mismas. Ninguna de ellas constituye, en principio, parte del contenido que el emisor pretende transmitir al receptor.

En primer lugar, nos encontramos con los llamados "datos de tráfico" *stricto sensu*. Su definición expresa en el marco comunitario vigente viene dada por el art. 2.b) DPCE, que ya hemos reproducido[198]. La DCD abraza esta definición cuando advierte en su art. 2.1 DCD que, a sus efectos, se aplicarán las definiciones de la Directiva 95/46/CE, de la Directiva 2002/21/CE y de la Directiva 2002/58/CE.

---

[197] Este último apartado es el resultado de una sugerencia del SEPD, quien recomendó incluir en el anexo de la Propuesta de Directiva criterios más sustanciales que aseguraran que los datos de contenido no fueran incluidos en la conservación, para lo cual proponía la inclusión de una cláusula conforme a la cual "el anexo no podrá incluir datos que revelen el contenido de una comunicación". Tal sugerencia cobró forma en lo que finalmente vino a ser el art. 5.2 DCD

[198] Dicha definición ha sido incorporada expresamente a nuestro ordenamiento jurídico en el art. 64 a) del RD 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Aunque se trata de una definición meritoria, por cuanto contribuye a clarificar el concepto, la misma no ha sido pacíficamente aceptada por la doctrina, por estimarla excesivamente reducida y excluyente de diversas categorías de datos que también deben considerarse «de tráfico» por su carácter accesorio a la comunicación, siendo lo cierto que, hasta la fecha, ninguna de las definiciones o conceptos proporcionados normativa o jurisprudencialmente ha merecido el apoyo unánime de la doctrina, a partir de diversos argumentos. Críticos con este concepto se muestran CORRIPIO GIL-DELGADO, M.ª 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, Agencia de Protección de Datos, Madrid, 2001, Premio Protección de Datos Personales, pág. 188, y RODRÍGUEZ LAINZ, J. L., Intervención judicial en los datos de tráfico de las comunicaciones, Bosch, Barcelona 2003, pág. 30.

En segundo término, han de mencionarse los "datos de localización". Son definidos en el art. 2.c) DPCE como "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible al público". La propia Directiva aclara en su considerando dñecimocuarto que tales datos pueden referirse a la latitud, la longitud y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de red en la que está localizado el equipo terminal en un determinado momento a la hora en que la información de localización ha sido registrada. Aunque conforme a un concepto amplio de "datos de tráfico", los datos de localización tratados en el curso de la comunicación[199], y distintos de aquellos precisos a efectos de permitir la realización de la comunicación, se hallarían incluidos en el concepto precedente —vg. los GPSs—, el propósito de la Directiva 2002/58/CE es precisamente deslindarlos, de manera que se sujeten a regímenes de protección diversos.

Dentro de los datos de localización pueden distinguirse a su vez dos categorías. Por un lado, nos encontramos los "datos de cobertura", esto es, los tratados por los operadores de comunicaciones a fin de ubicar en el espectro radioeléctrico los terminales de telefonía móvil. La telefonía móvil se apoya en la inclusión del concreto equipo terminal en el área —celda— cubierta por una determinada antena de telefonía —o satélite, en su caso— encargada de enviar la señal a efectos de realizar la eventual comunicación telefónica, la cual cambia al desplazarse el usuario y ubicarse en el área cubierta por una celda distinta. Por otro lado, están los "datos de localización distintos de los de tráfico", a que alude la DPCE en su art. 9. Aunque la denominación empleada por la directiva podría inducir a confundirlos con la anterior categoría, somos de la opinión de que el diferente régimen jurídico que se establece para estos datos respecto de los de tráfico se fundamenta en su distinción respecto de los "datos

[199] No cabe duda de que determinados datos de localización son tratados al margen de las comunicaciones efectivamente realizadas, pues, atendida la definición que proporciona la Directiva, deben considerarse datos de localización los tratados por los operadores de comunicaciones electrónicas a fin de ubicar en el espectro radioeléctrico, verbigracia los equipos terminales de telefonía móvil, aun en el caso de que en ese momento no se esté produciendo una comunicación.

de cobertura", equiparados a los de tráfico a efectos de la habilitación a los operadores para su tratamiento. Entendemos, en consecuencia, que el art. 9 se refiere a datos como los de GPS o similares, que los operadores tratan a efectos de prestación de servicios de valor añadido[200].

Finalmente, y en tercer lugar, además de los "datos de localización", encontramos otras informaciones de existencia anterior al proceso de comunicación, que se han calificado como "datos de suscripción" o "datos de abonado"[201]. Para disponer de una conexión telefónica es preciso celebrar un contrato con el operador de comunicaciones electrónicas, en virtud del cual se facilitan determinadas informaciones personales como la identidad, número de cuenta, etc. De igual manera, para disponer de una conexión a internet, se debe celebrar un contrato con el proveedor de acceso al mismo, que dispondrá igualmente de diversa información relativa al abonado. Ahora bien, estos datos no se limitan a la identificación del tal abonado, sino que también comprenden determinadas informaciones relativas al servicio cuya prestación se contrata. En este sentido, de acuerdo con la Memoria Explicativa del Convenio sobre el Cibercrimen, de 23 de noviembre de 2001, los "datos de suscripción" son "cualquier información contenida en formato informático o en cualquier otra forma, que es mantenida por el proveedor de servicios, relativa a usuarios de sus servicios, distintos de los de tráfico o de contenido, por los que puede establecerse: el tipo de servicio de comunicación usado, las previsiones técnicas adoptadas para ello y el período de servicio; la identidad del usuario, dirección postal o geográfica, teléfono u

---

[200] De acuerdo con el art. 2.g) de la Directiva 2002/58/CE, son «servicios de valor añadido», «todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación».
Se entiende así la afirmación realizada en Loza Corera, M. y Rodríguez Casal, C., «Nueva legislación europea en materia de protección de datos», en Diario La Ley, n.º 5549, 22 de mayo de 2002, pág. 2, de que los datos de localización, «más precisos de lo necesario para la transmisión de la comunicación» no son «meros datos de tráfico». Como veremos, los datos de GPS no son en ningún caso necesarios para hacer posible la conducción de la comunicación, sino que se tratan como servicio de valor añadido.

[201] Definidos como aquellos que constituyen «la información personal recabada del abonado a la hora de suscribir el contrato de prestación de servicios de comunicación», Hernández Guerrero, F. J., «La intervención de las comunicaciones electrónicas», Estudios Jurídicos del Ministerio Fiscal, III-2001, pág. 355.

otro número de acceso, información sobre cuentas corrientes y pago, disponible sobre la base de un contrato de servicio o acuerdo; cualquier otra información sobre el lugar de instalación del equipo de comunicaciones disponibles sobre la base del contrato de servicios o de un acuerdo".

De la celebración de un contrato de prestación de servicios entre un abonado y un operador o prestador de servicios de comunicaciones electrónicas se deriva una serie de datos referidos tanto al abonado —y, en su caso, usuario, cuando la prestación del servicio se contrata para varios usuarios individualizados— como al propio servicio contratado y al terminal del que se sirve el abonado, caso de la IMSI y la IMEI, en relación con la telefonía móvil[202]. La característica común a estos datos es que se trata de información vinculada a la comunicación en cuanto servicio prestado por un sujeto —intermediario técnico— a otro —abonado—, pero que no aparece con motivo de las concretas operaciones técnicas necesarias para hacer factible la comunicación pretendida, sino como marco previo para que esas actuaciones se lleven a cabo.

A estas tres clases de datos externos nos referimos cuando hablamos de la medida de conservación de datos cubierta por la DCD. El art. 2.2.a) DCD es claro en este punto, al indicar que "a efectos de la presente Directiva, se entenderá por "datos" los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario".

Respecto de las seis categorías recogidas en el art. 5.1 DCD junto con sus especificaciones, la diferenciación entre los datos sobre telefonía y los datos de internet debe valorarse positivamente pues —como bien observó el SEPD— a pesar del hecho de que llegue con el tiempo a ser menos relevante, desde la perspectiva de la protección de datos se trata de una distinción importante, dado que en internet no está bien

[202] La IMSI (International Mobile Subscriber Identity) es un código de identificación único para cada dispositivo de telefonía móvil, representado por una serie de algoritmos, que se integra en la tarjeta SIM y que su identificación a través de las redes GSM y UMTS. La IMEI (International Mobile Equipment Identity), por su parte, es un código de identificación, también incorporado a la tarjeta SIM, que identifica unívocamente el aparato de telefonía móvil a nivel internacional.

delimitada la frontera entre datos de contenido y datos de tráfico[203]. Al contrario de lo que sucedía en el malogrado proyecto de Decisión marco —que contenía una lista mínima con un margen amplio para que los Estados miembros añadieran datos— desde la perspectiva de la protección de datos la armonización completa había de considerarse un aspecto primordial.

Estas categorías establecidas en la Directiva deben interpretarse como una relación *numerus clausus*, que no permite imponer a los operadores obligaciones adicionales de conservación de datos[204]. La conveniencia de delimitar taxativamente los concretos tipos de datos que deben retenerse resulta igualmente importante si la contemplamos desde la perspectiva de la proporcionalidad de la medida y su injerencia en los derechos fundamentales[205].

La lista exhaustiva de las categorías de los datos del art. 5 DCD ha sido uno de los pocos aspectos de la materia en los que se ha alcanzado sin duda un alto nivel de armonización. Al analizar la transposición del art. 5 DCD, la Comisión Europea llegó a la conclusión en su Informe de Evaluación de 2011 de que veintiún Estados miembros han previsto en su legislación de transposición la conservación de cada una de estas

---

[203] Cf. Dictamen del SEPD…, doc. cit., punto 59.

[204] Aunque tal conclusión se extrae de una lectural integral del articulado, el GT29 lo ha dado sentado en su Informe sobre la segunda medida de ejecución, en los siguientes términos: "it should be recalled that directive 2006/24/EC derogates from the provisions of directive 2002/58/EC and the list of traffic data that have to be retained on a mandatory basis is to be regarded as exhaustive – i.e., no additional data retention obligations may be imposed on providers pursuant to the DR directive". Cf. Report 01/2010 on the second joint…, doc. cit., p. 10.

[205] Así, por ejemplo, lo puso de manifiesto el GT29 en lo que se refería a los datos de uso de internet. Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 2. El GT29 consideraba asimismo, preferible la conservación de un conjunto de datos máximo que el establecimiento de una lista mínima. En concreto, los datos que debían conservarse, a su parecer, habrían de "limitarse a los recogidos por los proveedores para fines técnicos y de facturación".

categorías de datos[206]. Al parecer —y según advierte el propio Informe—, los Estados miembros han manifestado a la Comisión que no consideran necesario modificar las categorías de datos que deben conservarse, si bien el Parlamento Europeo envió a la Comisión una declaración escrita pidiendo que el ámbito de la DCD se amplíe a los motores de búsqueda "para luchar rápidamente contra la pornografía infantil en línea y los abusos sexuales"[207].

Finalmente, en lo que se refiere al volumen de datos que se conservan en la práctica, vale la pena señalar que la cantidad y volumen de datos conservados a los que han accedido las autoridades nacionales competentes ha ido incrementando con el paso del tiempo[208]. De acuerdo con las estadísticas para 2008 y 2009 facilitadas a la Comisión por diecinueve Estados miembros, en cada uno de estos años se presentaron más de dos millones de solicitudes de datos, con grandes diferencias —eso sí— entre los Estados miembros; la cuantía varía desde las menos de cien al año en Chipre hasta más allá del millón en Polonia. Según la misma fuente, el tipo de datos solicitado con mayor frecuencia en el mismo período estaba relacionado con la telefonía móvil[209]. Como la propia Comisión ha reconocido, no hay una explicación clara para todas estas variaciones, aunque el tamaño de la población, las tendencias delictivas predominantes,

---

[206] Bélgica no ha previsto los tipos de datos de telefonía que deben conservarse, ni tampoco cuenta con ninguna disposición sobre los datos relacionados con Internet. Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 15.

[207] Cf. Declaración escrita de conformidad con el artículo 123 del Reglamento interno sobre la creación de un sistema europeo de alerta rápida contra los pederastas y los delincuentes sexuales (19.4.2010, 0029/2010). También se ha aclarado posteriormente que las búsquedas, es decir, los registros del servidor generados mediante la oferta de un servicio de motor de búsqueda, tampoco se incluyen en el ámbito de aplicación de la Directiva, pues se consideran contenido y no datos de tráfico. Cf. Dictamen del GT29, de 4 de abril de 2008, sobre cuestiones de protección de datos relacionadas con los motores de búsqueda.

[208] Cf. punto 5.1 del Informe de la Comisión

[209] Las estadísticas no indican la finalidad precisa para la que se presentó cada solicitud. La República Checa, Letonia y Polonia señalaron que, en el caso de los datos de telefonía móvil, las autoridades competentes tenían que presentar la misma solicitud a cada uno de los principales operadores de telefonía móvil y que, por tanto, las cifras reales de solicitudes por caso eran considerablemente inferiores a lo que arrojaban las estadísticas. Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 24.

las limitaciones de fines y las condiciones para el acceso y los costes de la adquisición de datos son sin duda factores relevantes[210].

8 Períodos de conservación

El período de conservación de los datos de tráfico está regulado en el art. 6 DCD[211] que —bajo la rúbrica de "períodos de conservación"— dispone que los Estados miembros han de garantizar que las categorías de datos indicadas en el art. 5 DCD se conserven por un período de tiempo no inferior a seis meses ni superior a dos años a partir de la fecha en que tuvo lugar la comunicación. Este plazo máximo de dos años puede ser ampliado ante circunstancias especiales, en los términos previstos en el art. 12 DCD, de los que nos ocuparemos en el siguiente apartado[212].

Al analizar este artículo, hemos de empezar recordando que tanto la Directiva 97/66/CE como por su sucesora, la vigente Directiva 2002/58/CE establecieron un principio general sobre el período de conservación de los datos de las comunicaciones electrónicas. Ambas normas, al tiempo que desarrollaban los principios de la Directiva 95/46/CE en los servicios de telecomunicaciones, establecieron en su art. 6 que los datos sobre tráfico relacionados con los usuarios y abonados tratados para establecer comunicaciones y almacenados por el proveedor de una red o servicio público de telecomunicación deben destruirse o hacerse anónimos en cuanto terminase la comunicación, excepto aquellos necesarios a efectos de la facturación de los usuarios

---

[210] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 25.

[211] Transcribimos aquí el tenor literal del precepto: "Artículo 6. *Períodos de conservación.* Los Estados miembros garantizarán que las categorías de datos mencionadas en el artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación".

[212] Nada se dice en nuestra LCD sobre esta posibilidad, como más adelante examinaremos.

hasta la expiración del plazo durante el cual pueda impugnarse la factura o cuando el abonado hubiera dado su consentimiento[213].

La aplicación y desarrollo de este principio de la Directiva 97/66/CE en las legislaciones internas de los Estados miembros dieron lugar a divergencias importantes en cuanto a los períodos efectivos de conservación. Tan pronto como septiembre de 1999, el GT29, en su *Recomendación 99/3*[214], había ya observado que los plazos de conservación de los servicios de telecomunicaciones variaba significativamente entre los Estados miembros. Por ejemplo, en Alemania los operadores de telecomunicaciones y los proveedores de servicios de telecomunicación podían almacenar los datos necesarios para facturación durante un plazo máximo de ochenta días a efectos de

[213] cf. art. 6 Directiva 97/66/CE

[214] Reunión de Ministros de Justicia e Interior de los Ocho, 9-10 de diciembre de 1997, Comunicado, Washington D.C., 10 de diciembre, Anexo al comunicado: Principios y plan de acción para combatir el delito de alta tecnología. En el comunicado oficial adoptado en Washington los días 9 y 10 de diciembre de 1997 sobre principios y un plan de acción de diez puntos para luchar contra la delincuencia de alta tecnología, los Ministros de Justicia e Interior del G8 declararon lo siguiente: "es el sector industrial el que diseña, despliega y mantiene estas redes globales, y él es el responsable principal de la elaboración de normas técnicas. Así pues, corresponde al sector industrial desempeñar su parte en el desarrollo y la distribución de sistemas seguros diseñados para ayudar a detectar el abuso informático, conservar las pruebas electrónicas y contribuir a determinar la situación e identidad de los delincuentes". Extraído de la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones - Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.
Históricamente, sin embargo, hasta los primeros años del siglo XXI, los Estados miembros no mostraron interés por la adopción de medidas de conservación de datos de las comunicaciones electrónicas con fines penales. De hecho, sólo fue a partir de la popularización de internet y la telefonía móvil a finales de los años noventa cuando las autoridades policiales empezaron a estudiar la posibilidad de arbitrar medidas que les permitieran vigilar el tráfico de datos en las comunicaciones electrónicas. Un importante hito en este proceso fue la reunión en Washington de los Ministros de Justicia e Interior de los países del G-8, los días 9 y 10 de diciembre de 1997, como resultado de la cual los Estados adoptaron un plan de acción de diez puntos que habían de ponerse en práctica con ayuda de un Subgrupo Especializado en Delitos de Alta Tecnología, formado por representantes de las autoridades policiales de estos países. Uno de los apartados más destacados del plan, y sin duda el más novedoso, era la necesidad de establecer medidas de conservación de los datos sobre tráfico, tanto histórico como futuro, por parte de los proveedores de internet a efectos de cumplimiento de las disposiciones legislativas y su puesta a disposición de las autoridades policiales

demostrar la corrección de la factura. En Francia, dependía del tipo de operador: un operador de telecomunicaciones tradicional podía conservar los datos sobre tráfico hasta un año, basándose en la ley que fijaba el plazo de impugnación de la factura. Este plazo quedaba fijado en diez años para los demás operadores. En Austria, la ley sobre telecomunicaciones no fijaba ningún plazo concreto para guardar los datos sobre tráfico a efectos de facturación, sino que lo limitaba al plazo durante el cual podía impugnarse la factura o exigirse el pago. En Reino Unido, de conformidad con la ley, la factura podía impugnarse durante seis años, pero los operadores y proveedores de servicio almacenaban los datos pertinentes durante unos dieciocho meses. En Bélgica, la ley no definía el plazo, pero el mayor proveedor de servicios de telecomunicación lo establecía en tres meses en sus condiciones generales. Otra práctica distinta se observaba en Portugal pues, dado que el plazo no estaba fijado por ley, la autoridad nacional de control de la protección de datos decidía de manera individualizada. En Noruega, por su parte, el plazo estaba fijado en sólo catorce días. Tampoco era homogénea la práctica de los proveedores de internet pues, como observaba el GT29, mientras los pequeños proveedores conservaban los datos sobre tráfico durante períodos muy breves —apenas unas horas— debido a falta de capacidad de almacenamiento, los proveedores más importantes podían permitirse conservar los datos sobre tráfico durante varios meses.

Todas estas divergencias —advertía el Grupo— podían plantear obstáculos en el mercado interior para la prestación transfronteriza de servicios de telecomunicación e internet, al tiempo que la existencia de plazos tan diferentes podía dificultar el control del cumplimiento legislativo, pues se podía dar el caso de que un proveedor de internet establecido en un Estado miembro no tuviera derecho a almacenar datos sobre tráfico durante más tiempo del permitido en el Estado miembro donde el cliente utilizara sus servicios, o bien que se viera obligado a conservar los datos sobre tráfico durante más tiempo del permitido en su propio Estado miembro porque el país de los usuarios así lo exigiera legalmente. A la vista de estas disparidades, el Grupo recomendó a la Comisión que propusiera medidas apropiadas para una mayor armonización del plazo durante el cual se permitía a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de internet conservar los datos sobre tráfico para facturación y pago de interconexiones. Este plazo debía a su entender ser suficiente para permitir a los consumidores impugnar la factura, pero lo más breve

posible para no sobrecargar a los operadores y proveedores de servicios y para respetar los principios de proporcionalidad y especificidad como componentes del derecho a la intimidad. En concreto, el GT29 recomendaba que el plazo debía ser conforme con los mayores niveles de protección observados en los Estados miembros, al tiempo que subrayaba el hecho de que en varios Estados miembros se habían aplicado satisfactoriamente plazos no superiores a tres meses.

La recomendación del GT29 sobre la necesidad de armonizar estos períodos no tuvo ningún efecto inmediato.

Pocos años después, ya entrado el nuevo siglo, varios Estados miembros adoptaron legislación que preveía la conservación de datos por los prestadores de servicios para la prevención, investigación, detección y enjuiciamiento de delitos. La competencia de los Estados miembros para adoptar este tipo de normas descansaba en que los tratamientos de datos que tuvieran por objeto "la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal" no estaban comprendidas en el ámbito de aplicación del Derecho comunitario, y por tanto, estaban excluidos del ámbito de aplicación de las Directivas 95/46/CE y 97/66/CE. Los Estados podían disponer la prolongación del período de tratamiento de los datos con estos fines penales y de seguridad en los ficheros ya existentes, o la creación de bases de datos especiales con los mismos fines por parte de los proveedores, estableciendo los plazos de conservación que tuvieran por convenientes.

De hecho, así lo hicieron, y los períodos de conservación de los datos de las comunicaciones electrónicas en este tipo de normativas se convirtió en uno de los aspectos divergentes que, junto con las demás "diferencias legales y técnicas entre disposiciones nacionales sobre conservación de datos con fines de prevención, investigación, detección y enjuiciamiento de delitos" creaban "obstáculos en el mercado interior de las comunicaciones electrónicas" en cuanto a los requisitos que los prestadores de servicios debían cumplir, lo que justificaba en parte la adopción de la DCD[215]. Es sobre estas legislaciones nacionales sobre las que la Comisión abordó su

[215] considerando sexto de la DCD

actividad "armonizadora", determinando en el art. 6 DCD que los Estados miembros han de garantizar que las categorías de datos indicadas en el art. 5 DCD se conserven por un período de tiempo no inferior a seis meses ni superior a dos años a partir de la fecha en que tuvo lugar la comunicación.

Vuelta la mirada sobre los estudios y debates previos a la tramitación de la DCD, la delimitación de estos plazos de conservación no se abordó con concreción en las primeras fases. Las *Conclusiones* del Consejo de Justicia e Interior de 19 de diciembre de 2002 se refirieron "a un período limitado de tiempo" [216], en tanto que la *Comunicación de la Comisión Europea COM(2000) 890 final al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones* reconocía la complejidad de la materia, indicando que las medidas propuestas debían ser "adecuadas, necesarias y proporcionadas, de acuerdo con el derecho comunitario y el derecho internacional", y que la Comisión consideraba que "cualquier solución al complejo problema de la conservación de los datos sobre tráfico deb[ía] tener un buen fundamento, ser proporcionada y lograr un equilibrio justo entre los distintos intereses en juego de las partes implicadas"[217]. Lo mismo puede decirse de las declaraciones político-legislativas del Consejo en los años siguientes, que se limitaron a prever en abstracto la aprobación de la medida.

El Proyecto de Iniciativa presentado por Francia, Irlanda, Reino Unido y Suecia en abril de 2004, con vistas a la adopción por el Consejo de una decisión marco sobre la conservación de los datos[218], regulaba en su art. 4 los plazos de conservación de los

---

[216] Ibíd., punto 6 del apartado Tecnologías de la información y la investigación y la acción penal contra la delincuencia organizada. Sesión nº 2477 del Consejo - Justicia y Asuntos de Interior - Bruselas, 19 de diciembre de 2002, C/02/404.

[217] Apart. 5.2, Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, sobre la creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos (eEurope 2002/COM/2000/0890 final). Texto íntegro accesible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0890:ES:HTML

[218] El título completo del documento era Proyecto de Decisión marco sobre la conservación de los datos tratados y almacenados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o el suministro de datos en redes públicas de comunicaciones a efectos de la prevención,

datos, estableciendo que cada Estado miembro adoptaría las medidas necesarias para garantizar que los datos se conservasen durante un plazo no inferior a doce meses ni superior a treinta y seis meses desde su generación. Los Estados miembros podrían disponer plazos mayores de conservación de los datos atendiendo a criterios nacionales, siempre que dicha conservación constituyera una medida necesaria, adecuada y proporcionada en el seno de una sociedad democrática[219].

Por su parte, el art. 7 PDCD, bajo la rúbrica de "períodos de conservación", establecía unos plazos distintos y más breves de los que finalmente están en vigor; la generalidad de los datos que mencionaba el artículo 4 y el Anexo debían conservarse durante un período de un año a partir de la fecha de la comunicación, en tanto que el plazo se reducía a seis meses para los datos relacionados con comunicaciones electrónicas que tuvieran lugar entera o principalmente a través de *Protocolo internet* (*sic* en la traducción oficial)[220]. Además, el art. 12 PDCD establecía que, a más tardar tres años desde la fecha límite de transposición, la Comisión debía presentar al Parlamento Europeo y al Consejo una evaluación de la aplicación de esta Directiva y su impacto en operadores económicos y consumidores, teniendo en cuenta los elementos estadísticos proporcionados a la Comisión a fin de determinar si era necesario modificar las

---

investigación, descubrimiento y represión de la delincuencia y de las infracciones penales, con inclusión del terrorismo, presentada por la República Francesa, Irlanda, el Reino de Suecia y el Reino Unido el 28 de abril de 2004 (CNS/2004/0813). El texto íntegro en su publicación oficial es accesible en el siguiente enlace: http://register.consilium.eu.int/pdf/es/04/st08/st08958.es04.pdf

[219] El considerando 12 advertía que "Se podrán conservar datos a priori durante períodos de tiempo variables en función del tipo de datos. Los plazos de conservación para cada tipo de datos dependerán de la utilidad de los datos en relación con la prevención, investigación, descubrimiento y represión de la delincuencia y las infracciones penales, así como del coste de su conservación. Los plazos de conservación serán proporcionados respecto de las necesidades de estos datos a efectos de prevención, investigación, descubrimiento y represión de la delincuencia y las infracciones penales, en contraposición con la intrusión en la vida privada que conllevará esta conservación en caso de revelación de los datos conservados".

[220] Reproducimos aquí el texto íntegro del artículo proyectado: "Artículo 7. *Períodos de conservación.* Los Estados miembros se asegurarán de que las categorías de datos mencionados en el artículo 4 se conserven durante un período de un año a partir de la fecha de la comunicación, a excepción de los datos relacionados con comunicaciones electrónicas que tengan lugar entera o principalmente a través del Protocolo Internet. Estos últimos se conservarán durante un período de seis meses".

disposiciones de la Directiva, "en particular, por lo que se refiere al período de conservación previsto" en el art. 7.

El establecimiento de estos períodos intentó presentarse por parte de la Comisión como un planteamiento equilibrado entre los intereses de los distintos actores implicados, a saber: las organizaciones europeas de las telecomunicaciones y de la industria de internet, los representantes de las autoridades de protección de datos y de asociaciones pro derechos civiles y las autoridades policiales.

De acuerdo con el relato de hechos que se contiene en la Exposición de Motivos de la PDCD, la industria de las telecomunicaciones había manifestado a la Comisión que un período de conservación largo generaría costes considerables, abogando en todo caso, por períodos de conservación no superiores a seis meses, ya que muchos de los datos que los servicios represivos solicitaban no sobrepasaban este plazo.

Por su parte, los representantes de las autoridades de protección de datos y de asociaciones de derechos civiles alegaron que la conservación de los datos suponía una interferencia en la vida privada de los ciudadanos, por lo que los períodos de conservación deberían ser lo más breves posible. En general, cuestionaron la proporcionalidad de los períodos de conservación superiores a seis meses.

Finalmente, las autoridades represivas indicaron que la conservación debía extenderse el tiempo necesario y comprender los datos necesarios, especialmente en las investigaciones complejas de delitos graves, que pueden tardar varios años en concluirse, se requieren datos de tráfico antiguos.

Con estos argumentos, la Comisión defendió los períodos de conservación establecidos en la Propuesta, advirtiendo que el de un año para datos de tráfico de telefonía móvil y fija y el de seis meses para datos de tráfico relacionados con el uso de internet cubrirían las principales necesidades de los servicios represivos, limitando al mismo tiempo los costes asociados para la industria y la intrusión en la vida privada de los ciudadanos[221].

[221] Advertía la EdM además que "el período de conservación más corto de los datos de tráfico generados por el uso de Internet, en comparación con los datos de tráfico generados por el uso de la telefonía móvil

"Un período de conservación de seis meses para todos los datos —advertía en concreto— hubiera sido demasiado corto, ya que aunque una gran parte de las solicitudes de los servicios represivos se refieren a datos de una antigüedad inferior a seis meses, suelen requerirse datos de antigüedad superior a seis meses en relación con los delitos más graves, como terrorismo, delincuencia organizada u homicidios"[222].

Al dictaminar sobre la Propuesta, el GT29 cuestionó el que los períodos máximos de conservación de datos propuestos fueran convincentes, pues no le parecía demostrado claramente y con pruebas su necesidad. En todo caso, el Grupo opinaba que debía regularse claramente un período de conservación general que fuera lo más breve posible y estar lo más cercano posible al período de conservación para cuyos fines originales los prestadores de servicios de comunicaciones registraron los datos. El período de conservación de datos mencionado en la Directiva debería considerarse como el límite máximo armonizado aplicable a todos los Estados miembros. Asimismo, debía quedar claro que los Estados miembros no tendrían que establecer períodos de conservación de datos más largos que los previstos en la Directiva, aunque tendrán libertad para establecer períodos de conservación más breves.

Por su parte, el SEPD acogió "con satisfacción" que los plazos de retención de la Propuesta fueran perceptiblemente más cortos que los plazos previstos en el proyecto de Decisión marco, si bien estimaba que el principio de proporcionalidad exigía que los plazos de retención, reflejaran sobre todo "las necesidades demostradas por los servicios policiales" [223]. En este sentido, a su entender, mientras que el plazo de un año sí reflejaba las prácticas de los servicios policiales, por haberse indicado mediante las cifras proporcionadas por la Comisión y la Presidencia del Consejo, tales cifras demostraban igualmente que, salvo en casos excepcionales, la retención de datos durante períodos más largos no reflejaba "las prácticas de los servicios policiales". El SEPD se hacía eco así —en el punto 16 de su dictamen— del hecho de que tanto la

---

y fija "estándar" tiene en cuenta las actuales prácticas comerciales reduciendo sustancialmente el volumen de datos que deben conservarse".

[222] Por otra parte, el SEPD consideraba *adecuado* el que en la Propuesta se estableciesen distintos plazos en función del dato a retener. Cf. Dictamen del SEPD…, doc. cit., puntos 61 y 62.

[223] Cf. Dictamen del SEPD…, doc. cit., puntos 61 y 62.

Comisión como la Presidencia del Consejo habían concedido importancia a un estudio de la policía del Reino Unido que mostraba que, aunque el 85% de los datos de tráfico requeridos por la policía tenían un máximo de seis meses de antigüedad, los datos de entre seis meses y un año se utilizaban en investigaciones complejas de delitos más graves, y que se habían presentado igualmente algunos ejemplos de casos concretos[224].

Por otra parte, el Supervisor entendía que un plazo más corto de seis meses para los datos relacionados con las comunicaciones electrónicas efectuadas utilizando única o principalmente el protocolo de internet era "importante desde la perspectiva de la protección de datos, puesto que […] la retención durante más de seis meses no refleja[ba] las prácticas de los servicios policiales"[225]. Finalmente, el dictamen estimaba que debían aclararse en el texto que los plazos de retención de seis meses y de un año eran plazos *máximos* de retención, y que los datos se habían de eliminar al concluir el plazo de retención. El texto exigía asimismo que se precisara cómo habían de borrarse los datos y se estableciera el deber para el proveedor de borrar los datos por medios automatizados "por lo menos a diario"[226].

Como vemos, las observaciones del SEPD en relación con los plazos fueron llanamente ignoradas: los plazos finalmente establecidos por la DCD superan ampliamente lo que el Supervisor había estimado proporcionado y razonable en aquel momento.

Abundando en la misma línea pero con tono más negativo, el dictamen del CESE juzgó que el período de retención de un año, tal como venía planteado en la Propuesta, resultaba demasiado largo, puesto que la Comisión no acreditaba "la necesidad de la retención por esos períodos". El Comité consideraba concretamente que seis meses era un período *prudencial* y *unificado*, siempre que concurrieran las medidas de seguridad y confidencialidad adecuadas[227]. Como sabemos, ninguna de estas consideraciones

---

[224] El Supervisor hacía referencia a la Declaración *Liberty and security, striking the right balance* — Libertad y seguridad: mantener un equilibrio adecuado—, documento de la Presidencia británica de la Unión Europea de 7 de septiembre de 2005. Puede accederse a su texto íntegro en http://www.edri.org/docs/UKpresidencypaper.pdf

[225] Cf. Dictamen del SEPD…, doc. cit., punto 61.

[226] Cf. Dictamen del SEPD…, doc. cit., punto 62.

[227] Cf. Dictamen del CESE…, doc. cit., punto 2.4.8.

prosperaron en el texto vigente, que hace posible conservaciones más allá de los seis meses, plazo este último que queda además establecido como el período mínimo obligatorio para cualquier proveedor[228].

Lo cierto es que la transposición de la Directiva en los Estados miembros ha puesto de manifiesto lo que cabía prever desde un primer momento; unos márgenes tan amplios de conservación, que pueden variar hasta en dieciocho meses, son manifiestamente inidóneos para alcanzar la finalidad de armonización pretendida por la DCD. Desde la entrada en vigor de la Directiva —y una vez transcurrido el plazo para su transposición— todos los Estados miembros aplican períodos de conservación que varían considerablemente entre sí, debido a los amplios límites del art. 6 DCD. Así, quince Estados miembros especifican un plazo único para todas las categorías de datos: un Estado miembro —Polonia— especifica un período de conservación de dos años; otro Estado miembro —Letonia— especifica año y medio; diez —Bulgaria, Dinamarca, Estonia, Grecia, España, Francia, Países Bajos, Portugal, Finlandia y Reino Unido— especifican un año; y tres —Chipre, Luxemburgo y Lituania— especifican seis meses.

Cinco Estados han definido diferentes períodos de conservación para las distintas categorías de datos: dos Estados miembros —Irlanda e Italia— especifican dos años para los datos de telefonía fija y móvil, y un año para los datos de acceso a internet, correo electrónico por internet y telefonía por internet; Eslovenia especifica catorce meses para los datos de telefonía y ocho para los datos de internet; Eslovaquia especifica un año para los datos de telefonía fija y móvil y seis meses para los datos de internet; Malta especifica un año para los datos de telefonía fija, móvil y por internet y seis meses para los datos de acceso a internet y correo electrónico por internet. Hungría conserva todos los datos durante un año, excepto los de llamadas infructuosas, que sólo se conservan seis meses. Bélgica no ha especificado ningún período de conservación de datos para las categorías mencionadas en la Directiva. Difícilmente puede imaginarse mayor disparidad.

[228] Cf. art. 6 DCD.

Para mayor concreción, exponemos a continuación las regulaciones en materia de plazos de conservación tal como se encuentran actualmente en vigor[229]:

— Alemania: no transpuesta;
— Austria: no transpuesta;
— Bélgica: entre un año y treinta y seis meses para los servicios telefónicos "accesibles al público" —no hay disposiciones respecto de los datos de internet—;
— Bulgaria: un año —los datos a los que se ha accedido podrán conservarse un período adicional de seis meses, previa solicitud—;
— Chipre: seis meses;
— Dinamarca: un año;
— Eslovaquia: un año para los datos de telefonía fija y telefonía móvil y seis meses para los datos de acceso a internet, correo electrónico por internet y telefonía por internet;
— Eslovenia: catorce meses para los datos de telefonía y ocho meses para los datos de internet;
— España: un año;
— Estonia: un año;
— Finlandia: un año;
— Francia: un año;
— Grecia: un año;
— Hungría: seis meses para llamadas infructuosas y un año para todos los demás datos;
— Irlanda: dos años para los datos de telefonía fija y telefonía móvil y un año para los datos de acceso a internet, correo electrónico por internet y telefonía por internet;
— Italia: dos años para los datos de telefonía fija y telefonía móvil y un año para los datos de acceso a internet, correo electrónico por internet y telefonía por internet;
— Letonia: dieciocho meses;
— Lituania: seis meses;
— Luxemburgo: seis meses;

[229] Cf. Informe de evaluación sobre la Directiva…, doc. cit., punto 4.5.

— Malta un año para los datos de telefonía fija, móvil y por internet y seis meses para los datos de acceso a internet y correo electrónico por internet;
— Países Bajos: un año;
— Polonia: dos años;
— Portugal: un año;
— República Checa: no transpuesta;
— Rumanía: No transpuesta —seis meses en virtud de la anterior legislación de transposición anulada—.

A la vista de tan dispares resultados —que por otra parte, eran completamente previsibles— no es de extrañar que la Comisión Europea haya expresado su insatisfacción al respecto en su Informe de Evaluación de 2011[230]. Aunque advierte que la Directiva permite este enfoque "diversificado", la institución ha declarado al mismo tiempo su intención de estudiar las opciones para una mayor armonización de los períodos de conservación en la Unión Europea y un más cuidadoso acomodo de los plazos a las necesidades reales y a los tipos de datos de que en cada caso se trate. De este modo, "con vistas a cumplir el principio de proporcionalidad, y a la luz de la información cuantitativa y cualitativa sobre el valor de los datos conservados en los Estados miembros, y de la evolución de las comunicaciones y tecnologías y de la delincuencia y el terrorismo, la Comisión se plantea estudiar la aplicación de diferentes períodos para diferentes categorías de datos, para las distintas categorías de delitos graves o una combinación de ambos"[231].

Por añadidura, tal intención no es sino la reacción necesaria frente a lo que han revelado los datos reales sobre la antigüedad de los datos conservados que han sido cedidos para la investigación de delitos en la práctica policial. El que la inmensa mayoría no superen los seis meses de antigüedad hace evidente la desproporción de los plazos previstos por la DCD, y correlativamente, pone en cuestión su misma legalidad.

Siendo aún más concretos —y utilizando los mismos datos manejados por la Comisión—, sobre la base del desglose estadístico facilitado por nueve Estados

[230] Ibíd.

[231] Ibíd.

miembros[232] para 2008, se observa que, cuando las autoridades judiciales o la policía realizan la solicitud de acceso inicial a los datos, cerca del 90% de los datos cuentan con una antigüedad de seis meses o menos y cerca del 75%, con una de tres meses o menos[233]:

Cuadro 5: Resumen de la antigüedad de los datos conservados a los que se accedió en nueve Estados miembros que proporcionaron el desglose por tipo de datos en 2008				
Antigüedad	*Telefonía fija*	*Telefonía móvil*	*Datos de Internet*	*Total*
3 meses	61 %	70 %	56 %	67 %
3-6 meses	28 %	18 %	19 %	19 %
6-12 meses	8 %	11 %	18 %	12 %
más de 1 año	3 %	1 %	7 %	2 %

Paradójicamente, pese a la evidencia, estas cifras no han hecho variar la opinión de la Comisión sobre la conveniencia de permitir en la Directiva plazos de conservación de hasta dos años. El motivo radica en que, a su entender, aunque según la mayoría de los Estados miembros el uso de los datos conservados con una antigüedad mayor de tres e incluso seis meses resulte menos frecuente, la existencia de tales plazos puede ser "de crucial importancia" cuando se considera que el uso de los datos retenidos tiende a dividirse en tres categorías[234].

En primer lugar, tenemos por una parte los "datos de internet", que a la luz de los estudios manejados por la Comisión suelen solicitarse en el curso de las investigaciones penales después de otras formas de prueba. El análisis de los datos de telefonía móvil y fija genera a menudo posibles pistas que conducen a la solicitud de datos más antiguos, lo cual justificaría la pertinencia de plazos más largos de seis meses. Así, la Comisión ofrece el ejemplo en su Informe de una investigación durante la que se descubre un nombre gracias a los datos de telefonía móvil o de red fija, y en la que los investigadores quieren identificar la dirección del protocolo de internet —IP— que dicha persona ha estado utilizando e identificar con quien ha estado en contacto durante un período de tiempo determinado utilizando esa dirección IP[235]. En tal caso, resultaría

[232] A saber: República Checa, Dinamarca, Estonia, Irlanda, España, Chipre, Letonia, Malta y Reino Unido. Cf. Informe de evaluación sobre la Directiva…, doc. cit., punto 5.2.

[233] Ibíd., de donde se extrae el cuadrante.

[234] Ibíd.

[235] Ibíd.

probable que los investigadores solicitasen datos que les permitan rastrear también las comunicaciones con otras direcciones IP y la identidad de las personas que han utilizado esas direcciones.

En segundo lugar, señala el Informe que las "investigaciones de delitos particularmente graves" —vg. la delincuencia organizada y el terrorismo— tienden a basarse en datos de cierta antigüedad, dado el dilatado tiempo que se necesita para planificar tales delitos. En estos supuestos, la policía necesita recurrir a datos de comunicaciones de muchos meses atrás para establecer la intencionalidad delictiva e identificar pautas de comportamiento criminal y relaciones entre los autores o cómplices. Algo parecido acontecería también con los delitos financieros complejos, que a menudo sólo se detectan una vez transcurridos muchos meses[236].

En tercer lugar —y excepcionalmente—, la Comisión también advierte que, en los "casos en que Estados miembros solicitan datos de tráfico conservados en otro Estado miembro", estos generalmente sólo pueden comunicarse previa autorización judicial en respuesta a una comisión rogatoria cursada por un juez del Estado miembro solicitante. Tal asistencia judicial suele ser un proceso largo que hace que en estos casos, al final, los datos empleados tengan una antigüedad superior a seis meses[237].

Por estas tres razones, la Comisión Europea entiende que de la información obtenida de la ejecución de la DCD no se desprende la necesidad de disminuir los márgenes inicialmente previstos en el texto de la norma, por más que en el nivel de armonización sea considerado insatisfactorio. Lo cierto es que, a pesar de ello —y en meridiana contradicción con sus otras afirmaciones— la institución ha abierto un período de estudio y revisión de los plazos junto con el de los demás aspectos de la vigente regulación[238].

---

[236] Ibíd.

[237] Ibíd.

[238] En concreto, la Comisión ha declarado que "En la evaluación de impacto deberán examinarse los siguientes ámbitos en particular: […] -una mayor armonización y posible reducción de los períodos obligatorios de conservación de datos". Cf. Informe de evaluación sobre la Directiva…, doc. cit., punto 8.5.

9 Medidas futuras

Por su estrecha relación con la cuestión de los plazos de conservación, abordamos seguidamente las previsiones del art. 12 DCD[239] que, compuesto de tres apartados, lleva por rúbrica "medidas futuras".

Por si el plazo máximo para la conservación —hasta dos años— resultara escaso, el art. 12 DCD prevé que todo Estado miembro que deba hacer frente a "circunstancias especiales" que "justifiquen una ampliación limitada del período máximo de conservación" podrá adoptar las medidas "que se impongan" (*sic*). El Estado miembro deberá informar inmediatamente a la Comisión y a los demás países de la Unión sobre las medidas adoptadas y las razones que le han llevado a adoptarlas[240]. Además, dentro de los seis meses posteriores a esta notificación, la Comisión habrá de aprobar o rechazar las medidas en cuestión, tras "haber examinado si constituyen una discriminación arbitraria o una restricción encubierta al comercio entre los Estados miembros o constituyen un obstáculo para el funcionamiento del mercado interior"[241]. Si transcurrido el plazo de los seis meses desde la notificación, la Comisión no ha

[239] Dispone la norma en su tenor literal lo siguiente:

Artículo 12. *Medidas futuras*

1. Todo Estado miembro que deba hacer frente a circunstancias especiales que justifiquen una ampliación limitada del período máximo de conservación recogido en el artículo 6 podrá adoptar las medidas que se impongan. El Estado miembro en cuestión informará inmediatamente a la Comisión y a los demás Estados miembros sobre las medidas adoptadas de conformidad con el presente artículo e indicará las razones que le llevan a adoptarlas.

2. En un plazo de seis meses tras la notificación mencionada en el apartado 1, la Comisión aprobará o rechazará las medidas nacionales en cuestión después de haber examinado si constituyen una discriminación arbitraria o una restricción encubierta al comercio entre los Estados miembros o constituyen un obstáculo para el funcionamiento del mercado interior. En caso de que la Comisión no adopte ninguna decisión en dicho plazo se considerará que las medidas nacionales han sido aprobadas.

3. Cuando, en virtud del apartado 2, las medidas nacionales adoptadas por un Estado miembro se aparten de las disposiciones de la presente Directiva, la Comisión examinará la oportunidad de proponer la modificación de la presente Directiva.

[240] Cf. art. 12.1 DCD.

[241] Ibíd.

adoptado ninguna decisión al respecto, se considerará que las medidas nacionales han sido aprobadas[242]. Finalmente, dispone el tercer apartado que cuando las medidas nacionales adoptadas por el Estado miembro "se aparten de las disposiciones" de la Directiva, la Comisión examinará la oportunidad de proponer la modificación de la Directiva —obsérvese que no de las medidas—[243].

Ha de advertirse primeramente que la Propuesta de Directiva no contenía ninguna previsión análoga a las contenidas en el vigente art. 12 DCD. Su introducción es debida a la enmienda 87 del Parlamento, que propuso la incorporación de un nuevo artículo —el 11 *bis*— que se convirtió en este vigente art. 12. Puesto que la previsión no se incluía en la Propuesta, los órganos dictaminantes no tuvieron ocasión de pronunciarse sobre su contenido, si bien es claro que el precepto choca frontalmente con algunas de las observaciones y recomendaciones que ya se habían formulado en diversos dictámenes. Por ejemplo, el GT29 había advertido que debía quedar claro que los Estados miembros no tendrían que establecer períodos de conservación de datos más largos que los previstos en la DCD, aunque en cambio deberían tener libertad para establecer períodos de conservación más breves[244]; exactamente lo contrario al resultado final[245].

En todo caso, como se echa de ver, mediante la vía del art. 12 DCD se confiere a los Estados la facultad de ampliar el plazo de conservación de los datos previsto en la DCD más allá del máximo de los dos años. Dado que este plazo es uno de los elementos que la DCD armoniza —o pretende armonizar—, se somete la validez de la modificación a la posterior aprobación de la Comisión mediante resolución expresa o silencio positivo.

La interpretación del artículo está abierta a numerosas dudas, empezando por la determinación del momento en que resultan aplicables las medidas aprobadas por el Estado en cuestión. Del tenor literal del precepto no resulta claro si debe ser tras su

---

[242] Cf. art. 12.2 DCD.

[243] Por su parte, en España, la Ley 25/2007, de 18 de octubre, tampoco ha desarrollado esta disposición al transponer la norma comunitaria.

[244] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 8.

[245] A este respecto, resulta un poco extraño que el GT29, en el informe adoptado con posterioridad a la aprobación de la Directiva, no haga ninguna referencia ni alerte sobre este precepto en cuestión. Cf. Report 01/2010 on the second joint…, doc. cit.

adopción por el Estado miembro, o bien cuando la Comisión las apruebe —expresamente o mediante silencio positivo—. Siguiendo a VILASAU, aunque puede parecer que las medidas no son directamente aplicables —pues el art. 12.2 DCD establece que la Comisión "aprobará o rechazará las medidas nacionales" tras examinarlas—, lo cierto es que el sintagma "podrá adoptar las medidas que se impongan" —art. 12.1 DCD— oscurece esta interpretación[246]. En este sentido, parece que las medidas no podrán aplicarse hasta que no conste la aprobación de la Comisión o bien transcurran seis meses sin que ésta se pronuncie. En cualquier caso, se ha de valorar negativamente el que medidas tan onerosas puedan ser aprobadas por silencio positivo.

Otro aspecto problemático del precepto —señalado también por VILASAU[247]— radica en que, mediante el mecanismo previsto en el art. 12 DCD, se produciría una modificación de la DCD sin la intervención del Parlamento Europeo. No puede olvidarse al respecto que, si una de las críticas a la PDCD era que dejaba en manos del sistema de "comitología" la determinación de los datos a conservar, el art. 12 DCD ha venido a incurrir en un error similar. Aunque el defecto se intenta corregir —de alguna forma— mediante el art. 12.3 DCD, al establecer que la Comisión examinará la oportunidad de proponer la modificación de la Directiva cuando las medidas nacionales adoptadas por un Estado miembro se aparten de las disposiciones de la DCD, lo cierto es que, en tanto que tal modificación se produzca, las medidas podrían estar ya aplicándose.

Finalmente, no podemos dejar de advertir que también resulta criticable el concepto de "circunstancias especiales" empleado por el precepto, término demasiado genérico que claramente abre un espacio amplio a la interpretación[248]. Puesto que la conservación de datos de las comunicaciones electrónicas comporta una limitación de los derechos fundamentales de los ciudadanos al respeto de la vida privada y de las comunicaciones y a la protección de los datos de carácter personal, consagrados en los arts. 7 y 8 CDF, la prórroga de ese plazo agudiza tal injerencia. En este sentido, el criterio que legitime

---

[246] Cf. Vilasau Solana, M., La Directiva 2006/24/CE sobre conservación…, op. cit., p.14.

[247] Ibíd.

[248] Ibid.

la ampliación de los plazos no podrá ser otro que el pleno respeto al sistema constitucional del Estado que lleve a cabo la ampliación, como es natural, así como a los derechos fundamentales garantizados en la CDF, dado que las disposiciones de la Carta se aplican a los Estados miembros cuando apliquen el Derecho de la Unión —art. 51.1 CDF—. Así pues, de acuerdo con el art. 52.1 CDF, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades; "sólo se podrán introducir limitaciones —añade el mismo artículo—, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás"[249]. Estos criterios son los que pueden justificar la ampliación unilateral del plazo máximo de dos años permitido por el art. 12 DCD.

Estas consideraciones contrastan con el peculiar criterio empleado por el art. 12.2 DCD, conforme al cual, la Comisión aprobará o rechazará las medidas nacionales examinando si las mismas "constituyen una discriminación arbitraria o una restricción encubierta al comercio entre los Estados miembros o constituyen un obstáculo para el funcionamiento del mercado interior". Puesto que la Comisión no tiene facultades para pronunciarse autorizadamente sobre el respeto a los derechos fundamentales, el art. 12.2 DCD ha recurrido a criterios de funcionamiento del mercado que son absolutamente inadecuados para el caso, puesto que la cuestión principal en juego será en primer lugar el respeto a los derechos fundamentales y, sólo una vez aclarado éste, podrá apreciarse si la reforma o no cumple con el principio de unidad de mercado comunitario.

[249] El respeto a los derechos fundamentales reconocidos por los sistemas constitucionales de los Estados miembros debe reputarse como el estándar más exigente al respecto, dado que, de conformidad con lo previsto por el art. 53 CDF, "ninguna de las disposiciones de la presente Carta podrá interpretarse como limitativa o lesiva de los derechos humanos y libertades fundamentales reconocidos, en su respectivo ámbito de aplicación […] por las constituciones de los Estados miembros".

10 Protección, seguridad y almacenamiento de los datos

Las "condiciones de conservación" de los datos de las comunicaciones electrónicas se cuentan entre las diferencias legales y técnicas de las disposiciones nacionales sobre conservación de datos con fines penales que, de acuerdo con el considerando sexto de la DCD, creaban obstáculos en el mercado único, afectando negativamente a los prestadores de servicios al obligarles a tener que cumplir una gran variedad de legislaciones con requisitos dispares al respecto.

La armonización de las medidas de protección para los datos conservados se lleva a cabo por el art. 7 DCD, bajo la rúbrica de "protección y seguridad de los datos" [250]. De acuerdo con el precepto, "sin perjuicio de lo dispuesto en las disposiciones adoptadas de conformidad con las Directivas 95/46/CE y 2002/58/CE", los Estados miembros deben velar por que los proveedores de servicios de comunicaciones electrónicas cumplan con unos mínimos estándares de seguridad respecto de los datos conservados en cumplimiento de la Directiva. Estos estándares se concretan en cuatro principios, a saber:

---

[250] Transcribimos aquí para su directo examen el tenor literal del art. 7 DCD:

Artículo 7. *Protección y seguridad de los datos.*

1. Sin perjuicio de lo dispuesto en las disposiciones adoptadas de conformidad con las Directivas 95/46/CE y 2002/58/CE, los Estados miembros velarán por que los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones cumplan, en lo que respecta a los datos conservados de conformidad con la presente Directiva, como mínimo los siguientes principios de seguridad de los datos:

a) los datos conservados serán de la misma calidad y estarán sometidos a las mismas normas de seguridad y protección que los datos existentes en la red; b) los datos estarán sujetos a las medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos;

c) los datos estarán sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas, y

d) los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación.

a) los datos conservados deben ser de la misma calidad y estar sometidos a las mismas normas de seguridad y protección que los datos existentes en la red;

b) los datos deben estar sujetos a las medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos;

c) los datos deben estar sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas; y por último,

d) los datos, excepto los que hayan sido accesibles y se hayan conservado, han de destruirse al término del período de conservación[251].

La redacción del precepto es gravemente defectuosa. Para entender el porqué, ha de partirse del sobreentendido de que la modificación que la DCD introduce en la regulación de datos de las comunicaciones electrónicas que lleva a cabo la Directiva 2002/58/CE consiste, eminentemente, en prolongar el tratamiento de una concreta serie de datos generados o tratados por los proveedores que, de otra manera, serían eliminados tan pronto como no fueran necesarios para la transmisión o la facturación, en aplicación de los artículos 5, 6 y 9 DPCE. Así se concluye claramente de la lectura del art. 3.1 DCD, que al establecer formalmente la obligación de conservación, dispone que:

> "Como excepción a los artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas…"

Así pues, entendemos que el legislador sólo pretendía una prolongación en el tiempo del tratamiento de una serie de datos que el proveedor suele tener o utilizar, pero no la creación de un nuevo fichero paralelo con un conjunto mínimo y obligatorio de datos. De hecho, cuando los datos listados por el art. 5 DCD no han sido generados o tratados por dichos proveedores, no es obligatorio conservarlos, tal como aclara el considerando

[251] Cf. art. 7 DCD.

vigésimo tercero. El legislador advierte en el mismo lugar que "la Directiva exige que se conserven exclusivamente los datos generados o tratados en el proceso del suministro de servicios de comunicación". Por su parte, el que los datos retenidos no han de constituir un nuevo fichero puede deducirse del considerando décimotercero, conforme al cual: "los datos deben conservarse de tal manera que se evite que se conserven más de una vez".

Así pues, la intención del legislador europeo se ha limitado meramente a disponer la prolongación en el tiempo del tratamiento de los datos listados por el art. 5 DCD —cuando se generen o traten—, o lo que es lo mismo, a obligar a los proveedores a conservarlos por al menos seis meses. De la lectura de la DCD nada hace deducir que fuera pretensión del legislador modificar ningún otro aspecto del régimen de protección de datos de las comunicaciones electrónicas contenido en la Directiva 2002/58/CE, que había de seguir aplicándose en su totalidad, con la única excepción de que los datos listados por el art. 5 DCD han de someterse a una conservación de al menos seis meses frente a lo previsto como regla general por los artículos 5, 6 y 9 DPCE.

Que éste era el planteamiento inicial del legislador europeo explica el hecho de que la PDCD no contuviera artículo alguno sobre las condiciones de seguridad o protección de los datos. Su Exposición de Motivos entendía que el tratamiento de los datos personales conservados por los proveedores quedaba bien cubierto "por las disposiciones generales y específicas de protección de datos establecidas con arreglo a las Directivas 95/46/CE y 2002/58/CE", con lo que no había necesidad de "disposiciones complementarias específicas sobre principios generales de protección y de seguridad de los datos"[252]. Igualmente, apuntaba la Comisión en el mismo lugar que el tratamiento de tales datos estaría "sometido al control absoluto de las autoridades de protección de datos establecidas en todos los Estados miembros" [253]. De este modo se entiende el que el art. 8 PDCD, bajo la rúbrica de "requisitos de almacenamiento para los datos conservados", en realidad sólo se preocupaba de asegurar la eficaz transmisión de los datos a las autoridades nacionales, determinando que los Estados miembros habían de garantizar que los datos se conservasen de conformidad con la Directiva de manera que los

[252] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 3.

[253] Ibíd.

mismos y cualquier otra información necesaria con ellos relacionada pudieran transmitirse sin demora cuando las autoridades competentes así lo solicitaran. Más allá de eso, el considerando 15 *recordaba* "que la Directiva 95/46/CE6 y la Directiva 2002/58/CE7 son plenamente aplicables a los datos conservados de conformidad con la presente Directiva"[254].

Los órganos dictaminantes de la PDCD no hicieron esta lectura. Por el contrario, dieron por sentado que la norma implicaba la creación de un nuevo fichero paralelo, a cargo de los proveedores, al que irían a parar copias de los datos listados por el art. 5 DCD. Este nuevo fichero requería el establecimiento de un régimen de protección específico que —para su disgusto— la PDCD omitía.

Así por ejemplo, el GT29 sostuvo que la DCD suponía la creación de uno o más ficheros que contuvieran los datos cuya conservación se proveía, por lo que recomendó que los sistemas de almacenamiento de datos a efectos de orden público debían estar separados lógicamente de los sistemas que los proveedores utilizasen a efectos empresariales y debían estar protegidos por medidas de seguridad más rigurosas —por ejemplo, mediante encriptación— para impedir el acceso y el uso no autorizados[255]. En consecuencia, las medidas comunitarias debían prever normas mínimas sobre medidas de seguridad —tanto técnicas como organizativas— a adoptar por los proveedores,

[254] (16) Es esencial que los Estados miembros adopten medidas legislativas para asegurar que los datos conservados de conformidad con esta Directiva solamente se faciliten a las autoridades nacionales competentes de conformidad con la legislación nacional respetando plenamente los derechos fundamentales de las personas concernidas; tales medidas incluyen, en particular, condiciones, límites y salvaguardias apropiados para asegurar la conformidad de los datos conservados con los derechos fundamentales, como garantiza, en particular, el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales; (19) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea. En especial, la presente Directiva, junto con la Directiva 2002/58/CE, intenta asegurar el pleno cumplimiento de los derechos fundamentales del respeto de la vida privada y de las comunicaciones y de la protección de los datos de carácter personal (artículos 7 y 8 de la Carta);

[255] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 10.

"especificando los requisitos generales relativos a las medidas de seguridad establecidas en la Directiva CE/2002/58"[256].

El SEPD, por su parte, también dio por hecho que el efecto de la directiva sería que los proveedores dispondrían de bases de datos distintas de las ya existentes "en las que se encontrará almacenada una cantidad significativa de datos de tráfico y de localización"[257], al tiempo que observaba que "la propuesta no contiene salvaguardias adicionales para la protección de datos", y advertía con alarma que "los considerandos [de la PDCD] hacen simplemente referencia a salvaguardias de la legislación existente y más en concreto a la Directiva 95/46/CE y a la Directiva 2002/58/CE"[258]. El SEPD discrepaba de este planteamiento y recomendaba que se incluyera un apartado en materia de protección de datos, en el que podría insertarse una serie de "recomendaciones" (*sic*) relacionadas con el ejercicio de sus derechos por parte de las personas a las que se refieren los datos, con la calidad y la seguridad de los datos, y con los datos de tráfico y de localización de personas no sospechosas de infracciones penales. Los puntos 62 a 64 y 79 a 84 de su dictamen contienen una profusa relación de estas recomendaciones.

La perspectiva adoptada por el Grupo y el Supervisor, así como sus sugerencias, encontraron eco durante la tramitación parlamentaria de la DCD, concretándose en la inclusión del vigente art. 7 DCD que hemos expuesto.

El tenor literal del art. 7 DCD incluye una serie de principios de protección, seguridad y almacenamiento de los datos, pero con el resultado, debido a la defectuosa redacción del precepto, de que resulta imposible determinar ahora si las disposiciones de las Directivas 95/46/CE y 2002/58/CE son o no aplicables a la medida de conservación de datos. Por un lado, la siempre confusa cláusula "sin perjuicio" que inicia el artículo, parece que ha de interpretarse en el sentido de que "la Directiva 95/46/CE y la Directiva 2002/58/CE son plenamente aplicables a los datos conservados de conformidad con la [DCD]", como dispone taxativamente el considerando

---

[256] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 11.

[257] Cf. Dictamen del SEPD…, doc. cit., p. 29.

[258] Cf. Dictamen del SEPD…, doc. cit., p. 57.

décimoquinto. Por otro lado, el mismo epígrafe indica a continuación que los proveedores habrán de cumplir "como mínimo" los cuatro principios de seguridad de los datos señalados por el artículo. Si las Directivas 95/46/CE y 2002/58/CE son plenamente aplicables a los datos conservados de conformidad con la DCD, ¿qué sentido puede tener el deber de los proveedores de cumplir "como mínimo" esos cuatro principios? El considerando décimosexto de la DCD aumenta la confusión, pues su redacción, tras las enmiendas efectuadas durante su tramitación parlamentaria, especifica que "las obligaciones impuestas a los proveedores de servicios en relación con las medidas para garantizar la calidad de los datos, derivadas del artículo 6 de la Directiva 95/46/CE, y sus obligaciones relativas a la garantía de la confidencialidad y seguridad del tratamiento de datos, derivadas de los artículos 16 y 17 de dicha Directiva, son plenamente aplicables a los datos conservados a efectos de la presente Directiva". No se llega a entender la necesidad de especificar la aplicabilidad de estos artículos de la Directiva 95/46/CE cuando, en el considerando inmediatamente anterior, se ha advertido que tanto ésta como la 2002/58/CE son plenamente aplicables. Tal confusión tiene consecuencias importantes, pues deja abierta la pregunta sobre la legalidad o no de una implementación nacional de la DCD que sólo cumpliera los cuatro principios, pero ignorar los otros principios y demás disposiciones de las directivas implicadas[259].

Una integración sensata de la DCD nos llevaría a concluir que la defectuosa regulación de la norma en este punto se debe al deseo del legislador de salir al paso de las críticas de la SEPD, del GT29 y de las asociaciones de derechos fundamentales en materia de privacidad, parcheando el proyecto inicial con previsiones sobre protección de datos aquí y allá, pero sin cuidarse de que éstas guardaran cierto sentido y coherencia. Así pues, la interpretación más plausible nos llevaría a concluir que las Directivas 95/46/CE y 2002/58/CE son, en efecto, plenamente aplicables en los términos que explicamos al principio.

---

[259] Finalmente, el considerando vigésimo advierte que tanto el Convenio del Consejo de Europa de 2001 sobre la delincuencia cibernética como el Convenio del Consejo de Europa de 1981 sobre la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal abarcan igualmente los datos conservados conforme a la DCD.

Sin embargo, esta interpretación ha sido implícitamente rechazada por la Comisión, ya que, en su Informe de Evaluación de 2011, el órgano dedica uno de los apartados a examinar cómo los Estados miembros han implementado en su legislación interna los cuatro principios de protección de los datos conservados del art. 7 DCD[260], no el conjunto de la normativa de protección de datos.

En este sentido, se comprueba que sólo quince países han transpuesto todos estos principios en la legislación pertinente. Cuatro —Bélgica, Estonia, España y Letonia— han transpuesto dos o tres de estos principios, pero no prevén explícitamente la destrucción de los datos al final del período de conservación. Dos —Italia y Finlandia— prevén la destrucción de datos[261]. En muchos casos, la Comisión no ve claro qué medidas de seguridad técnica y organizativa —como una autenticación de máxima seguridad o una gestión detallada de los registros de acceso[262]— se han aplicado.

La relación que sobre estos principios de protección y seguridad de los datos ha elaborado la Comisión arroja el siguiente resultado (por países):

— Alemania: no transpuesta.
— Austria: no transpuesta.
— Bélgica: los operadores deben garantizar que la transmisión de datos no pueda ser interceptada por un tercero y deberán cumplir las normas del ETSI sobre seguridad de las telecomunicaciones e interceptación lícita. No parece abordarse el principio de destrucción obligatoria de los datos al final del período de conservación[263].

---

[260] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 4.6.

[261] Ibíd.

[262] Ibíd. La autenticación fuerte implica mecanismos de doble autenticación tales como contraseña más datos biométricos o contraseña más testigo de autenticación para garantizar la presencia física de la persona responsable del tratamiento de los datos de tráfico. Por su parte, la gestión detallada de los registros de acceso consiste en el seguimiento detallado del acceso y las operaciones de tratamiento mediante la conservación de registros de la identidad del usuario, la hora de acceso y los ficheros a los que se ha accedido.

[263] Cf. Artículo 6 del Real Decreto de 9 de enero de 2003.

— Bulgaria: la ley de transposición incluye la obligación de aplicar los cuatro principios[264].

— Chipre: la legislación de transposición contempla los cuatro principios[265].

— Dinamarca: se contemplan los cuatro principios[266].

— Eslovaquia: la legislación de transposición contempla los cuatro principios[267].

— Eslovenia: la legislación de transposición contempla los cuatro principios[268].

— España: las disposiciones sobre seguridad de los datos cubren tres de los cuatro principios —calidad y seguridad de los datos conservados, acceso de personas autorizadas y protección contra el tratamiento no autorizado[269]—.

— Estonia: la legislación de transposición prevé tres de los cuatro principios. No existe ninguna disposición explícita para el cuarto principio, aunque toda persona cuyo derecho a la intimidad haya sido violado por actividades de vigilancia podrá solicitar la destrucción de los datos, previa sentencia judicial[270].

— Finlandia: la legislación de transposición sólo prevé expresamente la obligación de destruir los datos al final del período de conservación[271].

— Francia: la ley de transposición incluye la obligación de aplicar los cuatro principios[272].

— Grecia: la ley de transposición incluye la obligación de aplicar los cuatro principios, así como el requisito adicional para que los operadores de elaborar y

---

[264] Cf. Artículo 4, apartado 1, de la Ley sobre comunicaciones electrónicas (modificada) de 2010.

[265] Cf. Artículos 14 y 15 de la Ley 183 (I)/2007.

[266] Cf. Ley sobre tratamiento de datos personales; Decreto nº 714 de 26 de junio de 2008 sobre prestación de servicios y redes de comunicaciones electrónicas.

[267] Cf. Artículo 59a de la Ley de comunicaciones electrónicas; artículo S33 de la Ley nº 428/2002 relativa a la protección de los datos personales.

[268] Cf. Artículo 107a, apartado 6) y 107c de la Ley de comunicaciones electrónicas.

[269] Cf. Artículo 8 de la Ley 25/2007, artículo 38, apartado 3, de la Ley General de Telecomunicaciones. La Ley (artículo 9) se refiere a la excepción al acceso y a los derechos de cancelación establecidos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (artículos 22 y 23).

[270] Cf. Subsección 111 (9) de la Ley de comunicaciones electrónicas; subsección 122 (2) del Código de Enjuiciamiento Criminal.

[271] Cf. Artículo 16, apartado 3, de la Ley de comunicaciones electrónicas.

[272] Cf. Artículo D.98-5, CPCE; Artículo L-34-1 (V), CPCE; artículo 34 de la Ley n° 78-17; artículo 34-1, CPCE; artículo 11 de la Ley nº 78-17 de 6 de enero de 1978.

aplicar un plan para garantizar el cumplimiento, bajo la supervisión de un responsable de la seguridad de los datos[273].

— Hungría: la legislación de transposición contempla los cuatro principios [274].
— Irlanda: en cuanto a las disposiciones sobre protección y seguridad de los datos en el Derecho nacional, la ley de transposición incluye la obligación de aplicar los cuatro principios[275].
— Italia: no hay disposiciones explícitas en materia de seguridad de los datos conservados, aunque existe una obligación general de destrucción o anonimización de los datos de tráfico y de tratamiento consensuado de los datos de localización[276].
— Letonia: la legislación de transposición prevé dos de los principios: la confidencialidad y el acceso autorizado a los datos conservados, y la destrucción de datos al final del período de conservación[277].
— Lituania: la legislación de transposición contempla los cuatro principios[278].
— Luxemburgo: la legislación de transposición contempla los cuatro principios[279].
— Malta: la legislación de transposición contempla los cuatro principios[280].
— Países Bajos: la legislación de transposición contempla los cuatro principios[281].
— Polonia: la legislación de transposición contempla los cuatro principios[282].

---

[273] Cf. Artículo 6 de la Ley 3917/2011.

[274] Cf. Artículo 157 de la Ley C/2003, modificada por la Ley CLXXIV/2007, artículo 2 del Decreto 226/2003 y Ley LXIII/1992 sobre Protección de Datos.

[275] Cf. Artículos 4, 11 y 12 de la Ley de Comunicaciones (Conservación de Datos) de 2009.

[276] Cf. Artículos 123 y 126 del Código de Protección de Datos.

[277] Cf. Artículo 4, apartado 4, y artículo 71, apartados 6 a 8, de la Ley de comunicaciones electrónicas.

[278] Cf. Artículo 12, apartado 5, y artículo 66, apartados 8 y 9, de la Ley de comunicaciones electrónicas, modificada el 14 de noviembre de 2009.

[279] Cf. Artículo 1, apartado 5, de la Ley de 24 de julio de 2010.

[280] Cf. Artículos 24 y 25 del Anuncio Oficial 198/2008; artículo 40, letra b), de la Ley sobre protección de datos (cap. 440).

[281] Cf. Artículo 13, apartado 5, de la Ley de telecomunicaciones; el largo título del Protocolo de cooperación es: *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens.*

[282] Cf. Artículos 180a y 180e de la Ley de telecomunicaciones.

— Portugal: en cuanto a las disposiciones sobre protección y seguridad de los datos en el Derecho nacional, la legislación de transposición contempla los cuatro principios[283].
— Reino Unido: la legislación de transposición contempla los cuatro principios[284].
— República Checa: la legislación de transposición contempla los cuatro principios [285].
— Rumanía: no transpuesta.
— Suecia: no transpuesta.

A la vista de esta relación, no cabe extrañarse que, como resultado de su análisis, la Comisión haya concluido que la transposición del art. 7 DCD es "incoherente"[286]. Aunque realmente la mejora de las garantías de seguridad de los datos conservados no presentaría grandes dificultades técnico-legislativas, la Comisión ha manifestado expresamente su intención de "estudiar opciones" para reforzar la seguridad de los datos y los niveles de protección de datos, "incluida la introducción de soluciones de protección de la intimidad desde el diseño para garantizar el cumplimiento de tales normas, tanto a nivel del almacenamiento como de la transmisión" [287]. A mayor abundamiento, resulta esperanzador para una mejor protección de los derechos de los ciudadanos el que la institución se haya comprometido explícitamente a tener en cuenta las recomendaciones al respecto efectuadas en el *Informe relativo a la segunda acción común de control y ejecución* elaborado por el GT29, en el concreto sentido de "adoptar normas mínimas y medidas de salvaguardia y de seguridad técnica y organizativa"[288].

---

[283] Cf. Artículo 7, apartados 1 y 5, y artículo 11 de la Ley 32/2008; artículos 53 y 54 de la Ley de Protección de Datos Personales.

[284] Cf. Artículo 6 del Reglamento de conservación de datos.

[285] Cf. Artículos 87, apartado 3, y 88 de la Ley 127/2005 modificada por la Ley 247/2008; artículo 2 de la Ley 336/2005; articulo 3, apartado 4, de la Ley 485/2005; artículo 28, apartado 1, de la Ley 101/2000.

[286] Cf. Informe de evaluación sobre la Directiva…, doc. cit., punto 4.6.

[287] Ibíd.

[288] Ibíd.

11 Autoridades de control

Bajo la rúbrica de "autoridades de control" y compuesto de dos apartados, el art. 9 DCD prevé que cada Estado miembro nombre *una o más* autoridades públicas responsables de velar por la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros de conformidad con el ya examinado art. 7 DCD en relación con la seguridad de los datos conservados[289]. "Dichas autoridades —advierte el art. 9.1 *in fine*— podrán ser las mencionadas en el artículo 28 de la Directiva 95/46/CE"[290],

---

[289] El tenor literal del artículo en vigor establece lo siguiente:

Artículo 9. *Autoridades de control.*

1. Cada Estado miembro nombrará una o más autoridades públicas responsables de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros de conformidad con el artículo 7 en relación con la seguridad de los datos conservados. Dichas autoridades podrán ser las mencionadas en el artículo 28 de la Directiva 95/46/CE.

2. Las autoridades mencionadas en el apartado 1 actuarán con plena independencia en el ejercicio del control a que se refiere el apartado 1.

[290] Conforme a este artículo 28 —*Autoridad de control*—:

"1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

3. La autoridad de control dispondrá, en particular, de:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;

- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;

- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

esto es, las agencias de protección de datos existentes en todos los Estados de la Unión Europea en virtud del mismo cuerpo legal. Además, el apartado segundo especifica que las autoridades mencionadas en el apartado primero deberán actuar *con plena independencia* en el ejercicio de estos controles[291].

Este artículo no encuentra precedente en la PDCD. Como hemos visto, durante la elaboración de la misma, se entendió por la Comisión que el tratamiento de los datos personales conservados por los proveedores quedaba bien cubierto por las disposiciones generales y específicas de protección de datos establecidas con arreglo a las Directivas 95/46/CE y 2002/58/CE y que no había necesidad de disposiciones complementarias específicas sobre principios generales de protección y de seguridad de los datos, por lo que, en lógica consecuencia, el tratamiento de tales datos estaría "sometido al control absoluto de las autoridades de protección de datos establecidas en todos los Estados

---

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.
Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.
5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.
6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.
Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.
7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso".

[291] Sobre la figura de estas autoridades, destaca la monografía de Burkert, H., Organization and method of operation of the data protection authorities, Gesellschaft für Mathematik und Datenverarbeitung, Institut de recherche d'informatique et d'automatique, National Computing Centre Limited, Commission of the European Communities, 1990.

miembros" [292]. Es decir, se sobrentendía que, en la medida en que la DCD simplemente modificaba las condiciones del tratamiento de ciertos datos de las comunicaciones electrónicas, las autoridades nacionales de protección de datos velarían por la aplicación de la DCD como una parte más de la normativa.

La introducción del art. 7 DCD y el establecimiento de los cuatro principios de seguridad que "como mínimo" deben cumplir los proveedores deja abierta —como hemos expuesto— la cuestión de si las Directivas 95/46/CE y 2002/58/CE son o no "plenamente aplicables" respecto al régimen de conservación de los datos establecido por la DCD. La tesis negativa encuentra en este art. 9 DCD un argumento a su favor, ya que, tal como se encuentra redactado, no refleja exactamente la idea plasmada en la Exposición de Motivos de la PDCD. Las autoridades públicas responsables de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros pueden ser "una o más"; su competencia se extiende a un ámbito concreto: "las disposiciones adoptadas por los Estados miembros de conformidad con el artículo 7 en relación con la seguridad de los datos conservados" —esto es, sólo los cuatros principios de seguridad de los datos [293] — y, finalmente, pueden ser —pero no necesariamente— las agencias de protección de datos existentes en cada Estado en aplicación del art. 28 de la Directiva 95/46/CE. El art. 9.2 DCD especifica complementariamente que estas autoridades deberán actuar "con plena independencia en el ejercicio" de estos controles, una nota que se predica de las agencias nacionales que, conforme al art. 28.1 de la Directiva 95/46/CE.

La creación de una autoridad independiente que vele por la aplicación de los cuatro principios mínimos del art. 7 DCD, junto con otra autoridad que velaría por la aplicación de las Directivas 95/46/CE y 2002/58/CE, se antoja ciertamente problemática. Los cuatro principios no son más que especificaciones de las Directivas, que a su vez parecen seguir resultando de aplicación a la DCD —"sin perjuicio de, etc." —. La delimitación de las competencias entre la autoridad nacional de protección de datos —fiscalizadora de la normativa general— y la autoridad especializada —

[292] Ibíd.

[293] Cf. art. 8 DCD.

fiscalizadora de los cuatro principios— da lugar a un solapamiento de sus competencias, dado que compartirían el mismo ámbito material.

Probablemente, la solución más sensata es la alcanzada por países como España. Como tendremos ocasión de analizar pormenorizadamente más adelante, en el caso español la autoridad de control a la que se refiere el art. 9 DCD, es, por indicación directa del art. 8.4 LCD, la Agencia Española de Protección de Datos, como "autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados" en dicha Ley[294], al tiempo que en su art. 8. LCD remite a la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo para la determinación del nivel de protección de los datos almacenados.

Soluciones parecidas han sido arbitradas en la inmensa mayoría de los Estados miembros, que han optado hasta la fecha por encomendar esta tarea a su autoridad de protección de datos, a saber[295]:

— Alemania: no transpuesta.
— Austria: no transpuesta.
— Bélgica: Instituto de Servicios Postales y Telecomunicaciones.
— Bulgaria: la Comisión de Protección de los Datos Personales controla el tratamiento y almacenamiento de los datos para garantizar el cumplimiento de las obligaciones; la Comisión parlamentaria de la Asamblea Nacional controla los procedimientos de autorización y acceso a los datos.
— Chipre: el Comisario para la Protección de los Datos Personales controla la aplicación de la legislación de transposición[296].
— Dinamarca: la Agencia Nacional de Tecnología de la Información y Telecomunicaciones supervisa si los proveedores de redes y servicios de comunicaciones electrónicas aseguran que los sistemas y equipos técnicos

[294] Cf. art. 8.4 LCD.

[295] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 18 y ss.

[296] Cf. Artículos 14 y 15 de la Ley 183 (I)/2007.

permiten el acceso de la Policía a la información sobre tráfico de telecomunicaciones[297].

— Eslovaquia: la autoridad de regulación de precios en el ámbito de las comunicaciones electrónicas supervisa la protección de los datos personales[298].

— Eslovenia: Comisario de Información[299].

— España: la autoridad responsable es la Agencia Española de Protección de Datos[300].

— Estonia: la Autoridad de Vigilancia Técnica es la autoridad responsable[301].

— Finlandia: la Autoridad finlandesa reguladora de las comunicaciones supervisa el cumplimiento por parte de los operadores de la normativa sobre conservación de datos. El Defensor de la Protección de Datos supervisa la legalidad general del tratamiento de los datos personales[302].

— Francia: la Comisión Nacional de la Tecnología de la Información y de las Libertades supervisa el cumplimiento de las obligaciones[303].

— Grecia: Autoridad responsable de la protección de los datos personales y de la privacidad de las comunicaciones[304].

— Hungría: Comisario Parlamentario para la Protección de Datos y la Libertad de Información[305].

---

[297] Cf. Ley sobre tratamiento de datos personales; Decreto nº 714 de 26 de junio de 2008 sobre prestación de servicios y redes de comunicaciones electrónicas.

[298] Cf. Artículo 59a de la Ley de comunicaciones electrónicas; artículo S33 de la Ley nº 428/2002 relativa a la protección de los datos personales.

[299] Cf. Artículo 107a, apartado 6) y 107c de la Ley de comunicaciones electrónicas.

[300] Cf. Artículo 8 de la Ley 25/2007, artículo 38, apartado 3, de la Ley General de Telecomunicaciones. La Ley (artículo 9) se refiere a la excepción al acceso y a los derechos de cancelación establecidos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (artículos 22 y 23).

[301] Cf. Subsección 111 (9) de la Ley de comunicaciones electrónicas; subsección 122 (2) del Código de Enjuiciamiento Criminal.

[302] Cf. Artículo 16, apartado 3, de la Ley de comunicaciones electrónicas.

[303] Cf. Artículo D.98-5, CPCE; Artículo L-34-1 (V), CPCE; artículo 34 de la Ley n° 78-17; artículo 34-1, CPCE; artículo 11 de la Ley nº 78-17 de 6 de enero de 1978.

[304] Cf. Artículo 6 de la Ley 3917/2011.

[305] Cf. Artículo 157 de la Ley C/2003, modificada por la Ley CLXXIV/2007; artículo 2 del Decreto 226/2003 y Ley LXIII/1992 sobre Protección de Datos.

— Irlanda: el juez designado tiene la facultad de investigar e informar acerca de si las autoridades nacionales competentes cumplen las disposiciones de transposición de la legislación[306].

— Italia: la Autoridad de protección de datos supervisa el cumplimiento de la Directiva[307].

— Letonia: la Inspección Nacional para la Protección de Datos supervisa la protección de los datos personales en el sector de las comunicaciones electrónicas, pero no el acceso y el tratamiento de los datos conservados[308].

— Lituania: la Inspección Nacional para la Protección de Datos supervisa la aplicación de la Ley de transposición y es responsable de proporcionar estadísticas a la Comisión Europea[309].

— Luxemburgo: Autoridad de protección de datos[310].

— Malta: Comisario de Protección de Datos[311].

— Países Bajos: la Agencia de comunicaciones por radio supervisa las obligaciones de los proveedores de acceso a internet y telecomunicaciones; la Autoridad de Protección de Datos supervisa el tratamiento general de los datos personales; un protocolo detalla la cooperación entre las dos autoridades[312].

— Polonia: Autoridad de protección de datos[313].

— Portugal: Autoridad portuguesa de protección de datos[314].

---

[306] Cf. Artículos 4, 11 y 12 de la Ley de Comunicaciones (Conservación de Datos) de 2009.

[307] Cf. Artículos 123 y 126 del Código de Protección de Datos.

[308] Cf. Artículo 4, apartado 4, y artículo 71, apartados 6 a 8, de la Ley de comunicaciones electrónicas.

[309] Cf. Artículo 12, apartado 5, y artículo 66, apartados 8 y 9, de la Ley de comunicaciones electrónicas, modificada el 14 de noviembre de 2009.

[310] Cf. Artículo 1, apartado 5, de la Ley de 24 de julio de 2010.

[311] Cf. Artículos 24 y 25 del Anuncio Oficial 198/2008; artículo 40, letra b), de la Ley sobre protección de datos (cap. 440).

[312] Cf. Artículo 13, apartado 5, de la Ley de telecomunicaciones; el largo título del Protocolo de cooperación es: *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens.*

[313] Cf. Artículos 180a y 180e de la Ley de telecomunicaciones.

[314] Cf. Artículo 7, apartados 1 y 5, y artículo 11 de la Ley 32/2008; artículos 53 y 54 de la Ley de Protección de Datos Personales.

— Reino Unido: el Comisario de Información supervisa la conservación y el tratamiento de los datos de comunicaciones (y cualesquiera otros datos personales), asegurando un control adecuado en materia de protección de datos. El Comisario para la Interceptación de las Comunicaciones (un magistrado superior en activo o ya jubilado) supervisa la recogida de datos de comunicaciones por parte de las autoridades públicas al amparo de la Ley RIPA. Un tribunal con competencias de investigación investiga las denuncias por el uso indebido de los datos adquiridos al amparo de la legislación de transposición (Ley RIPA) [315].
— República Checa: Autoridad de protección de datos[316].
— Rumanía: no transpuesta.
— Suecia: no transpuesta.

12 Acceso a los datos

La DCD no define qué autoridades nacionales tendrán acceso a los datos. Su art. 4 DCD, bajo la rúbrica de "acceso a los datos", se limita a disponer que los Estados miembros deben adoptar medidas para garantizar que los datos conservados de conformidad con la Directiva solamente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional[317].

[315] Cf. Artículo 6 del Reglamento de conservación de datos.

[316] Cf. Artículos 87, apartado 3, y 88 de la Ley 127/2005 modificada por la Ley 247/2008; artículo 2 de la Ley 336/2005; articulo 3, apartado 4, de la Ley 485/2005; artículo 28, apartado 1, de la Ley 101/2000.

[317] Reproducimos seguidamente el precepto, que se expresa en los siguientes términos: Artículo 4. *Acceso a los datos.* Los Estados miembros adoptarán medidas para garantizar que los datos conservados de conformidad con la presente Directiva solamente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional.

Indica el precepto en su segundo párrafo que cada Estado miembro debe definir en su Derecho interno el procedimiento que ha de seguirse y las condiciones a cumplir para tener acceso a los datos conservados de conformidad los requisitos de necesidad y proporcionalidad, que a su vez deben de valorarse específicamente de conformidad con las disposiciones de el Derecho de la Unión o del Derecho internacional público, y en particular, el Convenio Europeo de Derechos Humanos en la interpretación del Tribunal Europeo de Derechos Humanos[318].

El precepto, como vemos, simple y formalmente remite la determinación sobre las condiciones de acceso a la legislación de los Estados miembros, limitándose a señalar la necesidad de respetar el Derecho en vigor y, particularmente, las condiciones para limitar legítimamente los derechos fundamentales implicados.

Esta remisión no podía ser de otra manera, ya que, como explicamos en el primer apartado de esta Primera Parte, cuestiones como la determinación de las autoridades que podían acceder a los datos conservados, de los delitos cuya persecución justificaba el acceso o de las condiciones de intercambio de información entre autoridades sólo podían regularse mediante un instrumento basado en el TUE, es decir, en el Tercer Pilar

---

Cada Estado miembro definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del Derecho de la Unión o del Derecho internacional público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos.

[318] El considerando decimoséptimo de la DCD hace un resumen de este artículo, advirtiendo que "es esencial que los Estados miembros adopten medidas legislativas para asegurar que los datos conservados de conformidad con la presente Directiva solamente se faciliten a las autoridades nacionales competentes de conformidad con la legislación nacional, respetando plenamente los derechos fundamentales de las personas afectadas".

El art. 3.2 de la Propuesta de la DCD establecía, en términos bastante parecidos al vigente art. 4 DCD, la necesidad de adoptar medidas para garantizar que los datos conservados de acuerdo con la Directiva solamente se proporcionasen a las autoridades nacionales competentes en casos específicos y de conformidad con la legislación nacional, con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como el terrorismo y la delincuencia organizada. Este final del artículo—"con fines de prevención [....] terrorismo y la delincuencia organizada"— se ha suprimido en el art. 4.1 DCD, lo que hay que poner en relación con el hecho de que en el propio art. 1 DCD se hace referencia a "delitos graves", sin especificar cuáles son.

—como vg. una decisión marco—, pues suponía establecer normas acerca de la actividad y competencias de las autoridades represivas de los Estados miembros, que era un materia de cooperación policial y judicial comprendida en este Pilar. La determinación de qué autoridades nacionales podían acceder a los mismos y bajo qué circunstancias comportaba armonizar las legislaciones penales y procesales de los Estados miembros, que era una competencia que caía fuera del ámbito del art. 95 TCE y, por tanto, del Derecho comunitario. No podía regularse en ningún caso a través de directivas o reglamentos, instrumentos propios del Primer Pilar[319].

Este reparto competencial se reconoce y explica en los considerandos de la DCD. Así, el considerando vigésimo quinto de la DCD establece que la norma se entiende sin perjuicio de la facultad de los Estados miembros para adoptar medidas legislativas "relativas al derecho de acceso de los datos por parte de las autoridades nacionales tal como determinen los mismos". Explica el considerando a renglón seguido que "las cuestiones relativas al acceso por parte de las autoridades nacionales a datos conservados con arreglo a la presente Directiva para las actividades contempladas en el artículo 3, apartado 2, primer guión, de la Directiva 95/46/CE[320], quedan fuera del ámbito de aplicación del Derecho comunitario. Sin embargo, pueden estar sometidas a la legislación nacional o a una acción como las previstas por las disposiciones del título VI del Tratado de la Unión Europea", esto es, una ley nacional o una decisión-marco. El considerando concluye en la misma línea que el art. 4 DCD, recordando las condiciones que tales regulaciones deberán observar:

> "Dichas leyes o acciones deben respetar plenamente los derechos fundamentales que se derivan de tradiciones constitucionales comunes de los Estados miembros y están garantizados por el CEDH.

---

[319] La cooperación policial y judicial en materia penal no se encontraba entre los fines y competencias de la Comunidad Europea, tal como eran descritos en el TCE —arts. 2 y 3.1.h) TCE—, por lo que tales materias no podían en consecuencia ser objeto de regulación comunitaria.

[320] "2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales: - efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal".

> Con arreglo al artículo 8 del CEDH, según la interpretación del Tribunal Europeo de Derechos Humanos, la injerencia de las autoridades públicas en el derecho a la vida privada debe respetar los requisitos de necesidad y proporcionalidad y debe, por consiguiente, servir a propósitos específicos, explícitos y timos y ejercerse de una manera adecuada, pertinente y no excesiva en relación con el objeto de la injerencia".

La misma idea se contiene, más resumidamente, en el considerando décimoseptimo, que considera que "es esencial" que los Estados miembros adopten medidas legislativas para asegurar que los datos conservados de conformidad con la DCD "solamente se faciliten a las autoridades nacionales competentes de conformidad con la legislación nacional, respetando plenamente los derechos fundamentales de las personas afectadas".

Aclarado así que la directiva no podía determinar qué autoridades nacionales podrían acceder a los datos conservados en su virtud, debe censurarse el que los órganos europeos dictaminantes quisieran ignorar las limitaciones de este reparto de competencias. Así, el SEPD no estaba de acuerdo con que la exclusión de disposiciones precisas sobre el acceso y la posterior utilización de los datos de tráfico y de localización fuera una consecuencia inevitable de la base jurídica de la propuesta —art. 95 TCE—. A su entender, si el legislador comunitario no podía establecer normas sobre el acceso y el uso de datos, no podría cumplir su obligación de conformidad con el art. 6 TUE, dado que dichas normas son imprescindibles para asegurarse de que los datos se retengan con el respeto debido a los derechos fundamentales: "en otras palabras —añadía—, […] las normas sobre el acceso, el uso y el intercambio de datos son inseparables de la propia obligación de conservar los datos"[321]. De este modo, el Supervisor defendía que, en lo que se refiere a la determinación de las autoridades —aun admitiendo que esta competencia incumbe a los Estados miembros—, "un acto comunitario puede imponer condiciones a los Estados miembros en lo que se refiere a la designación de las autoridades competentes, el control judicial o el acceso de los ciudadanos a la justicia. Estas disposiciones garantizan la existencia de mecanismos

[321] Cf. Dictamen del SEPD…, doc. cit., p. 40.

convenientes a nivel nacional para garantizar la plena eficacia del acto, incluido el cumplimiento completo de la legislación en materia de protección de datos"[322].

Con apoyo en este argumento, el SEPD recomendaba en concreto la adición a la propuesta de uno o más artículos sobre el acceso a los datos de tráfico y de localización por parte de las autoridades competentes y sobre la utilización posterior de los datos —para asegurarse de que los individuos distintos de estas autoridades no tengan acceso a los datos—, así como de una disposición en el sentido de que el acceso en casos específicos debía estar supeditado siempre a control judicial en cada Estado miembro[323].

Mucho menos ambicioso en sus planteamientos, el CESE opinaba por su parte que la remisión a las "autoridades nacionales competentes" resultaba excesivamente genérica, y que debía hacerse constar expresamente que solamente se podrían proporcionar los datos almacenados a unas "autoridades" que garantizasen la calidad, la confidencialidad y la seguridad de los datos obtenidos[324]. Además, el acceso a los datos no debía ser posible salvo autorización judicial[325], opinión compartida por el GT29, que admitía la excepción de los países donde existiera la posibilidad específica de acceso autorizado por ley, bajo supervisión independiente[326]. Además, el Grupo sugirió que la Directiva debía establecer que los datos sólo estarían disponibles para determinadas autoridades policiales específicamente designadas cuando fuera necesario a efectos de la investigación, detección, procesamiento o prevención del terrorismo, y que debía publicarse la lista de tales autoridades[327].

En todo caso, como era de prever, las inevitables omisiones del art. 4 DCD sobre las condiciones de acceso han hecho que cada Estado miembro haya regulado la materia según su conveniencia, sin que pueda apreciarse una armonización en este punto. Así, a la vista de la información recabada por la Comisión, parece que en todos los Estados

---

[322] Cf. Dictamen del SEPD…, doc. cit., 41.

[323] Cf. Dictamen del SEPD…, doc. cit., 81.

[324] Cf. Dictamen del CESE…, doc. cit., punto 2.4.10.

[325] Cf. Dictamen del CESE…, doc. cit., punto 2.4.7.

[326] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 6.

[327] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 2.

miembros —salvo en las jurisdicciones de *common law*, como Irlanda y Reino Unido—, pueden acceder a los datos conservados la Policía y el Ministerio Público. Catorce Estados miembros incluyen los servicios de seguridad, de inteligencia o militares entre las autoridades competentes. Seis Estados miembros incluyen las autoridades fiscales, y tres, las autoridades fronterizas. Un Estado miembro permite a otras autoridades públicas a acceder a los datos cuando estén autorizadas para fines específicos en virtud de la legislación secundaria. Once Estados miembros exigen una autorización judicial para cada solicitud de acceso a los datos conservados. En tres Estados miembros se requiere autorización judicial en la mayoría de los casos. Otros cuatro exigen la autorización de una autoridad de alto nivel, pero no de un juez. En dos, la única condición es que la solicitud se presente por escrito[328].

Individualizado por países, el régimen de acceso a los datos conservados se encuentra actualmente regulado de la siguiente manera[329]:

— Alemania: no transpuesta.
— Austria: no transpuesta.
— Bélgica: las autoridades nacionales competentes son la unidad de coordinación judicial, los jueces de instrucción, el fiscal y la Policía criminal. En cuanto a los procedimientos y condiciones, el acceso debe ser autorizado por un juez o un fiscal. Previa petición, los operadores deben proporcionar en "tiempo real" los datos del abonado y los de tráfico y localización de las llamadas realizadas durante el último mes. Los datos correspondientes a llamadas más antiguas deben proporcionarse lo antes posible.
— Bulgaria: las autoridades nacionales competentes son las direcciones y departamentos específicos de la Agencia Estatal de Seguridad Nacional, el Ministerio del Interior, el Servicio de Información Militar, la Policía Militar, el Ministerio de Defensa, la Agencia Nacional de Investigación, las autoridades judiciales y alas utoridades responsables de las actuaciones prejudiciales —estos

[328] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 10.

[329] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 11.

últimos con ciertas condiciones—. En cuanto a los procedimientos y requisitos, el acceso es posible únicamente por orden del presidente de un tribunal regional[330].

— Chipre: las autoridades nacionales competentes son los Tribunales, el Ministerio Fiscal y la Policía. En cuanto a los procedimientos y condiciones, el acceso debe ser aprobado por un fiscal si considera que puede aportar pruebas de la comisión de un delito grave. Un juez puede emitir una orden de este tipo si hay sospechas razonables de un delito grave y si es probable que los datos estén relacionados con el mismo[331].

— Dinamarca: la autoridad nacional competente es la Policía. En cuanto a los procedimientos y condiciones, el acceso exige una autorización judicial; el tribunal podrá autorizarlo si la solicitud cumple criterios estrictos en materia de sospecha, necesidad y proporcionalidad[332].

— Eslovaquia: las autoridades nacionales competentes son los servicios con funciones coercitivas y los tribunales. En cuanto a los procedimientos y condiciones, las solicitudes deben presentarse por escrito[333].

— Eslovenia: las autoridades nacionales competentes son la Policía, las agencias de inteligencia y seguridad, los organismos de defensa responsables de la inteligencia, contrainteligencia y misiones de seguridad. En cuanto a los procedimientos y condiciones, el acceso exige una autorización judicial[334].

— España: las autoridades nacionales competentes son las Fuerzas de Policía responsables de la detección, investigación y enjuiciamiento de los delitos graves, el Centro Nacional de Inteligencia y el Departamento de Aduanas. En cuanto a los

---

[330] Cf. Artículo 250b, apartado 1, de la Ley de comunicaciones electrónicas (modificada) de 2010 (autoridades); artículo 250b, apartado 1, y artículo 250c, apartado 1, de la Ley de comunicaciones electrónicas (modificada) de 2010 (acceso).

[331] Cf. Artículo 4, apartado 2, y artículo 4, apartado 4, de la Ley 183 (I)/2007.

[332] Cf. Capítulo 71 de la Ley de administración de justicia.

[333] Cf. Artículo 59a, apartado 8, de la Ley de comunicaciones electrónicas

[334] Cf. Artículo 107c de la Ley de comunicaciones electrónicas; artículo 149b del Código de enjuiciamiento criminal; artículo 24, letra b), de la Ley relativa a los servicios de seguridad; y artículo 32 de la Ley de defensa.

procedimientos y condiciones, el acceso a estos datos por las autoridades nacionales competentes exige una autorización judicial previa[335].

— Estonia: las autoridades nacionales competentes son la Policía y la Policía de Fronteras, la Dirección de la Policía de Seguridad y —para los objetos y las comunicaciones electrónicas— la Dirección de Impuestos y Aduanas. En cuanto a los procedimientos y condiciones, el acceso requiere la autorización de un juez de instrucción. Los operadores deben presentar los datos conservados en casos urgentes, a más tardar en diez horas, y en otros casos, en el plazo de diez días laborables a partir de la fecha de recepción de la solicitud[336].

— Finlandia: Para los datos conservados relativos a abonados, tráfico y localización, las autoridades nacionales competentes son la Policía, la guardia fronteriza y las autoridades aduaneras. Para datos de identificación y localización en situaciones de emergencia, lo son el Centro de Emergencias, los servicios de salvamento marítimo y el subcentro de salvamento marítimo. En cuanto a los procedimientos y condiciones, pueden acceder a los datos del abonado todas las autoridades competentes sin autorización judicial. Otros datos exigen una orden judicial[337].

— Francia: las autoridades nacionales competentes son la Fiscalía y los agentes de Policía y gendarmes autorizados. En cuanto a los procedimientos y condiciones, la Policía debe aportar una justificación para cada solicitud de acceso a los datos conservados y obtener la autorización de la persona designada en el Ministerio del Interior por la Comisión nacional de control de las interceptaciones de seguridad. Las solicitudes de acceso son tramitadas por un funcionario designado que trabaja para el operador[338].

— Grecia: las autoridades nacionales competentes son las autoridades judiciales, militares y policiales. En cuanto a los procedimientos y condiciones, el acceso

---

[335] Cf. Artículos 6 y 7 de la Ley 25/2007.

[336] Cf. Subsección 112 (2) y (3) del Código de enjuiciamiento criminal (autoridades y procedimiento); Subsección 111 (9) (Condiciones) de la Ley de comunicaciones electrónicas.

[337] Cf. Artículo 35, apartado 1, y artículo 36 de la Ley de comunicaciones electrónicas; artículos 31-33 de la Ley sobre la policía; artículo 41 de la Ley de la guardia fronteriza.

[338] Cf. Artículos 60-1 y 60-2 del Código de enjuiciamiento criminal (autoridades); Artículo L.31-1-1 (condiciones).

requiere una decisión judicial que declare que la investigación por otros medios es imposible o extremadamente difícil[339].

— Hungría: las autoridades nacionales competentes son la Policía, la Administración fiscal y aduanera, los servicios de seguridad nacional, el Ministerio Fiscal y los tribunales. En cuanto a los procedimientos y condiciones, la Policía y la Administración fiscal y aduanera requieren la autorización de la Fiscalía. El fiscal y las agencias de seguridad nacional pueden acceder a tales datos sin una orden judicial[340].

— Irlanda: las autoridades nacionales competentes son los miembros de la *Garda Síochána* —Policía— con categoría de *Chief Superintendant* o superior; los agentes de las Fuerzas de Defensa Permanentes de categoría equivalente o superior a coronel y los funcionarios de la Administración Fiscal de categoría equivalente o superior a responsable principal. En cuanto a los procedimientos y condiciones, las solicitudes deben presentarse por escrito[341].

— Italia: las autoridades nacionales competentes son la Fiscalía, la Policía y el abogado defensor del demandado o de la persona investigada. En cuanto a los procedimientos y condiciones, el acceso exige un "auto motivado" dictado por la Fiscalía[342].

— Letonia: las autoridades nacionales competentes son los funcionarios autorizados de las instituciones encargadas de la investigación prejudicial, las personas que realizan funciones de investigación, los funcionarios autorizados de los organismos de seguridad nacional, la Fiscalía y los tribunales. En cuanto a los procedimientos y condiciones, los funcionarios autorizados, la fiscalía y los tribunales deben evaluar la "adecuación y pertinencia" de una solicitud, registrarla y garantizar la protección de los datos obtenidos. Los organismos autorizados pueden firmar un

---

[339] Cf. Artículos 3 y 4 de la Ley 2225/94.

[340] Cf. Artículo 68, apartado 1, y artículo 69, apartado 1, letras c) y d), de la Ley XXXIV de 1994; artículos 9/A, apartado 1, de la Ley V de 1972; artículo 71, apartados 1, 3 y 4, artículo 178/A, apartado 4, y artículos 200, 201, 268, apartado 2, de la Ley XIX de 1998; artículo 40, apartados 1 y 2, artículo 53, apartado 1, y artículo 54, apartado 1, letra j), de la Ley CXXV de 1995.

[341] Cf. Artículo 6 de la Ley de comunicaciones (conservación de datos) de 2009.

[342] Cf. Artículo 132, apartado 3, del Código de protección de datos.

acuerdo con el operador, por ejemplo, para la codificación de los datos facilitados[343].

— Lituania: las autoridades nacionales competentes son los organismos responsables de la investigación prejudicial, los fiscales, los jueces y los funcionarios de inteligencia. En cuanto a los procedimientos y condiciones, las autoridades públicas autorizadas deben solicitar los datos conservados por escrito. Para acceder a las investigaciones prejudiciales es necesaria una orden judicial[344].

— Luxemburgo: las autoridades nacionales competentes son las autoridades judiciales —jueces de instrucción y fiscales—, las autoridades de seguridad del Estado, de defensa, de seguridad pública y prevención, investigación, detección y enjuiciamiento de delitos. En cuanto a los procedimientos y condiciones, el acceso exige una autorización judicial[345].

— Malta: las autoridades nacionales competentes son las Fuerzas policiales de Malta y el servicio de seguridad. En cuanto a los procedimientos y condiciones, las solicitudes deben presentarse por escrito[346].

— Países Bajos: las autoridades nacionales competentes son los funcionarios de Policía responsables de las investigaciones. En cuanto a los procedimientos y condiciones, el acceso se otorga previa orden del fiscal o del juez instructor[347].

— Polonia: las autoridades nacionales competentes son la Policía, la guardia fronteriza, los inspectores fiscales, la Agencia de seguridad interior, la Agencia de inteligencia exterior, la Oficina Central Anticorrupción, los servicios de contrainteligencia militar, los servicios de inteligencia militar, los tribunales y la Fiscalía. En cuanto a los procedimientos y condiciones, las solicitudes se han de presentarse por escrito y en el caso de la Policía, la guardia fronteriza y los

---

[343] Cf. Artículo 71, apartado 1, de la Ley de comunicaciones electrónicas (autoridades); Reglamento del Consejo de Ministros nº 820 (procedimientos).

[344] Cf. Artículo 77, apartados 1 y 2, de la Ley X-1835; informe oral a la Comisión.

[345] Cf. Artículo 5-2, apartado 1, y artículo 9, apartado 2, de la Ley de 24 de julio de 2010 (autoridades); Artículo 67-1 del Código de instrucción penal (condiciones).

[346] Cf. Artículo 20, apartados 1 y 3, del Anuncio oficial 198/2008.

[347] Cf. Artículo 126ni, Código de enjuiciamiento criminal.

inspectores fiscales deben ser autorizadas por el más alto funcionario de la organización[348].

— Portugal: las autoridades nacionales competentes son la Policía criminal, la Guardia Nacional Republicana, la Oficina de seguridad pública, la Policía criminal militar, el Servicio de inmigración y fronteras y la Policía marítima. En cuanto a los procedimientos y condiciones, la transmisión de datos exige una autorización judicial que justifique que el acceso es crucial para descubrir la verdad o que, de otra manera, resultaría imposible o muy difícil obtener pruebas. La autorización judicial está sujeta a requisitos de necesidad y proporcionalidad[349].

— Reino Unido: las autoridades nacionales competentes son la Policía, los servicios de inteligencia, las autoridades fiscales y aduaneras y otras autoridades públicas designadas en la legislación secundaria. En cuanto a los procedimientos y condiciones, el acceso se permite previa autorización de la "persona designada" y la prueba de la necesidad y proporcionalidad, en casos concretos y en circunstancias en las que la revelación de los datos esté permitida o se exija por ley. Se han acordado procedimientos específicos con los operadores[350].

— República Checa: no transpuesta.

— Rumanía: no transpuesta.

— Suecia: no transpuesta.

Como se comprueba, los regímenes de acceso a los datos presentan la mayor variedad imaginable, en una escala que oscila desde aquellos países que sólo confían el acceso a la autoridad judicial bajo firmes garantías procesales hasta aquellos que autorizan el acceso a una panoplia de órganos policiales, judiciales y administrativos bajo requisitos de mero trámite. En su Informe de Evaluación de 2011, la Comisión Europea ha adelantado su intención de evaluar en el futuro "la necesidad y las opciones para lograr

---

[348] Cf. Artículo 179, apartado 3, de la Ley de telecomunicaciones de 16 de julio de 2004, modificada por el artículo 1 de la Ley de 24 de abril de 2009.

[349] Cf. Artículo 2, apartado 1, artículo 3, apartado 2, y artículo 9 de la Ley 32/2008.

[350] Cf. Artículo 25, anexo 1 de la Ley sobre poderes de investigación de 2000; artículo 7 del Reglamento sobre conservación de datos. El artículo 22, apartado 2, de la Ley sobre poderes de investigación establece las finalidades para las que estas autoridades pueden acceder a los datos.

un mayor grado de armonización con respecto a las autoridades facultadas y los procedimientos para obtener acceso a los datos conservados"[351]. Entre las opciones a considerar que el propio Informe adelanta, se cuenta la posibilidad de incluir listas de autoridades competentes más claramente definidas, la supervisión independiente o judicial de las solicitudes de datos, o un nivel mínimo de garantías en relación con los procedimientos que han de seguir los operadores al proporcionar acceso a los datos a las autoridades competentes [352].

13 Estadística y evaluación

A partir del art. 9 DCD, el resto del articulado de la DCD se ocupa de aspectos menores de la regulación, cuyo análisis no obstante hemos de abordar en las páginas siguientes.

Nos detendremos primeramente en el art. 10 DCD que, compuesto de dos apartados bajo la rúbrica de *Estadísticas*, establece el deber de los Estados miembros de facilitar cada año a la Comisión Europea las estadísticas sobre la conservación de datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones[353]. El apartado

---

[351] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 4.4.

[352] Ibíd.

[353] A fin de que pueda ser examinado directamente por el lector, transcribimos ahora el tenor literal del precepto:

Artículo 10. *Estadísticas.*

1. Los Estados miembros velarán por que se faciliten anualmente a la Comisión las estadísticas sobre la conservación de datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones. Tales estadísticas incluirán:

— los casos en que se haya facilitado información a las autoridades

— competentes de conformidad con el Derecho nacional aplicable, — el tiempo transcurrido entre la fecha en que se conservaron los datos y la fecha en que la autoridad competente solicitó su transmisión,

— los casos en que no pudieron satisfacerse las solicitudes de datos.

2. Tales estadísticas no contendrán datos personales.

primero especifica el contenido de tales estadísticas, que deben incluir tres concretos aspectos:

— los casos en que se haya facilitado información a las autoridades competentes de conformidad con el Derecho nacional aplicable,

— el tiempo transcurrido entre la fecha en que se conservaron los datos y la fecha en que la autoridad competente solicitó su transmisión, y

— los casos en que no pudieron satisfacerse talas solicitudes de datos.

Por su parte, el apartado segundo del artículo se limita a indicar que tales estadísticas "no contendrán datos personales"[354].

A su vez, el contenido del art. 10 DCD está estrechamente vinculado con el art. 14 DCD que, bajo la rúbrica de "evaluación" y compuesto por dos apartados, previó que a más tardar el 15 de septiembre de 2010 la Comisión presentaría al Parlamento Europeo y al Consejo una evaluación de la aplicación de la propia Directiva, así como de su impacto tanto en los operadores económicos como en los consumidores[355]. Tal

---

[354] El artículo 9 de la Propuesta se pronunciaba en términos muy parecidos, prácticamente idénticos, si bien la redacción final del precepto resulta técnicamente más precisa, al explicitar que las estadísticas sobre la conservación de versarán sobre los datos generados —no sólo tratados— en el marco de la prestación de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones.

[355] Dispone el vigente tenor lo siguiente:

Articulo 14. *Evaluacion.*

1. A más tardar el 15 de septiembre de 2010, la Comisión presentará al Parlamento Europeo y al Consejo una evaluación de la aplicación de la presente Directiva y su impacto en operadores económicos y consumidores, teniendo en cuenta los avances en la tecnología de las comunicaciones electrónicas y las estadísticas proporcionadas a la Comisión de conformidad con el artículo 10 a fin de determinar si es necesario modificar las disposiciones de la presente Directiva, en particular por lo que se refiere a la lista de datos del articulo 5 y a los períodos de conservación establecidos en el artículo 6. Los resultados de esta evaluación se harán públicos.

2. Con este fin, la Comision examinará todas las observaciones que le comuniquen los Estados miembros o el GT29 de protección de las personas en lo que respecta al tratamiento de datos personales creado por el artículo 29 de la Directiva 95/46/CE.

evaluación debía hacerse teniendo en cuenta "los avances en la tecnología de las comunicaciones electrónicas y las estadísticas proporcionadas a la Comisión a las que se refiere el artículo 10"[356]. El fin de tal evaluación era determinar si es necesario modificar las disposiciones de la DCD, "en particular —indica— por lo que se refiere a la lista de datos del artículo 5 —o sea, las categorías de datos que deben conservarse— y los períodos de conservación establecidos en el artículo 6"[357]. El precepto también explicita que los resultados de esta evaluación se debían hacer públicos[358]. El art. 14.2 DCD indica por su parte que "la Comisión examinará todas las observaciones que le comuniquen los Estados miembros o el [GT29]"[359].

Tanto las estadísticas como la evaluación prescritas tienen como finalidad la relevante función de permitir una valoración empírica —basada en datos reales— de la incorporación de la DCD a los ordenamientos internos, su eficacia y —lo que es más importante— la proporcionalidad y necesidad de sus medidas. La disponibilidad de datos cualitativos y cuantitativos fiables resulta esencial para demostrar la necesidad y la importancia de medidas de seguridad como la conservación de datos, como se reconoció en el *Plan de acción para evaluar la delincuencia y la justicia penal* de 2006[360], que incluyó entre sus objetivos el desarrollo de métodos para la recogida

---

[356] Cf. art. 14.1 DCD.

[357] Ibíd.

[358] El art. 12 de la Propuesta tenía un contenido muy similar con algunas diferencias de precisión técnico-normativa en lo referente a las fechas —se señalaba un plazo de tres años desde la adopción de la DCD—. Sin embargo, esta primera redacción sólo se planteaba evaluar los períodos de conservación: "a fin de determinar si es necesario modificar las disposiciones de la presente Directiva, en particular". La redacción no mencionaba "la lista de datos" a conservar ya que estos se contenían en un Anexo que sería revisados mediante un régimen específico expresado en los artículos 5 y 6 de la Propuesta En concreto, dicho Anexo se revisaría "regularmente en la medida necesaria" por un Comité cuya misión consistiría en asistir a la Comisión Europea y que estaría integrado por "representantes de los Estados miembros y presidido por el representante de la Comisión". Por los motivos apuntados al tratar del art. 5 DCD, tal solución legislativa fue finalmente rechazada, y la redacción del art. 14 DCD vio reflejada tal decisión.

[359] No queda claro del tenor literal si el fin al que se está refiriendo —y al que pueden colaborar los Estados y el Grupo— es la elaboración de la evaluación, la tarea de determinar si es necesario modificar las disposiciones de la Directiva, o ambas.

[360] Cf. Comunicación (2006)437 de la Comisión sobre el desarrollo de una estrategia global y coherente de la UE para evaluar la delincuencia y la justicia penal: Plan de acción de la UE 2006-2010

periódica de datos y la inclusión de estadísticas en la base de datos de Eurostat —siempre que cumplieran las normas de calidad—. Además, no puede dejar de destacarse que tal obligación da efecto asimismo al principio de transparencia consagrado en Derecho europeo[361], al garantizar a los ciudadanos su derecho a saber cuál es la eficacia de la retención de los datos.

Los órganos que dictaminaron sobre la PDCD acogieron positivamente las previsiones de estos arts. 10 y 14 —entonces arts. 9 y 12 PDCD—. Así, el SEPD observó, al comentar el primero, que la obligación para los proveedores de suministrar estadísticas anuales ayudaría a las instituciones comunitarias a supervisar la eficacia de la ejecución y aplicación de la norma, pues como afirmaba en claros términos, "una evaluación reviste la mayor importancia en la perspectiva de las dudas sobre la necesidad de la propuesta y de su proporcionalidad"[362]. Por añadidura, el Supervisor sugirió además que se impusiera al proveedor la obligación explícita de mantener listas de enlaces y de llevar a cabo auditorías internas sistemáticas, para permitir que las autoridades nacionales de protección de datos controlasen en la práctica la aplicación de las normas relativas a la protección de datos[363]. Respecto del art. 14 DCD —art. 12 PDPD—, aconsejó el organismo que se previera una obligación aún más estricta, que contuviera una evaluación de la eficacia de la aplicación de la Directiva "desde la perspectiva de los servicios policiales", así como un diagnóstico del impacto en los derechos fundamentales de las personas a las que se refieren los datos[364]. Dicha evaluación debía tener lugar periódicamente —por lo menos cada dos años— y con tal fin la Comisión debía incluir "cualquier prueba que pudiese afectar a la evaluación". Asimismo, la Comisión debía tener la obligación de presentar modificaciones a la propuesta, siempre que resultara conveniente[365] —como prevé el artículo 18 DPCE[366]—. Aunque todas

---

(COM(2006) 437 final). El documento en su versión oficial está publicado en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0437:FIN:ES:PDF

[361] cf. art. 11 TUE.

[362] Cf. Dictamen del SEPD…, doc. cit., punto 65.

[363] Cf., en el mismo sentido, el Dictamen del SEPD de 23 de marzo de 2005 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el sistema de información de visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros, punto 3.9.

[364] Cf. Dictamen del SEPD…, doc. cit., punto 73.

[365] Ibíd.

estas sugerencias del SEPD eran ciertamente ambiciosas y altamente garantistas, lo cierto es que las mismas sólo fueron implícita y parcialmente acogidas por el legislador europeo, pues la evaluación que prevé el vigente art. 10 DCD se refiere a la aplicación de la DCD —lo que desde luego no excluye la limitación de derechos fundamentales— y su impacto en operadores económicos y consumidores teniendo en cuenta las estadísticas proporcionadas a la Comisión de conformidad con el propio precepto. Tales estadísticas, por el tipo de datos que han de contener —casos en que se haya facilitado información a las autoridades competentes, lapsos de tiempo, etc.— permiten en cierta medida un estudio de la eficacia de la aplicación de la Directiva desde la perspectiva de los servicios policiales [367]. Aunque no se haya reconocido la bianualidad de la evaluación, ni la necesidad de especificar los casos relevantes, el art. 14 DCD ha dispuesto finalmente el deber para la Comisión de examinar "todas las observaciones que le comuniquen los Estados miembros", que pueden transmitir las de sus autoridad nacionales de protección de datos, y las observaciones del propio GT29.

---

[366] Conforme al art. 18 de la Directiva 2002/58/CE —*Revisión*—, la Comisión "presentará al Parlamento Europeo y al Consejo, a más tardar tres años después de la fecha contemplada en el apartado 1 del artículo 17, un informe sobre la aplicación de la presente Directiva y su impacto en los operadores económicos y los consumidores, con especial atención a las disposiciones sobre comunicaciones no solicitadas y teniendo en cuenta la situación internacional. Para ello, la Comisión podrá recabar información de los Estados miembros, quienes deberán facilitarla sin retrasos indebidos. Cuando proceda, la Comisión presentará propuestas para modificar la presente Directiva teniendo en cuenta los resultados del informe mencionado, los cambios que hayan podido tener lugar en el sector y cualquier otra propuesta que juzgue necesaria para mejorar la eficacia de la presente Directiva".

[367] Por su parte, el GT29 coincidió en estas observaciones, aunque fue más allá en alguna de sus propuestas. En concreto, el Grupo señalaba que, "dado que la Propuesta se basa en la evaluación concreta de los supuestos y requisitos previos a los que hace referencia, […] las medidas de conservación de datos previstas deber[ía]n estar limitadas en el tiempo de conformidad con el concepto de "legislación sunset" (legislación de vigencia limitada) ". El GT29 consideraba además que la Directiva debía tener un período de vigencia de tres años. Al vencimiento de esos años, las medidas nacionales de ejecución que imponen la conservación de datos deberían "dejar de aplicarse, sin perjuicio de la posibilidad de iniciar el análisis requerido para que el Consejo y el Parlamento Europeo elaboren una nueva decisión y aprueben una nueva directiva también antes del vencimiento del período de tres años". Obviamente, tal propuesta no encontró acogida en la norma final. Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 8.

En todo caso, la puesta en práctica de las previsiones de los arts. 10 y 14 DCD tomó finalmente forma en el ya citado *Informe de Evaluación de la Comisión Europea al Consejo y al Parlamento Europeo sobre la Directiva de conservación de datos (Directiva 2006/24/CE)*[368], que vio la luz el 18 de abril de 2011, esto es, con bastante retraso respecto del plazo del 15 de septiembre de 2010 fijado por el art. 14.1 DCD. El texto, tal como manda el precepto, evalúa la aplicación de la DCD por parte de los Estados miembros y su impacto en operadores económicos y consumidores teniendo en cuenta los avances en la tecnología de las comunicaciones electrónicas y las estadísticas proporcionadas a la Comisión Europea, a fin de determinar si es necesario modificar las disposiciones de la misma, en particular por lo que se refiere a la lista de datos y a los períodos de conservación[369]. Adicionalmente, el Informe también ha incluido su propio examen acerca de la incidencia de la DCD en los derechos fundamentales, en respuesta a las numerosas críticas sobre la materia formuladas desde diversas instancias[370].

En lo que se refiere a su elaboración, el Informe se nutrió del resultado de los debates y contribuciones de los Estados miembros, expertos y partes interesadas, como su mera lectura del texto pone de manifiesto. Cabe además destacar la gran influencia que ha ejercido en el documento los informes adoptados por la *Plataforma para la conservación de datos electrónicos con fines de investigación, detección y enjuiciamiento de los delitos graves*[371] así como los del GT29[372], particularmente, su

---

[368] Puede accederse a la edición oficial del Informe de Evaluación en el siguiente link: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:ES:PDF

[369] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 1.

[370] Asimismo, también estudia la necesidad de medidas que aborden los aspectos ligados a la utilización de tarjetas SIM anónimas con fines delictivos, que en buena parte influyó en la elaboración de las Conclusiones del Consejo sobre la lucha contra la utilización, con fines delictivos, de las comunicaciones electrónicas y de su anonimato, Sesión n.º 2908 del Consejo de Justicia y Asuntos de Interior, celebrado en Bruselas los días 27 y 28 de noviembre de 2008.

[371] Este Grupo de Expertos —al que dedicamos un apartado más adelante— se creó en virtud de la Decisión 2008/324/CE de la Comisión, DO L 111 de 23.4.2008, pp. 11-14. La Comisión se ha reunido con el Grupo regularmente. Sus documentos pueden consultarse en: http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm

[372] El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales fue creado en virtud de lo dispuesto en el artículo 29 de la Directiva de protección de datos (Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24.10.1995 sobre la protección de las personas

informe sobre la segunda acción —*Evaluación del cumplimiento por parte de los Estados miembros de los requisitos de la Directiva sobre protección y seguridad de los datos*[373]—, que ya mencionamos en apartados anteriores.

Además de estas contribuciones, la Comisión organizó algunas actividades para obtener un mayor número de opiniones. Así, por ejemplo, en mayo de 2009 convocó una *Conferencia de Evaluación de la Directiva de conservación de datos*, a la que asistieron autoridades de protección de datos, representantes del sector privado, de la sociedad civil y de la universidad, y que tuvo su secuela en diciembre de 2010 con la *Conferencia sobre la Aplicación de la Directiva de conservación de datos*, en la que se compartieron las evaluaciones preliminares de la DCD y se debatieron los futuros retos a afrontar. Previamente, en septiembre de 2009, la Comisión había enviado un cuestionario a las partes interesadas que recibió setenta respuestas[374]. A nivel estatal, entre octubre de 2009 y marzo de 2010 se llevaron a cabo reuniones entre la Comisión y representantes de cada Estado miembro y de países asociados del Espacio Económico Europeo para debatir con más detalle cuestiones relativas a la aplicación de la DCD[375].

No deja de resultar parádojico que el objetivo armonizador de la DCD haya fracasado también en lo que se refiere a esta tarea de evaluación, o lo que es lo mismo, en la ejecución de los arts. 10 y 14 DCD. Aunque en cumplimiento de estas previsiones la Comisión Europea pidió a los Estados miembros que facilitasen información detallada sobre los casos de solicitudes individuales de datos, las estadísticas que estos

---

físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos - DO L 281 de 23.11.1995, p. 31).

[373] Informe 01/2010, sobre la segunda acción conjunta de ejecución: cumplimiento a escala nacional por los proveedores de telecomunicaciones y proveedores de servicios de internet de las obligaciones nacionales de conservación de datos de tráfico sobre la base jurídica de los artículos 6 y 9 de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas y de la Directiva 2006/24/CE sobre conservación de datos, por la que se modifica la Directiva sobre la privacidad y las comunicaciones electrónicas (WP 172, de 13.7.2010). Disponible en http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm.

[374] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 2. Las respuestas se han publicado en el sitio web de la Comisión: http://ec.europa.eu/homeaffairs/news/consulting_public/consulting_0008_en.htm.

[375] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 2.

proporcionaron diferían ampliamente en alcance y detalle, como lamenta el propio Informe[376]. Además, dado que una mayoría de países empezaron a aplicar la DCD más tarde de lo previsto —especialmente en lo que se refiere a los datos relacionados con internet—, los retrasos en la transposición se tradujeron en que sólo nueve Estados miembros pudiesen proporcionar, para 2008 y 2009, todas las estadísticas requeridas por el art. 10 DCD[377]. Por añadidura, sólo unos pocos países distinguieron en sus respuestas entre los diferentes tipos de comunicación o señalaron la antigüedad de los datos en el momento de la solicitud, mientras que la mayoría facilitó estadísticas anuales sin un desglose detallado, como era de desear[378]. En concreto, diecinueve Estados miembros proporcionaron alguna estadística sobre el número de solicitudes de datos en 2008 o 2009; entre ellos figuran Irlanda, Grecia y Austria —a quienes se solicitaron datos a pesar de la ausencia de transposición de la legislación en su momento— y la República Checa y Alemania, cuya legislación de conservación de datos fue posteriormente anulada. Por su parte, siete Estados miembros que habían traspuesto la DCD no facilitaron estadísticas, aunque, de entre ellos, Bélgica facilitó una estimación del volumen anual de las solicitudes de datos de telefonía —unas trescientas mil—. Para intentar compensar estas disparidades e insuficiencias, la Comisión se dirigió por escrito a los Estados miembros en julio de 2010 solicitándoles más información cuantitativa y cualitativa sobre la necesidad y utilidad práctica de los datos conservados. Sólo diez Estados miembros respondieron con detalles de casos concretos en los que resultó necesario contar con esos datos[379].

---

[376] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 22.

[377] Ibíd.

[378] Ibíd. A saber, República Checa, Dinamarca, Alemania, Estonia, Irlanda, Grecia, España, Francia, Chipre, Letonia, Lituania, Malta, Países Bajos, Austria, Polonia, Eslovenia, Eslovaquia, Finlandia y Reino Unido.

[379] Ibíd. A saber, Bélgica, República Checa, Chipre, Lituania, Hungría, Países Bajos, Polonia, Eslovenia y Reino Unido. Suecia también notificó varios casos de delitos graves específicos en las que los datos de tráfico históricos, que estaban disponibles a pesar de la ausencia de una obligación de conservación de datos, fueron cruciales para lograr las condenas.

Cabe destacar que la falta de interés de los Estados por los procedimientos de evaluación de la DCD encuentra en el caso español un claro ejemplo. Concretamente, la Ley 25/2007, de 18 de octubre —esto es, la norma española por la que se transpone en nuestro ordenamiento interno la Directiva — no ha

Todas estas carencias, unidas al hecho de que la mayoría de los Estados miembros no transpusieron completa y debidamente la Directiva hasta los dos últimos años y utilizaron diferentes interpretaciones respecto de la fuente de las estadísticas, son la causa de que el objetivo perseguido por los arts. 10 y 14 DCD puede considerarse parcialmente incumplido. Por una parte, la evaluación realizada por el Informe ha permitido llegar a ciertas conclusiones valiosas, buena parte de las cuales estamos utilizando en esta Tesis. Por otra, sin embargo, las estadísticas recogidas apenas cubren los concretos objetivos marcados por el art. 10 DCD, y en consecuencia, la evaluación pretendida por el art. 14 DCD no ha podido ser abordada de un modo mínimamente satisfactorio.

No es de extrañar por tanto que la Comisión, en la propuesta para revisar el marco de la conservación de datos que recoge el propio Informe, se haya visto obligada a declarar su intención expresa de arbitrar procedimientos "viables" para la medición y la presentación de informes que permitan controlar, "de forma transparente y adecuada", la conservación de datos, "sin que supongan cargas indebidas para los sistemas de justicia penal y los servicios con funciones coercitivas"[380].

Sólo cabe esperar que, en el futuro, las dificultades habidas en la elaboración del primer informe puedan ser superadas, de tal manera que posteriores evaluaciones puedan satisfacer más cumplidamente la finalidad marcada por los arts. 10 y 14 DCD.

---

regulado ningún cauce específico a través del cual nuestro país deba facilitar anualmente a la Comisión las estadísticas sobre la conservación de datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas en territorio español. Tampoco se ha previsto un procedimiento concreto por el que España, como Estado miembro, deba colaborar con sus observaciones —usando la terminología del artículo— a fin de determinar si es o no necesario la modificación de la Directiva, o de evaluar su aplicación e impacto en operadores económicos y consumidores. Tales lagunas sólo caben ser juzgadas negativamente.

[380] Ibíd.

14 Recursos judiciales, responsabilidad y sanciones

Alcanzando ya las últimas previsiones del articulado, hemos de detenernos ahora en el examen del art. 13 DCD, que regula en sus dos apartados todo lo relativo a recursos judiciales, responsabilidad y sanciones relacionados con la presente normativa[381].

El régimen de recursos judiciales, responsabilidad y sanciones de la DCD refleja de manera coherente los principios básicos en materia de protección de datos en la Unión Europea. La Directiva 95/46/CE exige que los Estados miembros protejan los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de datos personales —y, en particular, su derecho a la intimidad—, para asegurar el libre flujo de datos personales en la Comunidad. Con esta finalidad, impone a los Estados miembros la obligación de establecer sanciones por el incumplimiento de las disposiciones adoptadas en en ejecución de dicha Directiva. Así lo advierte expresamente su art. 24. Por otra parte, el art. 22 del mismo cuerpo legal establece que, sin perjuicio del recurso administrativo que pueda interponerse —en particular ante la autoridad nacional de protección de datos—, y antes de acudir a la autoridad judicial, los Estados miembros han de asegurarse que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate. Adicionalmente, el art. 23 dispone que los Estados miembros han de proveer para que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito de sus datos o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la propia

---

[381] Transcribimos a continuación el tenor del artículo:

Artículo 13. *Recursos judiciales, responsabilidad y sanciones.*

1. Cada Estado miembro adoptará las medidas que se impongan para velar por que se apliquen plenamente, en lo que se refiere al tratamiento de datos en el marco de la presente Directiva, las medidas nacionales de aplicación del capítulo III de la Directiva 95/46/CE relativas al establecimiento de recursos judiciales, responsabilidad y sanciones.

2. Cada Estado miembro adoptará, en particular, las medidas que se impongan para velar por que cualquier acceso intencionado o la transferencia de datos conservados de conformidad con la presente Directiva que no estén permitidos por la legislación nacional adoptada de conformidad con la presente Directiva se castiguen con sanciones, incluidas sanciones administrativas o penales, que sean eficaces, proporcionadas y disuasorias.

Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido[382].

Cuando la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas tradujo los principios establecidos en la Directiva 95/46/CE a normas específicas para el sector de las comunicaciones electrónicas, su art. 15.2 dispuso que los tres mencionados artículos sobre recursos judiciales, responsabilidad y sanciones de la Directiva 95/46/CE habían de aplicarse también a las disposiciones nacionales que se adoptaran con arreglo a la Directiva 2002/58/CE[383]. No es de extrañar, por tanto, que la DCD —que se enmarca también en el ámbito de la protección de datos y las comunicaciones electrónicas— haya dispuesto igualmente en su art. 13 que cada Estado miembro debe adoptar las medidas necesarias para velar por que se apliquen plenamente, en lo que se refiere al tratamiento de datos en el marco de la propia DCD, las medidas nacionales de aplicación del capítulo III de la Directiva 95/46/CE relativas al establecimiento de recursos judiciales, responsabilidad y sanciones, esto es: los ya

---

[382] Transcribimos aquí el tenor literal de los tres artículos:

"Artículo 22. Recursos. Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.

Artículo 23. Responsabilidad. 1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Artículo 24. Sanciones. Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de, las disposiciones adoptadas en ejecución de la presente Directiva".

[383] Por su parte, la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información (DO L 69 de 16.3.2005, p. 67.), establece que el acceso intencionado e ilícito a un sistema de información, incluido a los datos conservados dentro del mismo, debe ser sancionable como delito.

expuestos arts. 22, 23 y 24[384]. No obstante, puesto que estas medidas de tutela y sanción no cubren todas las ilicitudes que pueden cometerse en aplicación de la DCD, el art. 13.2 previene que cada Estado miembro ha de adoptar, en particular, las medidas "que se impongan" para velar por que cualquier acceso intencionado, o la transferencia de datos conservados de conformidad con la DCD que no estén permitidos por la legislación nacional adoptada de conformidad con la DCD, se castiguen con sanciones administrativas o penales que sean eficaces, proporcionadas y disuasorias. De esta manera, las nuevas violaciones de los derechos a la intimidad y la protección de datos que la DCD hace potencialmente factibles pueden recibir un tratamiento sancionador adecuado[385].

A la vista de esta regulación, hemos de hacer notar que la DCD deja libertad a los Estados miembros —dentro del marco del Derecho europeo y de las directrices mencionadas— para que establezcan a través de su legislación interna las sanciones, los recursos y el sistema de responsabilidad que consideren oportunos con el fin de garantizar la aplicación de estas disposiciones comunitarias.

En el caso de España, por ejemplo, estas previsiones de la DCD se plasman en nuestro Derecho interno en la LCD, resultado de la transposición de la DCD, que establece un capítulo III que, con su único art. 10, determina el "régimen aplicable al incumplimiento de obligaciones contempladas en esta Ley" y sus "infracciones y sanciones", remitiendo el incumplimiento de las obligaciones previstas en la norma a las sanciones previstas por la LGT, "sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados", que se regirá por el régimen de la LOPD[386]. Por su parte, el Título VI de

---

[384] Los Considerandos 18 y 19, DCD, citan lo dispuesto en las Directivas 95/46/CE y 2002/58/CE para justificar la regulación sobre sanciones, recursos y responsabilidad establecida en la DCD.

[385] La Propuesta de Directiva no contenía una referencia expresa a la necesidad de que los Estados miembros adoptasen medidas para castigar accesos no debidos a los datos conservados y transferencias no permitidas por la legislación nacional.

[386] Adelantamos aquí el contenido del Capítulo III. Infracciones y sanciones:

Artículo 10. *Régimen aplicable al incumplimiento de obligaciones contempladas en esta Ley.*

esta Ley —"infracciones y sanciones"—, que comprende los arts. 43 a 48 LOPD, regula todo lo relativo a la responsabilidad —art. 43 LOPD—, tipos de infracciones —art. 44 LOPD—, tipo de sanciones —art. 45 LOPD—, prescripción —art. 47 LOPD— o el procedimiento sancionador —art. 48 LOPD— en el ámbito de la protección de datos *stricto sensu*[387]. Sobre ellos volveremos al estudiar con detalle la ley española que ha traspuesto la DCD.

15 Modificación de la Directiva 2002/58/CE

El art. 11 DCD inserta un apartado *bis* en el art. 15.1 DPCM, conforme al cual el contenido de este art. 15.1 no se aplicará a los datos que deben conservarse de conformidad con la DCD para los fines de su art. 1.1[388]. Como ya hemos tenido ocasión de exponer anteriormente, el art.15.1 DPCE reconocía la facultad de los Estados miembros para limitar el alcance de los derechos y obligaciones establecidos en sus arts. 5, 6, 8 y 9, que obligan a los proveedores de servicios de comunicaciones electrónicas a borrar los datos o hacerlos anónimos cuando ya no se necesiten para la transmisión o la facturación, salvo consentimiento previo. Con la inclusión del art. 15.1 bis, los Estados ya no podrán regular la extensión de estos derechos cuando se trate de los datos del art. 5 DCD y para fines de "investigación, detección y enjuiciamiento de

---

El incumplimiento de las obligaciones previstas en esta Ley se sancionará de acuerdo con lo dispuesto en la Ley 32/2003, de 3 de noviembre, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

[387] Dígase de paso que estos artículos han sido recientemente modificados en su redacción por la Ley 2/2011, de 4 de marzo, de Economía Sostenible. En concreto se ha retocado la redacción de los artículos 43 (apdo. 2), 44 (apdos. 2, 3 y 4), 45 (apdos. 1 a 5), 46 (apdos. 1, 2 y 3) y 49.

[388] El artículo 11 de la Propuesta presentaba un contenido similar, si bien su redacción fue ampliamente mejorada en el texto finalmente aprobado: "Artículo 11. Modificación de la Directiva 2002/58/CE. Se insertará el siguiente apartado 1 bis en el artículo 15 de la Directiva 2002/58/CE: 1 bis. El apartado 1 no se aplicará a las obligaciones relativas a la conservación de datos con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como terrorismo y delincuencia organizada, derivadas de la Directiva 2005/.../CE. * * DO L ... de...".

delitos graves, tal como se definen en la legislación nacional de cada Estado miembro"[389].

La delimitación de las consecuencias jurídicas que comporta la inclusión de este apartado *bis* en el art. 15.1 DPCE resulta sumamente confusa, si bien intentaremos abordar a continuación una interpretación plausible.

Hemos de empezar recordando lo que ya se explicó en el primer capítulo de esta Primera Parte, en concreto, que la Directiva 2002/58/CE no se aplica a las actividades de los Estados que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado o a las actividades del Estado en materia penal. Así lo dispone el art. 1.3 DPCE, que no viene sino a reconocer que todas esas actividades no pueden ser objeto de una directiva porque no son competencia del Derecho comunitario. Así pues, cuando el art. 15.1 DPCE advierte que los Estados miembros pueden *limitar el alcance* de algunas de sus previsiones para proteger la seguridad del Estado, la persecución de delitos, etc., está haciendo una afirmación érronea que genera confusión, porque ni el art. 15 ni ningún otro artículo de la Directiva 2002/58/CE son de aplicación a las actividades penales, de defensa o seguridad de los Estados. Los Estados miembros pueden ignorar la Directiva cuando se trate de estos fines, estando sólo sujetos a su propia legislación, su sistema constitucional y sus compromisos comunitarios e internacionales, que es como ha de interpretarse las menciones del art. 15 DPCE a los principios generales del Derecho comunitario, al art. 6 TUE o a que la limitación ha de constituir una medida necesaria proporcionada y apropiada en una sociedad democrática.

Así pues, la integración de los arts. 1.1 y 11 DCD con los art. 15.1 y 15.1 *bis* y el resto de la Directiva 2002/58/CE nos lleva a concluir que, conforme a este marco legislativo, los Estados miembros no pueden ahora adoptar medidas legales que: 1) versen sobre

---

[389] Cf. art. 1.1 DCD. Transcribimos para su directo examen el tenor literal de la norma vigente: Artículo 11. Modificación de la Directiva 2002/58/CE. En el artículo 15 de la Directiva 2002/58/CE se inserta el apartado siguiente: «1 bis. El apartado 1 no se aplicará a los datos que deben conservarse específicamente de conformidad con la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, para los fines recogidos en el artículo 1, apartado 1, de dicha Directiva.

los datos del art. 5 DCD, y 2) tengan como fin garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves[390]. Esta interpretación parece confirmarse con lo advertido en el considerando de la DCD, según el cual el art. 15.1 DPCM "sigue aplicándose a los datos […] cuya conservación no se prescribe específicamente en la presente Directiva […], así como a la conservación a efectos, incluidos judiciales, diferentes de los contemplados en la presente Directiva".

Obviamente, dado que estamos ante medidas legales que tienen por objeto la seguridad pública y y las actividades del Estado en materia penal, estas previsiones están arrogándose competencias legislativas de los Estados reconocidas por el Derecho primario de la Unión y, expresamente, por el art. 1.3 DPCE, lo que nos devuelve a la cuestión de fondo sobre el problema de competencia y legalidad comunitarias que subyacen a la DCD.

En realidad, entendemos que lo que el legislador ha pretendido con la inclusión de este art. 15.1 *bis* DPCD es cerrar la posibilidad de que los Estados miembros, basándose en las facultades reconocidas por los arts. 1.3 y 15.1 DPCE, modifiquen las disposiciones de la DCD, por ejemplo, extendiendo unilateralmente los plazos de conservación. Esta extensión de los plazos debe efectuarse con la aquiescencia de la Comisión en los términos previstos por el art. 12 DCD, que a su vez presentan las dificultades que ya analizamos en un capítulo anterior.

La complejísima integración del art. 11 DCD ha dado lugar a que la Comisión "aclarara" en su Informe de Evaluación de 2011 que los Estados miembros "siguen teniendo la posibilidad de establecer excepciones al principio de confidencialidad de las comunicaciones", puesto que la DCD regula únicamente la conservación de datos para el fin más limitado de la investigación, detección y enjuiciamiento de delitos graves[391]. Por lo demás, la propia Comisión ha sostenido esto mismo y lo contrario, al no dudar en admitir que la ahora compleja relación e integración de la DCD y la Directiva

[390] Debido a la pésima y farragosísima técnica legislativa, cabe la duda si además cabría añadir una tercera condición, consistente en que la medida legal afecte a los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la DPCM.

[391] Cf. Informe de evaluación sobre la Directiva…, doc. cit., punto 3.2.

2002/58/CE, combinada con la ausencia de una definición en cualquiera de las dos Directivas de la noción de delito grave, hace igualmente "que sea difícil distinguir entre, por una parte, las medidas adoptadas por los Estados miembros para transponer las obligaciones de conservación de datos establecidas en la Directiva y, por otro, la práctica general en los Estados miembros" por lo que respecta la conservación de datos permitida por el art. 15.1 DPCE[392].

16 Transposición y entrada en vigor

Concluimos el estudio del articulado de la DCD con el examen de sus dos últimos preceptos, los arts. 15 y 16 DCD. Aunque hemos de volver sobre estos artículos al tratar las circunstancias que han rodeado la transposición de la Directiva, presentaremos aquí todo lo referente a sus antecedentes y contenido tal como ha quedado plasmado en el texto en vigor.

Así, el art. 16 DCD, bajo la rúbrica de "entrada en vigor", dispuso que la Directiva entraría en vigor "a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*". Dado que dicha publicación tuvo lugar el 13 de abril de 2006, la norma empezó a surtir efectos el 3 de mayo del 2006[393].

Por su parte, el art. 15 DCD —bajo la rúbrica de "transposición" y compuesto de tres apartados— determinó que los Estados miembros "pondrían en vigor" (*sic*) las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a la Directiva a más tardar el 15 de septiembre de 2007, informando de ello a la Comisión inmediatamente[394]. Como es de rigor, el precepto también advierte

[392] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 5.

[393] El artículo 14 de la Propuesta, bajo la rúbrica de "Entrada en vigor", contenía una redacción similar a la del finalmente art. 16, al disponer que "la presente Directiva entrará en vigor el vigésimo día siguiente al de su publicación en el Diario Oficial de la Unión Europea". Veinte días era, en cualquier caso, lo previsto desde el principio, y lo que finalmente se mantuvo.

[394] El tenor literal del precepto dispone:

que las correspondientes disposiciones adoptadas por los Estados miembros deben hacer referencia a la DCD o ir acompañadas de dicha referencia en su publicación oficial[395].

Seguidamente, el segundo apartado del art. 15 DCD establece la obligación para los Estados miembros de comunicar expresamente a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la DCD. Además —lo que resulta más importante—, el apartado tercero permitió que cada Estado miembro pudiera aplazar hasta el 15 de marzo de 2009 la aplicación de la Directiva en lo que se refiere a la conservación de los datos de comunicaciones en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet. Los Estados miembros que pretendieran acogerse a esta posibilidad debían notificarlo al Consejo y a la Comisión mediante una declaración, a formular en el

---

Artículo 15. *Transposición.*

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar el 15 de septiembre de 2007. Informarán de ello inmediatamente a la Comisión. Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

3. Cada Estado miembro podrá aplazar hasta el 15 de marzo de 2009 la aplicación de la presente Directiva en lo que se refiere a la conservación de los datos de comunicaciones en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet. Los Estados miembros que se propongan recurrir al presente apartado lo notificarán al Consejo y a la Comisión, mediante una declaración, en el momento de la adopción de la presente Directiva. Tal declaración se publicará en el *Diario Oficial de la Unión Europea*.

[395] El artículo 13 de la Propuesta, bajo la rúbrica de "Transposición", se componía sólo de dos apartados. El segundo apartado presentaba una redacción idéntica a la definitiva. El primero también presentaba una redacción similar a la finalmente adoptaba, si bien contenía la obligación para los Estados miembros de "comunicar inmediatamente a la Comisión el texto de esas disposiciones" —que fue eliminada por ser redundante con el apartado segundo— y "una tabla de correlaciones entre esas disposiciones y la presente Directiva", deber éste que también fue suprimido en el texto definitivo.

momento de la adopción de la DCD, la cual había de ser publicada en el Diario Oficial de la Unión Europea[396].

Respecto de la primera previsión mencionada, conforme a la cual la DCD había de transponerse por los Estados miembros a más tardar el 15 de septiembre de 2007, hemos de destacar que tal plazo resultaba demasiado breve, sobre todo si tenemos en cuenta la complejidad de la materia en presencia. No hay mejor prueba de esta insuficiencia que el hecho de que dieciséis de los veinticinco Estados miembros establecieron, en el momento de adopción de la Directiva, excepciones conforme al art. 15.3 DCD, con el fin de retrasar dieciocho meses la transposición de la norma en lo referido a la conservación de los datos de comunicaciones de acceso a internet, telefonía por internet y el correo electrónico. Si bien España no se contó entre ellos —de ahí que haya sido uno de los primeros países en aprobar legislación interna para transponer la DCD— el tenor literal de las declaraciones de los demás Estados fueron publicadas junto con la Directiva. Recogemos el texto completo de estas declaraciones para su directo examen entre los Anexos de la presente Tesis.

17 Grupo de Expertos "Plataforma para la conservación de datos electrónicos con fines de investigación, detección y enjuiciamiento de los delitos graves"

Al concluir el examen y comentario de las disposiciones de la vigente DCD, no podemos dejar de hacer referencia a un órgano estrechamente relacionado con esta

[396] El artículo 13 de la Propuesta no presentaba el tercer apartado, ni la posibilidad de aplazar hasta el 15 de marzo de 2009 la aplicación de la DCD en lo que se refiere a la conservación de los datos de comunicaciones en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet. Tal ausencia es en parte lógica ya que la Propuesta contemplaba un plazo distinto de retención —más breve— para los datos relacionados con comunicaciones electrónicas que tuvieran lugar entera o principalmente a través del Protocolo internet —cf. art. 7 de la Propuesta—. En la Directiva vigente no se prevé tal distinción.

normativa: el Grupo de Expertos *Plataforma para la conservación de datos electrónicos con fines de investigación, detección y enjuiciamiento de los delitos graves*.

Los motivos de su creación se recogen en el considerando decimocuarto de la DCD, que recoge la intención de la Comisión de crear un grupo integrado por autoridades policiales de los Estados miembros, asociaciones del sector de las comunicaciones electrónicas, representantes del Parlamento Europeo y autoridades de protección de datos, incluido el Supervisor Europeo de Protección de Datos[397]. Advirtiendo que las tecnologías relativas a las comunicaciones electrónicas están cambiando rápidamente y que las legítimas necesidades[398] de las autoridades competentes podrían evolucionar, el legislador consideró oportuna la existencia de un organismo que tuviera como fin ofrecer asesoramiento y fomentar el intercambio de experiencias de las mejores prácticas sobre estos asuntos[399]. Su creación y regulación se llevó a cabo dos años más tarde a través de la *Decisión 2008/324/CE, de la Comisión, de 25 de marzo de 2008, por la que se crea el Grupo de Expertos "Plataforma para la conservación de datos electrónicos con fines de investigación, detección y enjuiciamiento de los delitos graves"*[400]. Los considerandos segundo a quinto de la Decisión ofrecen tres argumentos adicionales acerca de la conveniencia de crear el Grupo. Además de repetir el ya mencionado por la DCD, de recabar opiniones y de fomentar el intercambio de buenas prácticas en los distintos asuntos relativos a la conservación de los datos personales[401], el considerando tercero recuerda la previsión del art. 14 DCD, conforme a la cual, a más tardar el 15 de septiembre de 2010, la Comisión habría de presentar al Parlamento

---

[397] Este órgano ya había sido previsto por la Propuesta de Directiva, lo cierto es que el texto final de la DCD omitió —por razones que se desconocen— su creación y regulación, que se llevó a cabo dos años más tarde a través de la Decisión 2008/324/CECf. Exposición de Motivos de la Propuesta…, doc. cit. p. 5.

[398] La versión española traduce por "requisitos" el término inglés "requirements", si bien el sentido del término aquí responde mejor al significado de "necesidades".

[399] Cf. Considerando decimocuarto, DCD

[400] Decisión 2008/324/CE, de la Comisión, de 25 de marzo de 2008, por la que se crea el Grupo de Expertos "Plataforma para la conservación de datos electrónicos con fines de investigación, detección y enjuiciamiento de los delitos graves (DO L 111 de 23.4.2008, p. 11/14).

[401] Cf. Considerando 2, Decisión 2008/324/CE, que reitera lo afirmado en el Considerando 14, DCD.

Europeo y al Consejo una evaluación sobre la aplicación de la Directiva y su impacto en los operadores económicos y los consumidores, teniendo en cuenta los progresos de la tecnología de las comunicaciones electrónicas y las estadísticas suministradas a la Comisión sobre la conservación de datos, contribuyendo dicha evaluación a determinar si es necesario modificar la Directiva de conservación de datos, en especial por lo que se refiere a la lista de datos contemplada en el art. 5 DCD y a los períodos de conservación previstos en el art. 6 DCD[402]. Por último, el considerando cuarto recuerda que el 10 de febrero de 2006, el Consejo y la Comisión hicieron pública una declaración conjunta en relación con la evaluación de la DCD, en la que se afirmaba que la Comisión invitaría a las partes interesadas a reuniones regulares de evaluación a fin de intercambiar información sobre los progresos tecnológicos, los costes y la eficacia de la aplicación de la Directiva y que durante este proceso se invitaría a los Estados miembros a informar a los demás socios de sus experiencias en la aplicación de la Directiva y a compartir sus buenas prácticas[403].

Sobre la base de estas consideraciones, la Plataforma es definida en el art. 1 de la Decisión 2008/324/CE como un grupo de expertos en asuntos relacionados con la conservación de los datos personales a efectos de aplicación de la ley en el sector de las comunicaciones electrónicas, cuyas tareas principales son responder las consultas de la Comisión en relación con cualquier asunto relativo a la conservación de los datos electrónicos pertinentes para la investigación, la detección y el enjuiciamiento de los delitos graves[404]. Más allá de su labor consultiva —que es la principal[405]—, el art. 2.2 de la Decisión encomienda al Grupo otras tareas que pueden enmarcarse en la misión más genérica de facilitar el intercambio de buenas prácticas y contribuir a la evaluación

---

[402] Cf. Considerando 3, Decisión 2008/324/CE.

[403] Cf. Considerando 4, Decisión 2008/324/CE. La declaración conjunta afirmaba también —recuerda este considerando 4— que sobre la base de tales discusiones, "la Comisión considerar[ía] la presentación de cualquier propuesta necesaria, incluido por lo que se refiere a cualquier dificultad que pueda haberse presentado a los Estados miembros en relación con la aplicación técnica y práctica de la Directiva, en especial su aplicación al correo electrónico y a los datos de telefonía por Internet".

[404] Cf. art. 2.1, Decisión 2008/324/CE. Prevé el mismo artículo que cualquier miembro del Grupo de Expertos puede aconsejar a la Comisión que consulte al mismo sobre una cuestión específica.

[405] "El grupo de expertos trabajará como grupo consultivo", advierte el Considerando 6, Decisión 2008/324/CE.

por parte de la Comisión de los costes y la eficacia de la Directiva, así como del desarrollo de las tecnologías pertinentes que pueden afectar a la DCD[406]. Más concretamente, son objetivos del órgano:

a) constituir un foro de diálogo y de intercambio de experiencias y buenas prácticas, en especial entre las autoridades competentes de los Estados miembros y los representantes del sector de las comunicaciones electrónicas, sobre las cuestiones relacionadas con la conservación de datos personales por los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones con el fin de garantizar que los datos estén disponibles con fines de investigación, detección o enjuiciamiento de los delitos graves;

b) fomentar y facilitar una orientación común sobre la aplicación de la DCD;

c) intercambiar información sobre los progresos tecnológicos pertinentes, los costes y la eficacia de la aplicación de la DCD;

d) ayudar a la Comisión a identificar y definir las dificultades a las que se enfrentan los Estados miembros en la aplicación técnica y práctica de la DCD, en especial su aplicación al correo electrónico y a los datos de telefonía por internet;

e) ayudar a la Comisión en su evaluación de la aplicación de la DCD y de su impacto en los operadores económicos y los consumidores.

La composición del Grupo se ordena a la correcta consecución de estas funciones. Sus miembros son elegidos de entre los grupos mencionados en el considerando 14 DCD, hasta un máximo de veinticinco miembros que los representen equilibradamente[407]. De este modo, componen la Plataforma:

a) las autoridades responsables de la aplicación de la ley en los Estados miembros —hasta un máximo de diez miembros—;

b) los miembros del Parlamento Europeo —hasta dos miembros—;

---

[406] Cf. Considerando 6, Decisión 2008/324/CE.

[407] Cf. considerando 8 y art. 3.1, Decisión 2008/324/CE, así como Considerando 14, DCD.

c) asociaciones de la industria de las comunicaciones electrónicas —hasta ocho miembros—;

d) representantes de las autoridades responsables de protección de datos —hasta cuatro miembros—;

e) el Supervisor Europeo de Protección de Datos —un miembro—.

Los miembros elegidos entre las autoridades responsables de la aplicación de la ley de conservación de datos en cada uno de los países de la Unión y los diputados del Parlamento Europeo son designados y nombrados por la Dirección General de Justicia, Libertad y Seguridad a propuesta de los Estados miembros, requeridos a tal efecto, y del Parlamento Europeo, respectivamente y a título personal[408]. Por otra parte, los miembros de las asociaciones de la industria de las comunicaciones electrónicas, los representantes de las autoridades responsables de protección de datos y del SEPD son nombrados por la misma Dirección General mediante invitación[409]. Además, la Comisión está facultada para invitar a participar en las tareas del Grupo, si ello fuera útil o necesario, a otros expertos u observadores externos con competencia específica en un tema concreto en un tema del orden del día, o a representantes oficiales de los Estados miembros, de los países candidatos o de terceros países y de organizaciones internacionales, intergubernamentales y no gubernamentales[410]. Otros funcionarios de la Comisión con interés en los procedimientos pueden asistir a las reuniones del Grupo o de los subgrupos que se creen[411].

Hasta su renovación en 2013, el Grupo ha estado formado por veintidós miembros de pleno derecho; nueve elegidos entre los diputados del Parlamento Europeo y las autoridades responsables de la aplicación de la ley de conservación de datos en cada

---

[408] No obstante, cualquiera de ellos puede designar a su vez a un experto que los represente en las reuniones del Grupo. Cf. art. 3.2, Decisión 2008/324/CE.

[409] Estas asociaciones u organismos tienen derecho a nombrar expertos que les representen en las reuniones. Cf. art. 3.2, Decisión 2008/324/CE.

[410] Cf. art. 5, Decisión 2008/324/CE.

[411] Cf. art. 4.3, Decisión 2008/324/CE.

uno de los países de la Unión[412], y trece elegidos entre los miembros de las asociaciones de la industria de las comunicaciones electrónicas, los representantes de las autoridades responsables de protección de datos y del SEPD[413]. La Plataforma cuenta además en la actualidad con seis observadores[414].

Acerca del estatus jurídico de sus miembros, cabe señalar que los mismos disponen de un mandato de cinco años renovables[415], si bien anualmente han de firmar un documento por el cual se comprometen a actuar de acuerdo con el interés público, así como una declaración que indica la ausencia o existencia de cualquier interés que

---

[412] De acuerdo con la información disponible en el Registro de grupos de expertos y otras entidades similares, actualizada a 23 de mayo de 2012 y accesible en http://ec.europa.eu/transparency/regexpert/detailGroup_pdf.cfm?groupID=2230, sus nombres, países y afiliación son los siguientes: Alexander Alvaro, Miembro del Parlamento Europeo (Alemania); Christian Aghroum, Chef de l'Office, de la Lutte contre la criminalité liée aux technologies de l'information et de la communication (Francia); Jesper Voigt Andersen, de la Danish National Police (Dinamarca); Jill Tan, Policy Lead for the Regulation of Investigatory Powers Act , RIPA (Reino Unido); Kurt Alavaara, Detective Superintendent del Security Service (Suecia); Luc Beirens Chief Commissioner, Federal Computer Crime Unit (Bélgica); Michael Bruns, Head of Computer and Internet Crime, Federal Court (Alemania); Stephen Conroy, Sergeant en Garda Headquarters (Irlanda); y, Tomasz Ksiaszkiewicz, Head of Operational Techniques, National Police HQ (Polonia).

[413] Las asociaciones de la industria con representación actualmente en la Plataforma son las siguientes: Cable Europe, ETIS, EuroISPA, European Competitive Telecommunications Association (ECTA), European Telecommunications Network Operators Association (ETNO), GSM Association Europe, PRISM International, TechAmerica Europe. Aparte del SEPD, las autoridades responsables de protección de datos presentes en la actual composición del Grupo son los siguientes: la Commission de la protection de la vie privée (Bélgica); la Agencia Española de Protección de Datos (España); la Commission National d'Informatique et Libertés (Francia) y el Garante per la protezione dei dati personali (Italia). Información extraída del Registro de grupos de expertos y otras entidades similares, actualizada a 23 de mayo de 2012 y accesible en http://ec.europa.eu/transparency/regexpert/detailGroup_pdf.cfm?groupID=2230

[414] A título individual, Caspar Bowden y Charles Miller (Reino Unido); y por parte de los entes públicos, disponen de un observador en la Plataforma la European Free Trade Association; el European Telecommunications Standards Institute (ETSI): Technical Committee on Lawful Interception; Europol y Noruega. Información extraída del Registro de grupos de expertos y otras entidades similares, actualizada a 23 de mayo de 2012 y accesible en http://ec.europa.eu/transparency/regexpert/detailGroup_pdf.cfm?groupID=2230.

[415] Cf. art. 3.3, Decisión 2008/324/CE.

pueda socavar su objetividad[416]. Para mayor transparencia, se prevé por la Decisión que sus nombres sean publicados en la página web de la Dirección General de Justicia, Libertad y Seguridad, en la serie C del Diario Oficial de la Unión Europea y en el Registro de Grupos de Expertos de la Comisión[417]. Ni los miembros ni los expertos y observadores invitados reciben remuneración alguna por los servicios que prestan[418].

En cuanto al funcionamiento de la Plataforma, sus reglas básicas se recogen en el artículo 4 de la Decisión 2008/324/CE así como en un reglamento interno aprobado por el propio Grupo sobre el modelo estándar diseñado por la Comisión[419]. Entre los principales rasgos de su régimen, de acuerdo con el art. 4, cabe destacar que el órgano es presidido por la Comisión, en cuyas dependencias se reúne normalmente el Grupo de expertos, según los procedimientos y el calendario que ésta determina[420]. La Comisión también desempeña las funciones de secretaría, y tiene facultad para publicar, en la lengua original del documento en cuestión, cualquier resumen, conclusión, conclusión parcial o documento de trabajo del Grupo[421]. Además, de común acuerdo con la Comisión, pueden crearse subgrupos para examinar cuestiones específicas, con un

---

[416] Cf. art. 3.5, Decisión 2008/324/CE.

[417] Cf. art. 3.6, Decisión 2008/324/CE. La información con los datos del Grupo son accesibles en el Registro de grupos de expertos y otras entidades similares, y pueden consultarse en el siguiente enlace: http://ec.europa.eu/transparency/regexpert/detailGroup_pdf.cfm?groupID=2230. La web con los nombres de los actuales miembros de la Plataforma y demás información se encuentra en el siguiente link: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/index_en.htm.

[418] Cf. art. 6, Decisión 2008/324/CE. No obstante, el precepto prevé que la Comisión reembolse los gastos de viaje y, si procede, de estancia, de los miembros, expertos y observadores en el marco de las actividades del Grupo con arreglo a las normas de la Comisión relativas a la retribución de los expertos externos.

[419] Cf. art. 4.6, Decisión 2008/324/CE. El reglamento interno de la Plataforma fue aprobado en su primera sesión, que tuvo lugar el 28 de noviembre de 2008. El texto íntegro del mismo puede consultarse en http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2230.

[420] Cf. art. 4.1, Decisión 2008/324/CE.

[421] Cf. art. 4.7, Decisión 2008/324/CE.

mandato definido[422], si bien hasta la actualidad la Plataforma no ha recurrido nunca a este método de trabajo[423].

De acuerdo con la información disponible, el Grupo se ha reunido en doce ocasiones, la última el 19 de octubre de 2012[424], para estudiar asuntos relacionados con la aplicación y mejora de la DCD. Entre 2009 y 2012 publicó diversos documentos que ofrecen sugerencias y clarificaciones muy técnicas sobre el modo de interpretar los términos, técnicamente complejos, empleados por la DCD. Naturalmente, dichas interpretaciones no tienen carácter vinculante ni pueden considerarse una interpretación auténtica, dado que la Plataforma es un mero órgano consultivo. Los documentos publicados hasta la fecha, con sus títulos originales, nos dan una idea de la labor desarrollada por el Grupo en este período[425]:

- "Webmail and web-based messaging", de 3 de diciembre de 2009;
- "Obligation to retain e-mail logs – when records of spam e-mails be retained?", de 16 de julio de 2009;
- "Closer understanding of the term 'transit providers' in relation to its application in Directive 2006/24/EC", de 3 de diciembre de 2009;
- "Closer understanding of the term 'third party networks and service providers' in relation to its application in Directive 2006/24/EC", de 23 de julio de 2009;
- "Closer understanding of the term 'internet telephony' in relation to its application in Directive 2006/24/EC"; de 3 de diciembre de 2009;

---

[422] Cf. art. 4.2, Decisión 2008/324/CE.

[423] Así consta en la información disponible en el *Registro de grupos de expertos y otras entidades similares*, actualizada a 23 de mayo de 2012 y disponible en http://ec.europa.eu/transparency/regexpert/detailGroup_pdf.cfm?groupID=2230.

[424] Información extraída del *Registro de grupos de expertos y otras entidades similares*, actualizada a 23 de mayo de 2012 y disponible en http://ec.europa.eu/transparency/regexpert/detailGroup_pdf.cfm?groupID=2230. En esta dirección también pueden hallarse las actas de las cinco últimas reuniones.

[425] Los documentos están disponibles en la web de la Plataforma, habilitada por la Dirección General de Interior de la Comisión Europea: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/index_en.htm

- "Closer understanding of the possibilities of providers to store traffic data in a Member State other than the Member State of origin of the data ('Central data storage') in relation to its application in Directive 2006/24/EC", de 11 de octubre de 2010;
- "Closer understanding of the term 'Data security' in relation to its application in Directive 2006/24/EC", de 11 de octubre de 2010.
- "Guidance on the term "unsuccessful call attempt" as defined in Directive 2006/24/EC", de 8 de junio de 2012.
- "Economic impact of Directive 2006/24/EC on providers of e-communication networks and services and reimbursement of costs", de 8 de junio de 2012.
- "Guidance on the Member States obligation to submit to the Commission annual statistics pursuant to Directive 2006/24/EC", de 30 de noviembre de 2012.

Finalmente, es importante señalar que tanto el Grupo de Expertos como su regulación permanecieron en vigor hasta el 31 de diciembre de 2012[426]. La Comisión, mediante Decisión de 18 de abril de 2013, volvió a poner en vigor la norma comentada y abrió la convocatoria para la formación de un nuevo Grupo de Expertos este año[427].

18 Costes

Aunque no se trata de un asunto estrictamente jurídico, un examen exhaustivo de la DCD no puede dejar de abordar la denominada cuestión de los costes. Es evidente que el cumplimiento de las prescripciones de la DCD comporta una carga económica para

[426] Cf. art. 7, Decisión 2008/324/CE.

[427] Cf. Commission Decision of 18.4.2013 on setting up an experts group on best practice in the implementation of electronic communications data retention for the investigation, detection and prosecution of serious crime ('the data retention experts group'). Texto complete disponible en http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/20130418_data_retention_expert_group_decision_en.pdf

los sujetos obligados por la norma a dar cumplimiento a sus previsiones, esto es, los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones —cf. art. 1.1 DCD—. Obviamente, tales gastos no comportan beneficio alguno para estas compañías.

Aunque el vigente articulado de la DCD no prevea ningún tipo de compensación económica a favor de los proveedores por los gastos de almacenamiento y gestión en que la misma les hace incurrir, no era ése el caso del art. 10 PDCD, que bajo la rúbrica de "costes", establecía que los Estados miembros habían de asegurarse que los proveedores de servicios de comunicación electrónica de acceso público o de una red de comunicaciones pública serían "reembolsados por los costes adicionales en que demuestren haber incurrido para cumplir con las obligaciones que la presente Directiva les impone".

Debe destacarse que durante la tramitación de la norma cinco grandes asociaciones industriales afirmaron, en una declaración conjunta a la Comisión, que el impacto económico de la DCD era "relevante" o "enorme" para los pequeños proveedores de servicios[428]. Además, un estudio realizado antes de la transposición de la Directiva en una mayoría de Estados miembros estimó el coste de crear un sistema de conservación de datos para un proveedor de servicios de internet con medio millón de clientes en, aproximadamente, 375.240 euros el primer año y 9.870 euros al mes de costes de funcionamiento en adelante, y los costes de creación de un sistema de extracción de datos en 131.190 euros, con unos costes de funcionamiento de 28.960 euros al mes[429].

En este estado de cosas, para cuando la enmienda 85 del Parlamento —por la que se suprimía este art. 10 de la Propuesta— eliminó definitivamente del texto toda referencia a los costes, la cuestión de quién debía hacer frente a los gastos que

[428] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 20. Dicha declaración puede consultarse en http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

[429] Cf. *Wilfried Gansterer & Michael Ilger, Data Retention: The EU Directive 2006/24/EC from a Technological Perspective, Wien: Verlag Medien und Recht,* 2008.

comportaría la aplicación de la DCD se había convertido en uno de los temas clave en su elaboración[430].

Lo cierto es que la cuestión económica guarda estrecha relación con los motivos en que se apoyó la Comisión para aprobar la Directiva. Como consecuencia de las disposiciones de conservación de datos que adoptaron los Estados miembros unilateralmente en los primeros años del siglo, los operadores de estos Estados miembros se habían visto obligados a adquirir equipos de conservación de datos y a emplear personal para recuperar datos en nombre de los servicios con funciones coercitivas, mientras que los de otros Estados miembros no tuvieron que hacerlo, dando lugar a distorsiones en el mercado comunitario[431]. Al decir de la Comisión, las diferencias en las disposiciones legislativas, reglamentarias y técnicas en los Estados miembros en materia de conservación de datos de tráfico plantearían "obstáculos para el mercado interior de comunicaciones electrónicas ya que los prestadores de servicios se enfrentan a requisitos diferentes en cuanto a los tipos de datos que deben conservarse"[432]. Por añadidura, las tendencias de los modelos empresariales y las ofertas de servicios, tales como la proliferación de tarifas planas y de servicios de comunicaciones electrónicas de prepago o gratuitos, tuvieron como efecto que los operadores dejaran gradualmente de almacenar datos de tráfico y de localización con fines de facturación, reduciendo así la disponibilidad de dichos datos a efectos de la justicia penal y con fines policiales[433]. Los atentados terroristas de Madrid en 2004 y de Londres en 2005 no hicieron sino añadir urgencia a los debates europeos sobre la forma de abordar estas cuestiones.

En favor de la compensación económica a los proveedores se usaron dos argumentos. Por una parte, podría suponer el que las medidas de seguridad que adoptasen las compañías probablemente no acabaran siendo todo lo apropiadas y necesarias que debían para ahorrar gastos. Por otra, se preveía que un incremento de los costes para las

---

[430] Cf. Informe de evaluación sobre la Directiva…, doc. cit., pp 14-20. No puede olvidarse tampoco que el asunto de los costes está relacionado con la duración de los plazos de conservación y los tipos de datos a retener —cuanto más tiempo y cuantos más datos a retener, mayores costes—.

[431] Cf. Informe de evaluación sobre la Directiva…, doc. cit., punto 3.2.

[432] Cf. Exposición de Motivos de la Propuesta…, doc. cit., p. 2, y Considerando 6 de la DCD.

[433] Ibíd.

empresas de telecomunicaciones sería finalmente repercutido contra los propios usuarios europeos[434].

En un intento de contentar a las compañías afectadas, la Exposición de Motivos de la Propuesta presentó la DCD como una norma en la que la carga financiera y administrativa para los gobiernos nacionales, los operadores económicos y los ciudadanos se había minimizado de varias maneras[435]. En primer lugar, la Directiva establecía una armonización a nivel europeo de la materia, lo que significaría por sí misma una reducción de los costes para los proveedores internacionales de servicios de comunicaciones electrónicas o de una red de comunicaciones pública[436]. En segundo lugar, los gastos se habían minimizado, limitando estrictamente los períodos de conservación y los grupos de datos que debían conservarse[437]. Dada la importancia de la medida para la prevención y lucha contra la delincuencia y el terrorismo, se consideraba que los costes adicionales para los Estados miembros causados por las disposiciones de reembolso de costes resultaban "proporcionados"[438].

Lo cierto es que durante la tramitación de la norma la compensación a los proveedores de los costes adicionales generados por la DCD acabó por convertirse en un punto de desacuerdo entre los distintos órganos dictaminantes.

Así, tanto el SEPD como el GT29 valoraron positivamente el reembolso de los costes[439]. El primero entendía que existía una relación directa entre la adecuación de las medidas de seguridad y los costes de estas medidas, es decir, entre la seguridad y los costes, y que por tanto, la previsión del art. 10 PDCD, al disponer el reembolso de los costes adicionales comprobados, podría servir de incentivo para que los proveedores invirtieran adecuadamente en la infraestructura técnica[440]. Según las estimaciones de la

---

[434] Cf. Exposición de Motivos de la Propuesta…, doc. cit., p. 12.

[435] Cf. Exposición de Motivos de la Propuesta…, doc. cit., p. 8.

[436] Ibíd.

[437] Ibíd.

[438] Ibíd.

[439] Cf. Dictamen del SEPD…, doc. cit., punto 36, y Dictamen 4/2005, del GT29…, doc. cit., pp. 67-70.

[440] Cf. Dictamen del SEPD…, doc. cit., punto 34: "tal incentivo podría consistir en una indemnización a los proveedores por los costes adicionales de las medidas de seguridad adecuadas".

evaluación de impacto trasmitidas por la Comisión al SEPD, para una red y un proveedor de servicios de grandes dimensiones, los costes ascenderían a más de ciento cincuenta millones de euros para un plazo de retención de doce meses, con costes de funcionamiento anuales de alrededor de cincuenta millones de euros[441]. Estas graves consecuencias económicas no podían ser ignoradas sin más por el legislador europeo, sin perjuicio de que el SEPD estimara en todo caso necesarias cifras "más precisas" en lo que se refería a las consecuencias financieras estimadas del reembolso total de los costes adicionales de los proveedores[442], para poder juzgar la Propuesta en toda su extensión.

Por su parte, el GT29 consideró importante que los gastos adicionales que soportasen los proveedores de comunicaciones electrónicas fueran compensados por los Estados miembros de modo que no se produjeran efectos negativos en el nivel de protección de datos ni tampoco en la esfera económica de los ciudadanos, a quienes se podría cargar parte de los gastos de los proveedores[443]. Más allá de esto, según el Grupo, las medidas de conservación de datos debían incluir igualmente el reembolso de las inversiones de adaptación de los sistemas de comunicaciones, de los gastos de la revelación de datos a las autoridades policiales y de las medidas de seguridad[444]. Finalmente, el órgano dejó planteada la cuestión acerca de si cabría considerar que el derecho de un proveedor al reembolso de los gastos debía estar sujeto al cumplimiento de las normas mínimas, así como tener lugar sobre una base individual, examinando caso por caso[445].

Pese tan buenos argumentos, la postura que finalmente prevaleció fue la diametralmente opuesta, sobre la base de los razonamientos esgrimidos por el CESE. En su opinión, los costes que comportaba la DCD debían contemplarse como "una carga que los operadores deberían asumir por el mero hecho de estar en el mercado, sin

---

[441] Cf. Dictamen del SEPD…, doc. cit., punto 68. Se trataba de las cifras calculadas por Asociación Europea de Operadores de Telecomunicaciones (ETNO) y a un informe del diputado europeo Alvaro sobre el proyecto de Decisión marco.

[442] Ibíd.

[443] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 11.

[444] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 12.

[445] Ibíd.

que el erario público, y por ende todos los ciudadanos, tengan que soportarla"[446]. Con un tono ciertamente agresivo, el punto 2.4.11 de su Dictamen empezaba manifestando que "sorprendía" que la Propuesta regulase los denominados "costes adicionales" en que incurrirían los operadores para cumplir con los deberes de almacenamiento y transmisión de datos. En concreto, el Comité no dudó en manifestar que discrepaba "totalmente" de la Comisión en cuanto a la necesidad de rembolsar los tales a costa del erario público porque los beneficios en términos de seguridad pública fueran hacerse sentir en el conjunto de la sociedad[447]. Tales afirmaciones eran a su entender "cuando menos, inexactas", porque cada Estado miembro establecería libremente la cantidad y fórmula de resarcimiento de dichos costes, atendiendo a criterios propios, según las circunstancias y necesidades de seguridad de su sociedad.

Con tono aún más terminante, el Dictamen lanzaba al aire los siguientes interrogantes:

> "de seguir el criterio de la Comisión, se podría llegar a cuestionar lo siguiente:
> — ¿acaso los proveedores de estos servicios no se benefician de la seguridad y estabilidad social que garantizan los Estados?
> — ¿acaso dichos proveedores no se benefician de la seguridad jurídica del Estado de Derecho?, o
> — ¿acaso, los proveedores no se benefician del acceso al mercado único donde encuentran su legítimo negocio empresarial gracias a la diligencia de los poderes públicos nacionales, y no solo a la acción de la Comisión"[448].

Por todo lo anterior, el Comité concluía que la propuesta de reembolso de costes adicionales resultaba "improcedente" y "debía suprimirse"[449].

Las últimas novedades respecto a la polémica de los costes han venido de la mano del Informe de Evaluación elaborado por la Comisión. En el mismo se afirma que la

---

[446] En relación con el tema de los costes, Cf. Dictamen del CESE…, doc. cit., puntos 2.4.11 a 2.4.14. Ha de notarse que este punto del Dictamen fue objeto de fuerte controversia en el seno del CESE; véase el anexo al mismo donde se encuentran las Propuestas de enmiendas al Dictamen y el resultado de las votaciones.

[447] Cf. Considerando 13 de la Propuesta

[448] Cf. Dictamen del CESE…, doc. cit., punto 2.4.13.

[449] Cf. Dictamen del CESE…, doc. cit., punto 2.4.14.

mayoría de los operadores, en su respuesta al cuestionario enviado en 2009 por la Comisión, fueron incapaces de cuantificar el impacto de la Directiva en la competencia, en los precios al por menor para los consumidores o en la inversión en nuevas infraestructuras y servicios, y que, por éste y otros motivos, no hay pruebas de ningún "efecto cuantificable o sustancial de la Directiva en los precios al consumo de los servicios de comunicaciones electrónicas"[450]. Tampoco los representantes de los consumidores realizaron contribuciones a estas consultas[451].

Asimismo, debe resaltarse que una encuesta realizada en Alemania en nombre de una organización de la sociedad civil indicó que los consumidores tenían previsto modificar su comportamiento en lo que respecta a las comunicaciones y evitar el uso de servicios de comunicaciones electrónicas en algunas circunstancias; sin embargo, parece que no hay pruebas que corroboren un cambio de comportamiento en Alemania, ni en la Unión Europea en general[452]. Por su parte, no puede dejar de destacarse que el Tribunal Constitucional alemán, en su Sentencia de 2 de marzo de 2010, llegó a la conclusión de que el establecimiento de un derecho de almacenamiento "no era particularmente gravoso para los proveedores de servicios afectados ni desproporcionado con respecto a las cargas económicas soportadas por las empresas como consecuencia de la obligación de almacenamiento"[453].

Por otra parte, en lo que se refiere a la aproximación de los países miembros a esta cuestion, se constata que en la actualidad sólo dos Estados miembros reembolsan tanto gastos operativos como de capital, en tanto que seis, únicamente los gastos operativos. El cuadro siguiente, extraído del Informe de Evaluación de la Comisión, muestra una panorámica de la situación a fecha de abril de 2011[454]:

---

[450] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 31.

[451] Ibíd.

[452] La encuesta fue realizada por Forsa y encargada por AK Vorratsdatenspeicherung y puede consultarse en este enlace: http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

[453] Cf. *Bundesverfassungsgericht*, 1 BvR 256/08 de 2 de marzo de 2010, parágrafo 299.

[454] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 31.

Cuadro 6: Estados miembros que reembolsan costes			
Estado miembro	**Gastos operativos**	**Gastos de capital**	**Costes de reembolso anuales (millones EUR)**
Bélgica	Sí	No	22 (2008)
Bulgaria	No	No	-
República Checa	No transpuesta		
Dinamarca	Sí	No	-
Alemania	No transpuesta		
Estonia	Sí	No	-
Irlanda	No	No	-
Grecia	No	No	-
España	No	No	-
Francia	Sí	No	-
Italia	-	-	-
Chipre	No	No	-
Letonia	No	No	-
Lituania	Sí, si se solicita y está justificado	No	-
Luxemburgo	No	No	-
Hungría	No	No	-
Malta	No	No	-
Países Bajos	Sí	No	-
Austria	No transpuesta		
Polonia	No	No	-
Portugal	No	No	-
Rumanía	No transpuesta		
Eslovenia	No	No	-
Eslovaquia	No	No	-
Finlandia	Sí	Sí	1
Suecia	No transpuesta		
Reino Unido	Sí	Sí	55 (reembolsados por los costes soportados a lo largo de tres años)

Por las razones expuestas, se concluye que —una vez más— la DCD no ha alcanzado plenamente su objetivo de armonización ni de establecimiento de unas condiciones de competencia equitativas para los operadores en la Unión Europea. Ante la evidencia, la Comisión ha hecho expreso propósito de estudiar "opciones" para reducir al mínimo los obstáculos para el funcionamiento del mercado interior "garantizando que se reembolse sistemáticamente a los operadores los costes en que incurran para cumplir con los requisitos de conservación de datos, poniendo especial atención en las pequeñas y medianas empresas"[455]. En este sentido, el Informe concreta que la Comisión tiene previsto evaluar el impacto de las futuras modificaciones de la Directiva para la

[455] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 31.

industria y los consumidores, incluyendo en su caso, una encuesta específica del Eurobarómetro para medir la percepción del público[456].

19 Transposición de la DCD en los Derechos nacionales

Aunque algunos detalles de la transposición de la DCD hayan sido analizados separadamente en los apartados anteriores, conviene ahora exponerlos de una manera conjunta y ordenada cronológicamente, de manera que dé cuenta de modo más nítido del cauce por el que ha tenido lugar y cómo ésta ha originado una incesante litigiosidad a nivel comunitario y nacional que hacen que podamos juzgar el resultado final como *problemático* e *insatisfactorio*.

Hemos de empezar recordando que los destinatarios de la DCD son —como los de cualquier otra directiva— los Estados miembros. Así lo expresa con concisión el art. 17 DCD. Además, los Estados tenían el deber conforme al art. 16 DCD de transponer la Directiva, poniendo "en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido" en la norma[457].

El plazo para tal tarea era el 15 de septiembre de 2007 "a más tardar"[458], si bien el art. 15.3 DCD previó que cada Estado pudiera aplazar hasta el 15 de marzo de 2009 la aplicación de la Directiva "en lo que se refiere a la conservación de los datos de comunicaciones en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet". Así, el ámbito material afectado por esta última previsión no se extendía a todos los datos. En concreto, ha de recordarse que el art. 5 DCD dispone seis categorías de datos que deben conservarse de conformidad con la Directiva, señalando para cada categoría los datos a retener con respecto a dos fuentes; por un lado, la telefonía de red fija y a la telefonía móvil, por otro, el acceso a internet, correo

[456] Ibíd.

[457] cf. art. 15.1 DCD.

[458] Ibíd.

electrónico por internet y telefonía por internet[459]. La posibilidad de aplazar la aplicación de la Directiva cubría sólo esta última fuente, lo que en concreto y en definitiva afectaba sólo a los siguientes tipos de datos[460]:

— la identificación de usuario asignada —art. 5.1.a).2).i) DCD—;
— la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía —art. 5.1.a).2).ii) DCD—;
— el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo internet —IP—, una identificación de usuario o un número de teléfono —art. 5.1.a).2).iii) DCD—;
— la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por internet —art. 5.1.b).2).i) DCD—;
— los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación —art. 5.1.b).2).ii) DCD—;
— la fecha y hora de la conexión y desconexión del servicio de acceso a internet, basadas en un determinado huso horario, así como la dirección del Protocolo internet, ya sea dinámica o estática, asignada por el proveedor de acceso a internet a una comunicación, así como la identificación de usuario del abonado o del usuario registrado —art. 5.1.c).2).i) DCD—;
— la fecha y hora de la conexión y desconexión del servicio de correo electrónico por internet o del servicio de telefonía por internet, basadas en un determinado huso horario —art. 5.1.c).2).ii) DCD—;

---

[459] Cf. art. 5 DCD, a saber: a) datos necesarios para rastrear e identificar el origen de una comunicación; b) datos necesarios para identificar el destino de una comunicación; c) datos necesarios para identificar la fecha, hora y duración de una comunicación; d) datos necesarios para identificar el tipo de comunicación; e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; y, f) datos necesarios para identificar la localización del equipo de comunicación móvil.

[460] Cf. art. 5.3 DCD.

— el servicio de internet utilizado —art. 5.1.d).2) DCD, "datos necesarios para identificar el tipo de comunicación"—;
— el número de teléfono de origen en caso de acceso mediante marcado de números —art. 5.1.e).3).i) DCD—;
— la línea digital de abonado —DSL— u otro punto terminal identificador del autor de la comunicación —art. 5.1.e).3).ii) DCD—.

Los Estados miembros que desearan aplazar hasta el 15 de marzo de 2009 la aplicación de la DCD en lo referente a la conservación de todos estos concretos datos debían notificarlo al Consejo y a la Comisión, mediante una declaración en el momento de la adopción de la norma[461]. El texto de tales declaraciones había de publicarse en el Diario Oficial de la Unión Europea[462], lo que finalmente se llevó a cabo conjuntamente con la publicación oficial del articulado de la DCD. Un total de dieciséis Estados —de los veinticinco que formaban la Unión Europea en el momento de la adopción del texto— se acogieron a esta posibilidad. Por orden alfabético, son los siguientes: Alemania, Austria, Bélgica, Chipre, Eslovenia, Estonia, Finlandia, Grecia, Letonia, Lituania, Luxemburgo, Países Bajos, Polonia, Reino Unido, República Checa y Suecia[463].

Estudiadas con detalle, se constata que el contenido de las dieciséis declaraciones de aplazamiento no es homogéneo, aunque las diferencias apenas poseen relevancia jurídica. Algunos países se limitaron a manifestar una eventual voluntad de acogerse a dicha excepción. Así, Alemania se *reservó* el derecho a posponer la aplicación "por un período de 18 meses"[464]; Luxemburgo *declaró su intención de acogerse* al art. 15.3[465];

---

[461] Ibíd.

[462] Ibíd.

[463] Ver Anexo a la publicación oficial de la DCD (DO L 105 de 13.4.2006, p. 54/63).

[464] En las siguientes notas a pie de página reproducimos el tenor literal de estas declaraciones: "Declaración de Alemania en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Alemania se reserva el derecho a posponer la aplicación de la presente Directiva a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet, por un período de 18 meses a partir de la fecha especificada en el artículo 15, apartado 1".

[465] "Declaración de Luxemburgo en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Conforme a lo dispuesto en el apartado 15, apartado 3, de la Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados o generados en relación con la prestación de servicios de

y Suecia *deseó tener la opción de aplazar la aplicación*[466]. Otros, en cambio, directamente se acogieron a la previsión anunciando que agotarían tal plazo, como Chipre[467], Lituania[468] o Letonia[469]. La mayoría, en cambio, simplemente anunciaron su voluntad de aplazamiento, sin más detalle, como fue el caso de Reino Unido[470], Austria[471], Países Bajos[472] o República Checa[473].

---

comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, el Gobierno del Gran Ducado de Luxemburgo declara que tiene la intención de acogerse al artículo 15, apartado 3, de la Directiva en cuestión, a fin de poder aplazar su aplicación en lo que respecta a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet".

[466] "Declaración de Suecia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Suecia, en virtud del artículo 15, apartado 3, desea tener la opción de aplazar la aplicación de la presente Directiva a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet".

[467] "Declaración de Chipre en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. La República de Chipre declara que aplazará la aplicación de la Directiva, respecto a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet, hasta la fecha fijada en el artículo 15, apartado 3".

[468] "Declaración de Lituania en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. En virtud del artículo 15, apartado 3, del proyecto de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (en lo sucesivo, «la Directiva»), la República de Lituania declara que, una vez adoptada la Directiva, aplazará su aplicación a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet durante el período mencionado en el artículo 15, apartado 3".

[469] Declaración de Letonia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. De acuerdo con el artículo 15, apartado 3, de la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, Letonia declara que aplazará la aplicación de la Directiva a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet hasta el 15 de marzo de 2009.

[470] "Declaración del Reino Unido en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. El Reino Unido declara, de acuerdo con el artículo 15, apartado 3, de la Directiva sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de

Conviene hacer ahora una breve aclaración sobre las fechas y plazos en los que se desarrolló la transposición de la DCD. Así, la fecha de adopción de nuestra norma fue el 15 de marzo de 2006, que es la que se ha incorporado al título oficial[474] de la norma[475]. Distinta de la fecha de adopción es la de publicación de la Directiva, que tuvo lugar el 13 de abril de 2006 en el Diario Oficial de la Unión Europea —número L 105,

---

acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, que aplazará la aplicación de esa Directiva a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet".

[471] "Declaración de Austria en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Austria declara que aplazará la aplicación de la presente Directiva a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet durante un período no superior a 18 meses a partir de la fecha especificada en el artículo 15, apartado 1".

[472] "Declaración de los Países Bajos en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Por lo que se refiere a la Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE, los Países Bajos harán uso de la opción de aplazar la aplicación de la Directiva a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet, durante un período no superior a 18 meses a partir de la fecha de entrada en vigor de la Directiva".

[473] "Declaración de la República Checa en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. En virtud del artículo 15, apartado 3, la República Checa declara que aplazará la aplicación de la presente Directiva a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet hasta 36 meses después de la fecha de su adopción".

En el caso de España, nuestro país no formuló tal declaración y, en consecuencia, la obligación de los proveedores de conservar los datos de comunicaciones en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet se inició con la entrada en vigor de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, exactamente el 8 de noviembre de 2007 —a los veinte días de su publicación en el Boletín Oficial del Estado (cf. Disposición final quinta. Entrada en vigor), que tuvo lugar un día después de su promulgación: el 19 de octubre de 2007

[474] Tal como figura en el DOUE: "Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE".

[475] De acuerdo con el Derecho europeo, la adopción es el momento …..

páginas 105/54 a 105/63 de la edición española[476]—. La fecha de publicación es relevante en tanto que determina a su vez la fecha en que la norma ha de entrar en vigor. Puesto que el art. 16 DCD estableció un plazo de veinte días desde la publicación oficial, la Directiva entró finalmente en vigor el 3 de mayo de 2006[477].

La siguiente fecha a la que debe hacerse mención es el 15 de septiembre de 2007, límite del plazo de los Estados para adoptar las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la Directiva. De este modo, los Estados miembros dispusieron de dieciocho meses para la transposición. No conviene olvidar que, aunque a fecha de 15 de septiembre de 2007 la DCD debía estar íntegramente transpuesta en cada uno de los ordenamientos nacionales, la vigencia del deber para los proveedores de conservar datos de acceso a internet, telefonía por internet y correo electrónico por internet podía ser pospuesta por los ordenamientos interno otros dieciocho meses; no más allá, por tanto, del 15 de marzo de 2009, fecha en que el deber de conservación pasó a aplicarse plenamente respecto de la totalidad de los datos listados en la DCD[478]. En conclusión, en los países que se acogieron a esta posibilidad de aplazamiento, discurrieron treinta y seis meses —tres años— desde la adopción de la Directiva hasta el momento en que los proveedores empezaron a retener los datos de tráfico de internet.

Por otra parte, para facilitar una coordinada y eficaz implementación de la Directiva, el art. 15 DCD estableció unas mínimas medidas de control, que se concretaron en la obligación para los Estados miembros de informar inmediatamente a la Comisión de la transposición, así como en el deber, cuando los Estados miembros adoptasen dichas disposiciones, de hacer referencia a la propia Directiva o de incluir la misma en su

---

[476] El texto oficial en su edición digital puede consultarse en la base de datos legislativa de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF
Como cualquier otro ordenamiento jurídico moderno, la publicación de las normas en el Derecho europeo es imprescindible conforme….

[477] Por si cupiera alguna duda en el cómputo, tal fecha de entrada en vigor es la que consta en la información oficial proporcionada por la Comisión en su base de datos: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:ES:NOT

[478] Cf. art. 15.3 DCD.

publicación oficial, si bien los Estados eran libres para establecer las "modalidades" de tal referencia[479].

En el caso español, por ejemplo, esta última previsión se ha visto cumplida con la inclusión en la Exposición de Motivos de la norma de transposición —la *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*—, de un párrafo tercero en que se afirma lo siguiente:

> "Precisamente en el marco de este último objetivo [persecución del delito] se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, *cuya transposición a nuestro ordenamiento jurídico* es el *objetivo principal* de esta Ley"[480].

Si bien la Exposición de Motivos no forma parte del articulado, y por tanto ocupa un lugar menos visible en la norma, nada parece indicar que tal inclusión incumpla lo exigido por la legislación europea.

No obstante, para mayor garantía de una correcta transposición en fondo, forma y plazo, la DCD previó expresamente en su art. 15.2 el deber de los Estados miembros de comunicar a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la Directiva. De este modo, la Comisión —así como cualquier otro Estado, institución o ciudadano— puede tener un conocimiento adecuado de cuáles han sido las denominadas "medidas nacionales de aplicación y ejecución" a través de las cuales se ha transpuesto la DCD en cada país[481].

---

[479] Cf. art. 15.1 DCD.

[480] El subrayado es mío.

[481] Las medidas nacionales de ejecución puede consultarse en la base de datos oficial de la UE —EUR-Lex—, concretamente en el siguiente enlace: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:ES:NOT

Vuelta nuestra mirada sobre el proceso de transposición de la Directiva en los Estados miembros, se constata que el mismo ha sido *problemático* e *insatisfactorio*.

El aspecto *problemático* del proceso se pone de manifiesto en el hecho de que, a fecha de junio de 2011, si bien la legislación de transposición está en vigor en veintitrés de los veintisiete Estados miembros[482]; un Estado aún tiene que transponerla —Suecia— y otros tres han visto su legislación de transposición anulada por sus tribunales constitucionales —Alemania, República Checa y Rumanía—. Nos ocuparemos a continuación de estos casos con cierto detalle.

Respecto del caso sueco, el proyecto legislativo ha sido debatido sin éxito en diversas ocasiones. En este Estado miembro no hay ninguna obligación de conservar los datos, pero los servicios con funciones coercitivas pueden pedir y obtener datos de tráfico a los operadores —y de hecho lo hacen— en la medida en que dichos datos estén disponibles. Lo cierto es que, a la fecha en que se escriben estas líneas, la Comisión no ha recibido aún notificación de medida de transposición alguna.

En cuanto a la situación en la República Checa, Alemania y Rumanía, sus respectivos tribunales constitucionales anularon la legislación nacional de transposición de la Directiva una vez aprobada y actualmente están estudiando cómo volver a transponerla[483].

El Tribunal Constitucional de la República Checa anuló la legislación de transposición sobre la base de que, como medida que interfiere con los derechos fundamentales, la

---

[482] Ciertamente, si se tiene en cuenta el gran volumen de incumplimiento que se constata en la incorporación de las directivas europeas a los derechos nacionales, tales cifras pueden ser valoradas positivamente.

[483] Cf. Decisión nº 1258, de 8 de octubre de 2009, del Tribunal Constitucional rumano, Diario Oficial rumano nº 789 de 23 de noviembre de 2009; sentencia del Bundesverfassungsgericht 1 BvR 256/08, de 2 de marzo de 2010; Gaceta Oficial de 1 de abril de 2011, sentencia del Tribunal Constitucional de 22 de marzo sobre las disposiciones del artículo 97, apartados 3 y 4 de la Ley nº 127/2005 Coll. sobre las comunicaciones electrónicas y por la que se modifican determinados actos relacionados, y Decreto nº 485/2005 Coll. sobre la conservación de datos y su transmisión a las autoridades competentes.

legislación de transposición no es suficientemente clara y precisa en su formulación[484]. La sentencia criticó la limitación de la finalidad por no ser suficientemente restrictiva, habida cuenta de la escala y alcance del requisito de conservación de datos, y advirtió que la definición de las autoridades competentes para acceder y utilizar los datos conservados, así como los procedimientos para dicho acceso y uso, no eran suficientemente claros en la legislación de transposición para garantizar la integridad y confidencialidad de los datos. Los ciudadanos, por tanto, no contaban con suficientes garantías y salvaguardias contra posibles abusos poder por parte de las autoridades públicas. El Tribunal no criticó la propia Directiva y declaró que permitía un margen de maniobra suficiente para que República Checa la transpusiera conformidad con la Constitución. Sin embargo, el Tribunal, *obiter dictum,* manifestó dudas cuanto a la necesidad, eficiencia y adecuación de la conservación de datos de tráfico habida cuenta de la aparición de nuevos métodos de delincuencia, como los realizados mediante uso de tarjetas SIM anónimas.

Por su parte, el Tribunal Constitucional rumano aceptó que puede permitirse la interferencia con los derechos fundamentales si se respetan determinadas normas y se establecen unas salvaguardias adecuadas y suficientes para la protección contra posibles medidas arbitrarias del Estado [485] . Sin embargo, sobre la base de la jurisprudencia del TEDH, el Tribunal constató que la ley de transposición era ambigua en su alcance y finalidad y que no contaba con suficientes salvaguardias, y alegó que "una obligación legal continuada" de conservar todos los datos de tráfico durante seis meses era incompatible con los derechos a la intimidad y la libertad de expresión del art. 8 CEDH[486].

Por último, el Tribunal Constitucional Federal alemán[487] alegó que la conservación de datos genera una percepción de control que podría obstaculizar el libre ejercicio de los derechos fundamentales. Reconoció explícitamente que la conservación de datos para

[484] Sentencia del Tribunal Constitucional de la República Checa de 22 de marzo sobre la Ley nº 127/2005 y Decreto nº 485/2005; véanse en particular los apartados 45-48, 50, 51 y 56.

[485] Cf. Decisión nº 1258 del Tribunal Constitucional rumano de 8 de octubre de 2009.

[486] Cf. Tribunal Europeo de Derechos Humanos, Rotaru contra Rumania, 2000; Sunday Times contra Reino Unido, 1979; y Príncipe Hans-Adam de Liechtenstein contra Rumania, 2001.

[487] Cf. *Bundesverfassungsgericht*, 1 BvR 256/08, parágrafos 1 a 345.

usos estrictamente limitados, junto con una seguridad de los datos suficientemente elevada, no viola necesariamente la Ley Fundamental de Bonn. Sin embargo, el Tribunal destacó que la conservación de estos datos constituye una restricción grave del derecho a la intimidad y, por tanto, sólo debe ser admisible en circunstancias particularmente limitadas; y que un período de conservación de seis meses era el límite máximo —*an der obergrenze*— que podría considerarse proporcionado —apartado 215—. Los datos sólo pueden solicitarse cuando ya exista una sospecha de delito grave o pruebas de peligro para la seguridad pública, y la obtención de datos debe prohibirse en determinadas comunicaciones privilegiadas —es decir, las relacionadas con necesidades sociales o emocionales— que se basan en la confidencialidad. Los datos también deberán codificarse con una supervisión transparente de su utilización[488].

Aparte de estas sentencias, la transposición de la DCD ha dado lugar al pronunciamiento de otros tribunales constitucionales, aun sin graves consecuencias ulteriores. Tal es el caso de Bulgaria, cuya ley de transposición hubo de revisarse[489]; Chipre, donde se consideró que las resoluciones judiciales dictadas con arreglo a la ley transposición eran inconstitucionales[490]; y Hungría, donde está pendiente un asunto relativo a la omisión de los fines legales del tratamiento de datos en la legislación de transposición[491].

Ante la alta litigiosidad que a la que la DCD ha dado lugar, no es de extrañar que la propia Comisión Europea —en su Informe de Evaluación de 2011— manifestase su voluntad de estudiar todos los aspectos problemáticos apuntados por las jurisdicciones constitucionales de los Estados en su futura propuesta para revisar el marco de la conservación de datos[492], si bien, al mismo tiempo, tampoco ha dejado pasar la ocasión

---

[488] Cf. Ortiz Pradillo, J. C., Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas, La Ley Penal, Nº 75, Sección Jurisprudencia aplicada a la práctica, Octubre 2010, Editorial La Ley, versión digital.

[489] Cf. Tribunal Supremo Administrativo búlgaro, Decisión n° 13627 de 11 de diciembre de 2008.

[490]Cf. Tribunal Supremo de Chipre, recurso nº 65/2009, 78/2009, 82/2009 y 15/2010-22/2010 de 1 de febrero de 2011.

[491] La solicitud de apreciación de la constitucionalidad fue presentada por la Unión de Libertades Civiles de Hungría el 2 de junio de 2008.

[492] Cf. Informe de evaluación sobre la Directiva…, doc. cit., punto 4.9.

para exhortar a aquellos Estados miembros que aún no han transpuesto plenamente la Directiva, o que todavía no han adoptado legislación que sustituya a la legislación de transposición anulada por los tribunales nacionales, a que lo hagan lo antes posible. "De no ser este el caso, la Comisión —advertía— se reserva el derecho de ejercer sus competencias en virtud de los Tratados de la UE".

Ciertamente, esta última advertencia se ha materializado en la actividad de la Comisión durante los últimos años. A través de una serie de recursos interpuestos por la institución, la repercusión de la Directiva en el plano constitucional se ha extendido a la propia jurisdicción europea, cuyo Tribunal de Justicia ha considerado que cuatro Estados miembros hasta la fecha —Austria, Suecia, Irlanda y Grecia— han violado sus obligaciones conforme al Derecho de la Unión. El propio Tribunal de Justicia resolverá en 2014 una cuestión de legalidad sobre la DCD, planteada por Irlanda y Austria, esta vez sobre la base del respeto a los arts. 7 y 8 de la Carta de Derechos Fundamentales de la Unión.

Expuestos cronológicamente, el primer pronunciamiento al respecto vino de la mano de la Sentencia del Tribunal de Justicia —Sala Sexta— de 4 de febrero de 2010 —Asunto C- 185/09[493]—, en el que el Tribunal falló que el Reino de Suecia había incumplido las obligaciones que le incumben en virtud de la DCD al no haber adoptado dentro del plazo señalado las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a dicha Directiva y, en consecuencia, condenó en costas al Estado sueco[494].

---

[493] Resolución publicada en el Diario Oficial C 180, de 1.8.2009.

[494] El texto del recurso interpuesto por la Comisión Europea contra Suecia decía así: "Recurso interpuesto el 26 de mayo de 2009 por la Comisión de las Comunidades Europeas contra el Reino de Suecia [DO C 180 de 1.8.2009, p. 32/33], en el que se solicita que se declare ·que el Reino de Suecia ha incumplido las obligaciones que le incumben en virtud del artículo 15, apartado 1, de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, al no haber adoptado todas las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo dispuesto en dicha Directiva o al no haber comunicado a la Comisión dichas disposiciones", y que se condene en costas al Reino de Suecia.

Seguidamente, en la Sentencia del Tribunal de Justicia —Sala Séptima— de 29 de julio de 2010 —Asunto C-189/09[495]—, el Tribunal falló declarar que la República de Austria había incumplido las obligaciones que le incumben en virtud de la DCD, resolviendo el mismo sentido que en el caso sueco[496].

En tercer lugar, por Sentencia del Tribunal de Justicia —Sala Octava— de 26 de noviembre de 2009 —Asunto C-202/09[497]— y la Sentencia del Tribunal de Justicia —Sala Segunda— de igual fecha —Asunto C-211/09—, el Tribunal condenó a la República irlandesa[498] y a Grecia[499], respectivamente, en términos similares a los anteriores.

El único motivo y principal alegación es que el plazo de adaptación del Derecho nacional a la Directiva expiró el 15 de septiembre de 2007".

[495] Resolución publicada en el Diario Oficial C 246 de 11/09/201, p. 0008 – 0008.

[496] El texto del recurso interpuesto por la Comisión Europea contra Austria decía así: "Recurso interpuesto el 28 de mayo de 2009 por la Comisión de las Comunidades Europeas contra la República de Austria [DO C 180 de 1.8.2009, p. 33/33], en el que se solicita "que se declare que la República de Austria ha incumplido las obligaciones que le incumben en virtud de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, al no haber adoptado todas las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a dicha Directiva o al no haber comunicado a la Comisión dichas disposiciones", y que se condene en costas a la República de Austria.

El único motivo y principal alegación es que "el plazo de adaptación del Derecho nacional a la Directiva expiró el 15 de septiembre de 2007. En el momento en el que se interpone el presente recurso la demandada aún no ha adoptado las medidas necesarias para dar cumplimiento a lo dispuesto en la Directiva o en todo caso no las ha comunicado a la Comisión".

[497] Cf. DO C 24 de 30.1.2010, p. 16/16 y DO C 167, de 18.7.2009.

[498] El texto del recurso interpuesto por la Comisión Europea contra Austria decía así: "Recurso interpuesto el 5 de mayo de 2009 por la Comisión de las Comunidades Europeas contra Irlanda [DO C 167 de 18.7.2009, p. 7/7], en que solicita que se declare "que Irlanda ha incumplido las obligaciones que le incumben en virtud de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE al no haber adoptado las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo dispuesto en la citada Directiva o,

Por añadidura, en abril de 2011, a raíz de una Decisión del Parlamento de Suecia de posponer doce meses la adopción de legislación de transposición, la Comisión decidió llevar por segunda vez a este país ante el Tribunal de Justicia, solicitando esta vez la imposición de sanciones financieras en virtud del artículo 260 del Tratado de Funcionamiento de la Unión Europea por haber incumplido la sentencia emitida en el asunto C-185/09.

Paralelamente a estos procesos, se han planteado cuestiones prejudiciales ante el Tribunal de Justicia por parte del *Högsta domstolen* de Suecia[500] —sobre la aplicación de la DCD a cuestiones civiles— y del *Verwaltungsgericht Wiesbaden* alemán[501] —que

---

en cualquier caso, al no haber comunicado dichas disposiciones a la Comisión", y que se condene en costas a Irlanda. El único motivo y principal alegación es que "el plazo para la adaptación del Derecho interno a la citada Directiva expiró el 15 de septiembre de 2007".

[499] Cf. DO C 193, de 15.8.2009.

[500] Cf. Petición de decisión prejudicial planteada por el Högsta domstolen de Suecia el 20 de septiembre de 2010 (Asunto C-461/10):

"En el Asunto C-461/10, el Högsta domstolen de Suecia, con ocasión del caso en que son partes en el procedimiento principal como recurrentes Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget Aktiebolag y Storyside AB, y recurrida la Perfect Communication Sweden AB, ha planteado con fecha de 20 de septiembre de 2010 las siguientes cuestiones prejudiciales:

"1) ¿La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 , sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, y en particular sus artículos 3, 4, 5 y 11, se opone a la aplicación de una disposición de Derecho nacional basada en el artículo 8 de la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004 , relativa al respeto de los derechos de propiedad intelectual, que permite que, a efectos de identificación de un abonado, se requiera en un procedimiento civil a un proveedor de acceso a internet para que facilite al titular de un derecho de autor o a su representante información relativa al abonado al que dicho proveedor de acceso asignó una dirección IP concreta, supuestamente utilizada para infringir dicho derecho? La cuestión presupone que el demandante ha aportado la prueba de la infracción de un determinado derecho de autor y que la medida es proporcionada.

2) ¿Influye en la respuesta a la primera cuestión el hecho de que el Estado miembro no haya adaptado su Derecho interno a las disposiciones de la Directiva 2006/24 pese a haber vencido el plazo establecido a tal efecto?".

[501] Cf. Petición de decisión prejudicial planteada por el Verwaltungsgericht Wiesbaden (Alemania) el 6 de marzo de 2009 — Volker y Markus Schecke GbR/Land Hessen, interviniente: Bundesanstalt für

Landwirtschaft und Ernährung (C-92/09). En el Asunto C-92/09, el Verwaltungsgericht Wiesbaden (Alemania) el 6 de marzo de 2009, con ocasión del caso en que son partes en el procedimiento principal como demandantes Volker y Markus Schecke GbR, demandada, e interviniente Bundesanstalt für Landwirtschaft und Ernährung Land Hessen, ha planteado con fecha de 6 de marzo de 2009 las siguientes cuestiones prejudiciales:

"1) ¿Son inválidos los artículos 42, párrafo primero, número 8 ter), y 44 bis del Reglamento (CE) no 1290/2005 del Consejo, de 21 de junio de 2005, sobre la financiación de la política agrícola común (DO L 209, de 11.8.2005, p. 1), añadidos por el Reglamento (CE) no 1437/2007 del Consejo, de 26 de noviembre de 2007, que modifica el Reglamento (CE) no 1290/2005 sobre la financiación de la política agrícola común (DO L 322, de 7.12.2007, p. 1)?

2) ¿El Reglamento (CE) no 259/2008 de la Comisión, de 18 de marzo de 2008, por el que se establecen disposiciones de aplicación del Reglamento (CE) no 1290/2005 del Consejo en lo que se refiere a la publicación de información sobre los beneficiarios de importes a cargo del Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (Feader) (DO L 76, de 19.3.2008, p. 28),

a) es inválido

b) o únicamente válido por ser inválida la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105, de 13.4.2006, p. 54)?

En caso de ser válidas las disposiciones indicadas en la cuestión primera y segunda:

3) ¿El artículo 18, apartado 2, segundo guión, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, de 23.11.1995, p. 31), debe ser interpretado en el sentido de que la publicación con arreglo al Reglamento (CE) no 259/2008 de la Comisión, de 18 de marzo de 2008, por el que se establecen disposiciones de aplicación del Reglamento (CE) no 1290/2005 del Consejo en lo que se refiere a la publicación de información sobre los beneficiarios de importes a cargo del Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (Feader), solamente puede efectuarse cuando se haya seguido el procedimiento, previsto en ese artículo, que sustituye a la notificación a la autoridad de control?

4) ¿El artículo 20 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, de 23.11.1995, p. 31), debe ser interpretado en el sentido de que la publicación con arreglo al Reglamento (CE) no 259/2008 de la Comisión, de 18 de marzo de 2008, por el que se establecen disposiciones de aplicación del Reglamento (CE) no 1290/2005 del Consejo en lo que se refiere a la publicación de información sobre los beneficiarios de importes a cargo del Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo

plantea abiertamente la legalidad de la Directiva—. Ambas cuestiones aún están pendientes de resolución.

Finalmente, como anunciamos, está previsto que el Tribunal de Justicia se pronuncie en 2014 sobre la compatibilidad de la DCD con los derechos fundamentales. El caso tiene su origen en dos cuestiones judiciales elevadas respectivamente por Austria (C-594/12 Seitlinger and Others) e Irlanda (C-293/12 Digital Rights Ireland). Una audiencia preliminar tuvo lugar el pasado 9 de julio de 2013, en el que las partes respondieron oralmente las preguntas que el Tribunal les había facilitado previamente por escrito, y que giran todas en torno a los arts. 7, 8 y 11 de la Carta de Derechos Fundamentales[502]. Buena parte de estas cuestiones son estudiadas en la Segunda Parte de esta Tesis.

Rural (Feader), solamente puede efectuarse cuando se haya realizado el control previo previsto por el Derecho nacional para este supuesto?

5) En caso de respuesta afirmativa a la cuarta pregunta: ¿El artículo 20 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, de 23.11.1995, p. 31), debe ser interpretado en el sentido de que no existe un control previo efectivo si se ha efectuado basándose en un registro conforme al artículo 18, apartado 2, segundo guión, de esa Directiva, que omite información preceptiva?

6) ¿El artículo 7, y aquí especialmente la letra e), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, de 23.11.1995, p. 31), debe ser interpretado en el sentido de que se opone a la práctica de almacenar las direcciones IP de los usuarios de una página web sin su expreso consentimiento?".

[502] El cuestionario, tal como fue publicado por el Grupo EDRI (www.edri.org) es el siguiente:

"Section II 1 The parties are invited to comment at the hearing as to whether the area covered by the Directive 2006/24 data retention can serve the purpose of detection and prosecution of serious crime. You will be asked in this context to an explanation of the impact it has that many options for anonymous use of electronic communications services exist.

2 The parties will be asked to explain at the hearing as to whether and to what extent it is possible, using the information to create personal profiles and use, from which - independent of the question of the legality of such a process - the social and professional environment a person, their habits and activities are described.

3 As is - especially considering the answer to the question II.2 - the interference with the guaranteed under Articles 7 and 8 of the Charter of Fundamental Rights to assess individuals whose data was stored?

En cualquier caso, la incesante actividad jurisdiccional —a nivel comunitario y estatal— originada en torno a la DCD es probablemente la mejor prueba de la existencia de defectos en el texto en vigor. Tal apreciación nos lleva de la mano a la otra nota que predicábamos acerca de la transposición, a saber, su carácter insatisfactorio.

---

4 The parties will be asked in light of the case law of the Court that the European Union legislature is obliged to base its choice on objective criteria to answer the following questions at the hearing:

a. In a What objective criteria the EU legislature based its decision in adopting Directive 2006/24?

b. On what data the legislature was to assess the usefulness of data retention for the detection and prosecution of serious crime?

c. Due to data which the legislature could assume that storage of the data over a period of at least six months is required?

d. Are there any statistics which suggest that the detection and prosecution of serious crime since the adoption of the Directive has improved 2006/24?

5 If a protected by the legal order of the EU fundamental rights and protected by the legal system in general interest objective against each other, is the proportionality requires a restriction of the fundamental right in accordance with the case law of the Court that the requirements for the protection of the law with the relevant target be reconciled. The necessary proper balance must be made before the adoption of the measure in question. Moreover, the exceptions and restrictions must be limited to the protection of personal data to the absolute minimum.

- Taking account of this case law, the parties are asked to answer the following questions at the hearing:

a Has the European Union legislature made before the adoption of Directive 2006/24, a proper balance between the requirements of the protection of fundamental rights and the standing at issue in the present case, the public interest? He has in this context the importance of guaranteed under Articles 7 and 8 of the Charter of Fundamental Rights of fundamental rights and the fact that numerous opportunities for anonymous use of electronic communications services are taken into account?

b. Can be assumed, given the importance of the fundamental rights concerned that the security measures adopted by the data retained in the legislature, necessary and sufficiently precise to prevent any possible abuse? Is it possible in the face of such arrangements that the provider of electronic communications services as defined in Directive 2006/24, the required data storage to other outsourcing service providers in other Member States or in third countries, particularly because of the cost of that storage? What impact does such outsourcing of data storage on the security of data?

c. Can - especially considering the answer to the question to 11.5.3 - be assumed that the legislature has limited the interference with the fundamental rights concerned to the absolute minimum?"

La transposición puede calificarse de *insatisfactoria* en la medida en que, como ha reconocido la propia Comisión, la DCD "no ha armonizado plenamente el enfoque en cuanto a la conservación de datos y no ha creado unas condiciones equitativas para los operadores"[503]. Como ya hemos tenido ocasión de demostrar con detalle en los apartados anteriores, se constata la existencia de considerables diferencias entre las legislaciones nacionales en relevantes aspectos que la DCD pretendía armonizar, principalmente los plazos de conservación y las condiciones de seguridad de los datos. La elaboración de estadísticas sobre la conservación de datos en cada país, fundamentales para evaluar la proporcionalidad de la DCD, ha sido un notorio fiasco dada la escasa implicación de los Estados y las diferencias en su confección.

Lo que sí que ha conseguido la DCD es lo que, a nuestro parecer, era su principal y casi único objetivo: el establecimiento en todos los países de la Unión de la medida de conservación generalizada de datos de las comunicaciones electrónicas con fines penales durante un mínimo de seis meses. Todo ello a riesgo, naturalmente, de que buena parte de estas normativas nacionales puedan presentar serias fallas que pongan en riesgo —cuando no vulneren claramente— los derechos fundamentales. Tal era el caso de la normativa alemana, ya anulada. La propia Comisión ha reconocido que la Directiva no garantiza por sí misma que los datos conservados se almacenen, recuperen y utilicen con pleno respeto del derecho a la intimidad y la protección de los datos personales[504], dado que "la Directiva sólo busca una armonización parcial de los enfoques sobre conservación de datos" y "la responsabilidad de garantizar estos derechos corresponde a los Estados miembros"[505].

En todo caso, los defectos e insuficiencias que hemos puesto de manifiesto a lo largo de este análisis del articulado han abierto nuevas amenazas al mercado único, como el que no se regule el reembolso de los gastos a los operadores o no armonice la tecnología de conservación de datos, cuya elección —nos advierte el considerando vigésimo tercero de la DCD— "es una cuestión que debe resolverse a nivel nacional". Estas concretas omisiones pueden crear obstáculos en el mercado interior de las comunicaciones

---

[503] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 36.

[504] Cf. Informe de evaluación sobre la Directiva…, doc. cit., pp. 36 y 37.

[505] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 37.

electrónicas del mismo modo que las diferencias legales y técnicas que la DCD pretendía eliminar.

A la vista del más grave de estos problemas —el de la protección de la privacidad—, distintos organismos han sugerido en los últimos años diversos aspectos en los que la DCD debe ser mejorada.

En concreto, debe destacarse el Informe del GT29 sobre la segunda medida de ejecución, que alegando que los riesgos de violación de la confidencialidad de las comunicaciones y de la libertad de expresión son inherentes al almacenamiento de los datos de tráfico, criticó también determinados aspectos de la aplicación nacional, en particular el registro de datos, los períodos de conservación, los tipos de datos conservados y las medidas de seguridad adoptadas[506]. El GT29 ya ha puesto en conocimiento de la Comisión casos en que se conservaron detalles del contenido de comunicaciones por internet, fuera del ámbito de aplicación de la Directiva, incluidas direcciones IP y URL de sitios web, encabezamiento de correos electrónicos y listas de destinatarios en copia[507]. En este sentido, el Grupo ha pedido expresamente que se aclare que las categorías son exhaustivas, y que no pueden imponerse a los operadores obligaciones adicionales de conservación de datos[508].

Por su parte, el SEPD ha declarado en relación con la transposición que la DCD "no ha logrado armonizar la legislación nacional" y que el uso de los datos conservados no se limita estrictamente a la lucha contra los delitos graves, lo que le ha llevado a solicitar a las instituciones europeas la adopción de un marco legislativo global que no sólo imponga a los operadores obligaciones de conservar datos, sino que también regule la manera en que los Estados miembros utilizan los datos a efectos de la aplicación de la Ley, al objeto de crear "seguridad jurídica para los ciudadanos" [509].

---

[506] Cf. Report 01/2010 on the second joint…, doc. cit., p. 1.

[507] Cf. Report 01/2010 on the second joint…, doc. cit., p. 6.

[508] Cf. Report 01/2010 on the second joint…, doc. cit., p. 9.

[509] Discurso pronunciado por Peter Hustinx en la conferencia *Taking on the Data Retention Directive*, de 3 de diciembre de 2010. Los *proceedings* del encuentro puede consultarse en http://www.statewatch.org/news/2010/dec/eu-mandatory-data-retention-meeting-note.pdf.

Finalmente, y como era de esperar, el análisis de la Comisión sobre la aplicación de las medidas de conservación de datos ha sido el más optimista. La institución reiteró en su Informe de Evaluación que estamos ante "una herramienta valiosa para los sistemas de justicia penal en la Unión Europea y para la aplicación de la legislación" y que, a su parecer, la mayoría de los Estados miembros consideran que la norma europea sobre conservación de datos siguen siendo necesarias como herramienta para la aplicación de la ley, la protección de las víctimas y los sistemas de justicia penal[510]. Abundando en su conocida argumentación, la institución defiende que los datos conservados proporcionan valiosas pistas y pruebas en la prevención y enjuiciamiento de delitos, así como que "su utilización ha dado lugar a condenas por delitos que, sin la conservación de datos, nunca podrían haberse resuelto" al tiempo que "también a dado lugar a sentencias absolutorias de personas inocentes"[511].

No obstante, la Comisión también ha reconocido que hay ámbitos en los que se ha fracasado o se puede mejorar. En concreto, resulta palmario que la contribución de la DCD a la armonización de la conservación de datos ha sido escasa en lo que se refiere sobre todo a la limitación de la finalidad que justifica el acceso a los datos y a los períodos de conservación. Dadas las implicaciones y riesgos para el derecho a la intimidad y la protección de los datos personales, la Comisión estima que la Unión debe continuar garantizando mediante normas comunes el mantenimiento sistemático de niveles muy elevados respecto del almacenamiento, la recuperación y el uso de datos de tráfico y de localización[512].

A la luz de estas conclusiones, la Comisión ha manifestado su intención de proponer modificaciones a la Directiva sobre la base de otra evaluación de impacto, a realizar en un futuro próximo. De acuerdo con el apartado octavo del Informe, la propuesta de la Comisión sobre la revisión del marco para la conservación de datos se inspirará en una

[510] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 1.

[511] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 27.

[512] Cf. Informe de evaluación sobre la Directiva…, doc. cit., p. 1.

larga serie de recomendaciones, cuyo contenido parafraseamos en los siguientes ordinales[513]:

1. La Unión debe apoyar y regular la conservación de datos como medida de seguridad. En concreto, la armonización de normas en este ámbito ha de garantizar que la conservación de los datos sea una herramienta eficaz en la lucha contra la delincuencia, que la industria tenga una seguridad jurídica en un mercado interior que funcione bien, y que se apliquen de modo coherente en toda la Unión elevados niveles de respeto de la intimidad y protección de los datos personales.

2. Frente a la desigual transposición de la norma, la Comisión pretende seguir colaborando con todos los Estados miembros con el fin de garantizar la aplicación efectiva de la Directiva, así como continuar con su función de velar por la aplicación de la legislación comunitaria, recurriendo en última instancia a los procedimientos de infracción en caso necesario.

3. La Directiva no ha armonizado plenamente el enfoque en cuanto a la conservación de datos y no ha creado unas condiciones equitativas para los operadores, como ya expusimos en los apartados anteriores.

4. Deben reembolsarse sistemáticamente a los operadores los gastos en que incurran. La Comisión Europea ha sido meridianamente clara a este respecto. En sus propias palabras:

> "sigue existiendo una falta de seguridad jurídica para el sector. La obligación de conservar y recuperar datos representa un coste considerable para los operadores, en particular para los más pequeños, y los operadores se ven afectados y son reembolsados en diferentes grados en unos Estados miembros en comparación con otros, si bien no existen pruebas de que el sector de las telecomunicaciones en general se haya visto afectado negativamente como consecuencia de la Directiva. La Comisión estudiará maneras de proporcionar un reembolso homogéneo a los operadores"[514].

---

[513] Cf. Informe de evaluación sobre la Directiva…, doc. cit., pp. 38 y ss., de donde se extraen los siguientes puntos.

[514] Ibíd.

5. Debe garantizarse la proporcionalidad en el proceso integrado de almacenamiento, recuperación y utilización: La Comisión se ha comprometido a velar por que cualquier propuesta futura sobre conservación de datos respete el principio de proporcionalidad y sea adecuada para lograr el objetivo de la lucha contra el terrorismo y los delitos graves y no vaya más allá de lo que sea necesario para lograrlo. Al mismo tiempo, también se reconocerán que las excepciones o limitaciones en lo que respecta a la protección de los datos personales sólo se apliquen en tanto que sean necesarias para la eficacia y eficiencia del sistema de justicia penal. De hecho, en la próxima evaluación de impacto se examinarán por parte de la Comisión los siguientes concretos ámbitos:

- la coherencia entre la limitación de las finalidades de la conservación de datos y los tipos de delitos para los que los datos conservados puedan consultarse y utilizarse;
- una mayor armonización y posible reducción de los períodos obligatorios de conservación de datos;
- un control independiente de las solicitudes de acceso y del régimen general de acceso y de conservación de datos aplicado en todos los Estados miembros;
- la limitación de las autoridades autorizadas para acceder a los datos;
- la reducción de las categorías de datos que deben conservarse;
- la elaboración de orientaciones sobre las medidas de seguridad técnicas y organizativas de acceso a los datos, incluidos los procedimientos de transferencia;
- la elaboración de orientaciones sobre utilización de los datos, incluida la prevención de la búsqueda aleatoria de datos —*data mining*—; y
- el establecimiento de criterios de medida realistas y de procedimientos de notificación para facilitar las comparaciones sobre la aplicación y evaluación del futuro instrumento[515].

[515] La Comisión se ha comprometido a estudiar asimismo si un enfoque europeo sobre la preservación de datos puede complementar la conservación de datos, y de qué manera. Por lo que respecta a la "lista de control" de los derechos fundamentales y el enfoque de la gestión de la información en el espacio de libertad, seguridad y justicia, la Comisión estudiará cada uno de estos ámbitos a la luz de los principios

Finalmente, la Comisión se ha comprometido a proponer una revisión del actual marco de conservación de datos así como una serie de opciones en consulta con los servicios con funciones coercitivas, el poder judicial, la industria y los grupos de consumidores, las autoridades de protección de datos y las organizaciones de la sociedad civil. Finalmente, el órgano ha declarado su voluntad de estudiar "en profundidad" la percepción del público sobre la conservación de datos y su impacto en el comportamiento.

Todas estas conclusiones se incorporarán a una evaluación de impacto de las opciones estratégicas señaladas, que habrá de servir de base para la propuesta de la Comisión.

A pesar de tan buenas intenciones, parece en todo caso evidente que la práctica de la conservación de datos supone en sí misma un riesgo de posibles violaciones de la intimidad, la protección de datos y otros derechos fundamentales, que la DCD ha creado pero no abordado satisfactoriamente. Si bien hasta la fecha no hay resoluciones judiciales que hayan reconocido un caso grave de vulneración de derechos fundamentales a causa de las medidas de la Directiva, las probabilidades de que esto suceda no son escasas, e incluso cabe prever que —a menos que se establezcan nuevas salvaguardias— incrementarán con la evolución de la tecnología y de las formas de comunicaciones, con independencia de si los datos se almacenan bien para fines comerciales o de seguridad, bien dentro o fuera de la Unión Europea.

---

de proporcionalidad y del requisito de previsibilidad. También garantizará la coherencia con la revisión en curso del marco europeo en materia de protección de datos.

SEGUNDA PARTE. DERECHOS FUNDAMENTALES EN LA DIRECTIVA 2006/24/CE, DE 15 DE MARZO DE 2006, SOBRE LA CONSERVACIÓN DE DATOS

Estudiado el contenido objetivo del articulado de la DCD en la Primera Parte de esta Tesis, resta ahora concentrar nuestra atención sobre el modo en que este conjunto regulatorio limita los derechos y libertades reconocidos en el sistema de derechos fundamentales de la Unión Europea, para determinar si tal afectación es o no legítima conforme a dicho sistema[516].

---

[516] Debe advertirse que, al tiempo de redactar estas líneas, aún está pendiente de decisión el asunto C-293/12, por el que la High Court of Ireland (Irlanda), planteó con fecha de 11 de junio de 2012 petición de decisión prejudicial al Tribunal de Justicia sobre la compatibilidad de la DCD con los derechos fundamentales de la CDF. Publicadas en DOUE C-258, de 25 de agosto de 2012, las cuestiones planteadas son textualmente las siguientes:

"1) ¿Es incompatible la restricción de los derechos del demandante en relación con el uso de telefonía móvil derivada de los requisitos establecidos en los artículos 3, 4, y 6 de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, con el artículo 5, apartado 4, TUE, en la medida en que resulta desproporcionada e innecesaria o inadecuada para lograr los objetivos legítimos de: a) garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves?, y/o, b) garantizar el funcionamiento adecuado del mercado interior de la Unión Europea?

2) En particular:

i) ¿Es compatible la Directiva 2006/24/CE con el derecho de los ciudadanos a circular y residir libremente en el territorio de los Estados miembros establecido en el artículo 21 TFUE?

ii) ¿Es compatible la Directiva 2006/24/CE con el derecho al respeto de la vida privada establecido en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH)?

20 El sistema de derechos fundamentales de la Unión Europea

Con la adopción del Tratado de Lisboa en 2009, el lugar de los derechos fundamentales en el ordenamiento europeo ha experimentado una profunda mejora, puesto que, desde entonces, la Unión cuenta con una Carta de los Derechos Fundamentales jurídicamente vinculante[517]. Si bien el respeto a los derechos fundamentales ha formado parte del acervo comunitario durante décadas, lo cierto es que los tratados originarios no incluyeron un catálogo de estos derechos, sino que se limitaron a hacer referencia al CEDH o a reconocerlos como principios generales del Derecho comunitario, resultantes de las tradiciones constitucionales comunes de los Estados miembros.

El vigente art. 6.1 TUE dispone ahora que la Unión reconoce los derechos, libertades y principios enunciados en "la Carta de los Derechos Fundamentales de la Unión Europea […], la cual tendrá el mismo valor jurídico que los Tratados", mientras que el art. 6.2 establece la adhesión de la Unión al Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales. Finalmente, el art. 6.3 advierte que los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros "formarán parte del

---

iii) ¿Es compatible la Directiva 2006/24/CE con el derecho a la protección de los datos de carácter personal establecido en el artículo 8 de la Carta?

iv) ¿Es compatible la Directiva 2006/24/CE con el derecho a la libertad de expresión establecido en el artículo 11 de la Carta y en el artículo 10 CEDH?

v) ¿Es compatible la Directiva 2006/24/CE con el derecho a una buena administración previsto en el artículo 41 de la Carta?

3) ¿En qué medida exigen los Tratados, y en particular el principio de cooperación leal establecido en el artículo 4, apartado 3, del Tratado de la Unión Europea, a los órganos jurisdiccionales nacionales indagar y evaluar la compatibilidad de las medidas nacionales de transposición de la Directiva 2006/24/CE con respecto a las garantías que otorga la Carta de los Derechos Fundamentales, incluido su artículo 7 (en relación con el artículo 8 CEDH)?".

[517] La Carta entró en vigor con la adopción del Tratado de Lisboa el 1 de diciembre de 2009. La redacción del artículo 6.1 TUE que citamos es la dada por éste.

Derecho de la Unión como principios generales"[518]. Otros muchos artículos del Derecho primario contienen normas que desarrollan o especifican estas previsiones[519].

De esta manera, la CDF ha pasado en la actualidad a formar parte del denominado Derecho primario de la Unión Europea, y en consecuencia, cualquier norma o acto perteneciente al Derecho secundario —entre ellas, las directivas— deben ser conformes al contenido de la Carta[520] so pena de su nulidad[521]. La legalidad de la DCD queda de

---

[518] En su anterior versión, el artículo 6.2 TUE establecía que la Unión debía respetar los derechos fundamentales tal y como se garantizaban en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

[519] El art. 7 TUE recupera una disposición, ya existente en el marco del anterior Tratado de Niza, que instaura un mecanismo de prevención ante la existencia de "un riesgo claro de violación grave" por parte de un Estado miembro de los valores contemplados en el art. 2 TUE, así como un mecanismo de sanción en caso de que se constate "una violación grave y persistente" por parte de un Estado miembro de esos valores. El Parlamento Europeo cuenta a la vez con un derecho de iniciativa que permite poner en marcha estos mecanismos y con un derecho de control democrático, ya que debe dar su aprobación a la ejecución de los mismos. También encontramos una referencia a los derechos humanos y las libertades fundamentales en las disposiciones relativas a la acción exterior de la Unión (art. 21 TUE). El art. 67 Tratado de Funcionamiento de la Unión Europea (TFUE) dispone que «la Unión constituye un espacio de libertad, seguridad y justicia dentro del respeto de los derechos fundamentales y de los distintos sistemas y tradiciones jurídicos de los Estados miembros». Disposiciones específicas del Tratado consagran determinados derechos. Es el caso, en particular, del art. 8 TFUE, relativo a la igualdad entre el hombre y la mujer, y del artículo 10, relativo a la lucha contra la discriminación.
El art. 15 TFUE, que recupera una disposición del anterior Tratado de Niza, establece que toda persona física o jurídica de un Estado miembro tendrá derecho a acceder a los documentos de las instituciones, órganos y organismos de la Unión. Lo mismo ocurre con el artículo 16, relativo al derecho a la protección de los datos de carácter personal.

[520] Cf., a este respecto, los casos C-188/10 y C-189/10, 2010 ECJ (sobre la vigencia de la CDF en el Derecho primario y los derechos que consagra). Cf. también los art. 263 TFUE ("el Tribunal de Justicia de la Unión Europea será competente para pronunciarse sobre los recursos por incompetencia, vicios sustanciales de forma, violación de los Tratados o de cualquier norma jurídica relativa a su ejecución, o desviación de poder, interpuestos por un Estado miembro, el Parlamento Europeo, el Consejo o la Comisión") y art. 267 TFUE ("El Tribunal de Justicia de la Unión Europea será competente para pronunciarse, con carácter prejudicial: a) sobre la interpretación de los Tratados; b) sobre la validez e interpretación de los actos adoptados por las instituciones, órganos u organismos de la Unión").

[521] Obviamente, no es una novedad que el Derecho secundario de la UE debe ser conforme con el primario y los derechos fundamentales en él contenidos. Cf., vg. caso 11/70, Internationale

esta manera condicionada a que sus previsiones sean compatibles con aquel texto fundamental.

El Tribunal de Justicia de la Unión Europea y su jurisprudencia tiene un papel relevante a este respecto, pues es su misión examinar la compatibilidad de la legislación adoptada por la UE con los derechos fundamentales y la de las medidas adoptadas a escala nacional por los Estados miembros en aplicación o en el marco del Derecho de la Unión[522].

Volviendo al contenido de la CDF, baste recordar aquí que el documento enuncia los derechos clasificándolos en tres categorías:

— *derechos civiles*: derechos humanos y derecho a la justicia tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales adoptado por el Consejo de Europa;

— *derechos políticos* propios de la ciudadanía europea creada por los Tratados;

— *derechos económicos y sociales*, que comprenden los derechos establecidos en la *Carta comunitaria de los derechos sociales fundamentales de los trabajadores*, adoptada el 9 de diciembre de 1989 en la cumbre de Estrasburgo por los Jefes de Estado o de Gobierno de once Estados miembros en forma de declaración.

Estos derechos, obviamente, no son nuevos: la Carta refunde en un mismo documento los derechos fundamentales reconocidos por los Tratados de la Unión, los principios constitucionales comunes de los Estados miembros, el CEDH y las Cartas Sociales de la UE y del Consejo de Europa. Además, al reunir en un mismo texto todos los derechos de las personas, la CDF aplica el principio de "indivisibilidad" de los derechos fundamentales al acabar con la diferenciación que los textos europeos e internacionales habían mantenido hasta entonces entre derechos civiles y políticos, por

---

Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, 1970 E.C.R. 1125, § 4.

[522] La jurisprudencia del TJUE se ha desarrollado fundamentalmente en el marco de las decisiones con carácter prejudicial, reguladas ahora en el art. 267 TFUE.

un lado, y económicos y sociales, por otro, y agrupa todos los derechos con arreglo a determinados principios básicos: la dignidad humana, las libertades fundamentales, la igualdad entre las personas, la solidaridad, la ciudadanía y la justicia. Además, según el principio de universalidad, casi todos los derechos recogidos en la Carta se aplican a todas las personas, con independencia de su nacionalidad o su lugar de residencia[523], si bien ha de tenerse en cuenta que el texto pretende proteger los derechos fundamentales de las personas frente a acciones emprendidas por las instituciones de la UE y por los Estados miembros en aplicación de los Tratados de la Unión.

En cuanto a la adhesión de la UE al CEDH[524], debe recordarse que este Convenio, adoptado en el marco del Consejo de Europa en 1950 y modificado por varios protocolos, ha constituido un texto esencial en materia de derechos fundamentales, junto con la importante labor interpretativa del Tribunal Europeo de Derechos Humanos. Hasta ahora, la UE —como tal— no es parte del Convenio, a diferencia de todos sus Estados miembros, que sí lo son. La adhesión de la UE está prevista por el art. 6.2 TUE tendrá como consecuencia el sometimiento de la UE —como ocurre actualmente con sus Estados miembros—, en materia de respeto de los derechos fundamentales, al control de una jurisdicción ajena a la Unión, especializada en materia de protección de los derechos fundamentales[525]. En particular, esta adhesión permitirá a los ciudadanos europeos —pero también a los ciudadanos de terceros países presentes en el territorio de la Unión—, recurrir directamente ante este Tribunal, basándose en las disposiciones del CEDH, los actos jurídicos adoptados por la UE en las mismas

[523] No obstante, los derechos vinculados directamente con la ciudadanía de la Unión se otorgan solo a los ciudadanos (por ejemplo, el derecho a participar en las elecciones al Parlamento Europeo o en las elecciones municipales), y algunos derechos se limitan a determinadas categorías de personas (por ejemplo, los derechos de los niños y algunos derechos sociales de los trabajadores).

[524] El Convenio se divide en dos partes: una primera relativa a los derechos y libertades, que comprende 17 artículos, y una segunda parte que describe las modalidades de funcionamiento y las competencias del TEDH.

[525] Recientemente se ha publicado una completa monografía sobre este difícil aspecto: Gragl, P., The Accession of the European Union to the European Convention on Human Rights, Hart Publishing, Londres, 2013.

condiciones que los actos jurídicos de sus Estados miembros[526]. En relación con los derechos que son también garantizados por el CEDH, el art. 52.3 CDF establece que "en la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio". En este sentido, es relevante destacar que el CEDH constituye un mero mínimo nivel de protección respecto del provisto por la Carta[527].

Para finalizar esta brevísima introducción, ha de tenerse asimismo presente que el Preámbulo de la CDF indica el modo de interpretar sus previsiones. Así, afirma que la CDF:

> "reafirma, respetando las competencias y misiones de la Comunidad y de la Unión, así como el principio de subsidiariedad, los derechos reconocidos especialmente por las tradiciones constitucionales y las obligaciones internacionales comunes de los Estados miembros, el Tratado de la Unión Europea y los Tratados comunitarios, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, las Cartas Sociales adoptadas por la Comunidad y por el Consejo de Europa, así como por la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas y del Tribunal Europeo de Derechos Humanos".

21 Derechos fundamentales limitados por DCD

Explicado sucintamente el marco de derechos y libertades que nos ha de servir de parámetro para nuestro análisi, no es necesario profundizar mucho en el contenido de la

---

[526] Esta adhesión plantea varios problemas, especialmente en el ámbito jurídico e institucional (por ejemplo, el nombramiento de un juez procedente de la UE en el seno del Tribunal, las relaciones entre el Tribunal de Justicia de la UE y el Tribunal de Estrasburgo o la aplicación del mecanismo de «codemandado», que llegado el caso permite a la UE personarse en los procesos que afectan a uno de sus Estados miembros). Actualmente, la Unión Europea y el Consejo de Europa mantienen negociaciones a este respecto.

[527] Cf. art. 52.3 *in fine*: "Esta disposición no impide que el Derecho de la Unión conceda una protección más extensa". Al respecto, cf. también *Explicaciones sobre la Carta de los Derechos Fundamentales* (2007/C 303/02).

DCD para constatar que las medidas que prevee suponen una limitación de ciertos ámbitos de libertad ciudadana.

Prima facie, la consecuencia más importante de la aprobación de la DCD es la adopción en todos los Estados miembros de medidas de conservación de datos con fines penales.

La existencia de esta afectación no ha sido nunca objeto de polémica. La propia Comisión Europea así lo reconoció cuando, al presentar la Propuesta de Directiva, advirtió que "aunque esta[ba] claro que la Directiva propuesta surtir[í]a un efecto en el derecho al respeto a la intimidad de los ciudadanos garantizado por el artículo 7 de la Carta [de Derechos Fundamentales], al igual que en el derecho a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta, la interferencia con estos derechos se justifica[ba] según el artículo 52 de la Carta"[528]. A renglón seguido, como era de esperar, la Comisión aseveró que las limitaciones de estos derechos eran "proporcionadas" y "necesarias" para alcanzar "los objetivos generalmente reconocidos de prevenir y combatir la delincuencia y el terrorismo"[529]. Además, la institución advertía que la DCD *limitaba* sus efectos en la vida privada de los ciudadanos, en primer lugar, estableciendo claramente el propósito para el cual los datos conservados pueden utilizarse, y, en segundo, limitando las categorías de datos objeto de conservación y el período de ésta[530].

Frente a la postura de la Comisión, ha de recordarse, sin embargo, que la mayoría de las instituciones que emitieron dictamen durante la tramitación de la DCD no se mostraron de acuerdo con esta valoración tan positiva. De entre ellas, se han de destacar la

---

[528] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 3.

[529] Ibíd.

[530] Ibíd. Otra salvaguardia importante era —a su entender— el que la DCD no fuera aplicable al contenido de las comunicaciones —cosa que equivaldría a la interceptación de las telecomunicaciones—, que queda fuera del ámbito de este instrumento jurídico.

opinión del CESE así como la del SEPD. Este último, siendo la máxima autoridad europea en la protección del derecho fundamental a la protección de datos, merece obviamente especial atención en sus dictámenes sobre la materia. Expondremos a continuación las opiniones de estas instituciones antes de desarrollar en los apartados siguientes nuestro propio análisis.

En cuanto al CESE, su informe empezaba manifestando que resultaba "difícil de comprender" el tratamiento dado en la norma propuesta a los derechos fundamentales, especialmente al derecho a la intimidad[531]. A su entender, la Comisión había utilizado en su ponderación de derechos dos parámetros de legalidad inaceptables. Por un lado, se había utilizado expresamente una interpretación *ex novo* e "inadecuada" del *Pacto Internacional de Derechos Civiles y Políticos* —artículos 4 y 12— y del CEDH —artículos 9.10 y 11—, al margen de la abundante y exhaustiva interpretación de estos preceptos por los órganos y jurisdicciones competentes[532]. Por otro, el test de legalidad se había hecho depender de las disposiciones la CDF, un instrumento normativo que, "aún gozando del máximo consenso europeo, no est[aba] aún en vigor y no p[odía] ser invocado por los justiciables con garantías de justiciabilidad"[533]. Es evidente que este último argumento ha perdido su fuerza en tanto que, con la adopción del Tratado de Lisboa el 1 de diciembre de 2009, la Carta de Derechos Fundamentales ya ha entrado en vigor y, de acuerdo con lo establecido por el art. 6.1 TUE, dispone ahora del mismo valor jurídico que los Tratados.

Más allá de estas observaciones, el dictamen del CESE incrementaba el tono de su crítica en el punto siguiente al advertir que "incomprensiblemente", la endeblez de dicho test cobraba "dimensiones más criticables" cuando se observaba que la Comisión sólo había tomado en consideración los artículos 7 —respeto de la vida privada y familiar[534]— y 8 —protección de datos de carácter personal[535]— de la Carta, con

---

[531] Cf. Dictamen del CESE…, doc. cit., punto 2.3.4.

[532] Cf. Dictamen del CESE…, doc. cit., punto 2.3.5.

[533] Cf. Dictamen del CESE…, doc. cit., punto 2.3.6.

[534] El art. 7 CDF —*Respeto de la vida privada y familiar*— dispone que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicación".

[535] Conforme al art. 8 CDF —*Protección de datos de carácter personal*—, "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

olvido de otros preceptos, como son los artículos 36 —acceso a los servicios de interés general[536]—, 38 —protección de los consumidores[537]—, 47 —derecho a la tutela judicial efectiva[538]— o 48 —presunción de inocencia[539]—. Así pues, la conclusión del CESE no era otra sino que la Comisión debía "reflexionar" y "actuar de forma más meticulosa y con escrupuloso respeto a los derechos fundamentales, para evitar en el futuro que los tribunales constitucionales de los Estados miembros declarasen la inconstitucionalidad de la norma como, final y lamentablemente, ha[bía] sucedido"[540].

En términos similares se expresó el SEPD, que manifestó su preocupación sobre el modo en que la Propuesta de Directiva afectaba claramente a los derechos fundamentales, cuyo respeto sólo podía ser considerado como "esencial"[541]. A su entender, las circunstancias en la sociedad podrían quizás haber cambiado debido a los

---

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

[536] Dispone el art. 36 CDF —*Acceso a los servicios de interés económico general*— que "la Unión reconoce y respeta el acceso a los servicios de interés económico general, tal como disponen las legislaciones y prácticas nacionales, de conformidad con los Tratados, con el fin de promover la cohesión social y territorial de la Unión".

[537] El art. 38 CDF —*Protección de los consumidores*— establece que "en las políticas de la Unión se garantizará un nivel elevado de protección de los consumidores".

[538] Según el art. 47 CDF —*Derecho a la tutela judicial efectiva y a un juez imparcial*—: "Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo.

Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la Ley. Toda persona podrá hacerse aconsejar, defender y representar.

Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia".

[539] El art. 48 CDF garantiza la *presunción de inocencia* y los *derechos de la defensa* en los siguientes términos: "1. Todo acusado se presume inocente mientras su culpabilidad no haya sido declarada legalmente.

2. Se garantiza a todo acusado el respeto de los derechos de la defensa".

[540] Cf. Dictamen del CESE…, doc. cit., puntos 2.3.7 y 2.3.8.

[541] Cf. Dictamen del SEPD…, doc. cit., punto 8.

recientes ataques terroristas, pero esto no podía tener como efecto que se comprometieran los estándares elevados de protección en el Estado de Derecho. Dentro de este marco, el SEPD estimaba concretamente que la DCD tenía "un impacto directo" sobre la protección garantizada por el art. 8 CEDH, dado que la obligación de retener datos entraba dentro del ámbito de este artículo, al tiempo que recordaba que las justificaciones para la injerencia debían ser "más importantes que las consecuencias perjudiciales que la existencia misma de las disposiciones legislativas de que se trata pudiera entrañar para las personas"[542]. De este modo, el SEPD entendía como necesaria una "justificación apremiante" que respetase la doctrina de la TEDH, debiendo demostrarse en particular "la necesidad y la proporcionalidad de la obligación de retener datos, en su sentido más extenso"[543]. Como ya subrayamos, dado que el Supervisor es la más alta autoridad ejecutiva europea en materia de protección de datos, su opinión al respecto resulta particularmente relevante.

En virtud de todo lo expuesto, se concluye tanto de las propias declaraciones del autor de la norma —la Comisión Europea— como de sus dictaminantes más acreditados, que existe un acuerdo general en cuanto a que buena parte de las medidas contenidas en la DCD suponen una relevante limitación de ciertos derechos fundamentales, punto que damos, en consecuencia, por demostrado. Cuestión distinta —y mucho más polémica— es cuáles sean los concretos derechos afectados, así como si tal afectación es o no legítima. Abordaremos tales aspectos en los siguientes apartados.

[542] Cf. Dictamen del SEPD…, doc. cit., punto 9. El SEPD citaba al respecto la Sentencia del TEDH de 22 de octubre de 1981, Duden, A45, Demanda no 7525/76.

[543] Cf. Dictamen del SEPD…, doc. cit., punto 12.

21.1 Impacto de la Directiva en el derecho a la intimidad

Tanto la intimidad[544] como el secreto de las comunicaciones se garantizan como derechos fundamentales en todas las constituciones contemporáneas y en un buen número de convenios internacionales, tales como la Declaración Universal de Derechos Humanos[545] o el Pacto Internacional de Derechos Civiles y Políticos[546]. La inviolabilidad de la intimidad y de la correspondencia y de las demás formas de comunicación se protegen tanto en la CDF como en el CEDH. Así, el art. 7 CDF —bajo la rúbrica de *Respeto de la vida privada y familiar*— ha dispuesto que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. Por su parte, el art. 8 CEDH declara en términos más detallados que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia, sin que sea admisible la injerencia de la autoridad pública en el ejercicio de ese derecho, salvo cuando esa injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria, entre otras cosas, para la seguridad nacional o la seguridad pública, la prevención de desórdenes o delitos, o la protección de los derechos y las libertades de terceros[547]. De este modo,

---

[544] Traducimos aquí por "intimidad" el término legal inglés "privacy", que es el empleado por la versión en que se redactó la CDF.

[545] Dispone su art. 12 que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias y ataques".

[546] Conforme al art. 17 del Pacto, "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y su reputación. 2. Toda persona tiene derecho a la protección de la Ley contra tales injerencias y ataques".

[547] El tenor literal del precepto reza así:

Artículo 8. *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, 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.

como ha señalado el TEDH[548], en el estado actual del orden público europeo que instauran estos textos, y de las tradiciones constitucionales de los Estados miembros, el derecho a la privacidad no se configura solamente desde un aspecto pasivo, sino también, y con menor intensidad, en el aspecto activo; es decir, los particulares —sean o no ciudadanos de la Unión Europea— tienen el derecho a saber quién interfiere sus comunicaciones, por qué razones y con qué frecuencia, así como acceder a cualquier base de datos, pública o privada, donde figuren este tipo de actuaciones.

Aplicando estos principios a la DCD, el hecho de que la medida de conservación de datos impuesta por la norma constituye una limitación específicamente del derecho a la intimidad y al secreto de las comunicaciones ha sido reconocido por la propia Comisión Europea, tanto en el Preámbulo de la DCD como en el Informe de Evaluación[549], al tiempo que había sido subrayado por diversos órganos dictaminantes, en los términos ya expuestos en el apartado anterior. A este respecto, ha de señalarse también que, ya desde desde 1997, la Conferencia de las Autoridades Europeas de Protección de Datos[550] y el GT29[551] habían cuestionado clara y firmemente en varias ocasiones la

---

[548] Cf. Sentencias del TEDH recaídas en los asuntos Amann (2000), Kopp (1998), Halford (1997), y Malone (1984).

[549] Cf. Considerando 9, DCD, e Informe de evaluación sobre la Directiva…, doc. cit., puntos 7.1 y 7.2.

[550] Cf. Declaraciones adoptadas en Estocolmo (abril de 2000) y Cardiff (abril de 2002).

[551] Cf., vg., su Dictamen 9/2004, sobre un proyecto de Decisión marco; el Dictamen 1/2003, sobre el almacenamiento de los datos sobre tráfico a efectos de facturación; Dictamen 5/2002, sobre la declaración de los Comisarios europeos de protección de datos en la Conferencia Internacional de Cardiff (9-11 de septiembre de 2002) sobre la conservación sistemática obligatoria de los datos de tráfico de las telecomunicaciones; el Dictamen 10/2001, sobre la necesidad de un enfoque equilibrado en la lucha contra el terrorismo; Dictamen 4/2001, sobre el proyecto de convención del Consejo de Europa sobre la delincuencia cibernética; Dictamen 7/2000, sobre la propuesta de la Comisión Europea de Directiva 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, de 12 de julio de 2000. En la misma línea, también son dignas de reseña la Recomendación 3/99, sobre la conservación de los datos sobre tráfico por los proveedores de servicios de internet a efectos de cumplimiento de la legislación; la Recomendación 2/99, sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones; o, finalmente, la Recomendación 3/97 sobre el anonimato en internet. Todos los documentos que acabamos de citar están disponibles en http://europa.eu.int/comm/internal_market/privacy.

necesidad de establecer medidas generales de conservación de datos de las telecomunicaciones. En opinión de este último, la DCD obligaba a analizar la circunstancia de que una obligación tan general de conservación de datos afectase a determinadas comunicaciones que susciten cuestiones delicadas en relación a ciertas categorías de secreto profesional y de investigación, o a ciertas actividades de instituciones particulares, específicamente protegidas por ley[552].

En la misma línea argumentativa abundó la muy negativa opinión del CESE en su dictamen a la DCD, en que el órgano remarcaba que el proyecto "afectaba a derechos fundamentales, en concreto al artículo 8 del CEDH", y podía causar en consecuencia un *considerable impacto* en las libertades públicas y los derechos fundamentales[553].

Ciertamente, la DCD tiene un impacto directo sobre la protección garantizada por el artículo 8 CEDH si se contempla desde la jurisprudencia del TEDH, que ha considerado que el almacenamiento de información sobre un individuo es una injerencia en la vida privada, incluso aunque no contuviera ningún dato sensible[554].

En lo específicamente referido al secreto de las comunicaciones el art. 8.1 CEDH reconoce —como ya hemos indicado— el derecho de toda persona al respeto de su *correspondencia*, expresión que comprende la generalidad de sus comunicaciones. Más concretamente, para delimitar el objeto del derecho resulta obligado tomar como punto de partida la citadísima sentencia del TEDH en el caso Malone contra Reino Unido, de 2 de agosto de 1984, según la cual el concepto del secreto de la comunicación no sólo cubre su contenido sino que alcanza a todos los aspectos de la misma, como por ejemplo, la propia existencia de la comunicación, la identidad subjetiva de los interlocutores, así como la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino; y ello con independencia del

---

[552] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 6.

[553] Cf. Dictamen del CESE…, doc. cit., punto 2.4.5.

[554] Cf. Sentencia del TEDH de 16 de febrero de 2000, Amann, 2000-II (demanda nº 27798/95). Lo mismo se aplica a la práctica de la "medición" de llamadas telefónicas, que implica el uso de un dispositivo que registra automáticamente los números marcados en un teléfono y el tiempo y la duración de cada llamada. Cf. Sentencia del TEDH de 2 de agosto de 1984, Malone, A82 (demanda nº 8691/79). Véase también Dictamen del SEPD…, doc. cit., punto 10.

carácter público o privado de la red de transmisión de la comunicación y del medio de transmisión —eléctrico, electromagnético u óptico, etc.— de la misma. Así, y dado que el bien protegido es la libertad de las comunicaciones, la jurisprudencia del TEDH reconoce expresamente la posibilidad de que el art. 8 CEDH pueda resultar violado por el empleo de un artificio técnico que permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma[555].

Si bien en una sociedad democrática, cualquier interferencia con este derecho fundamental puede justificarse si es necesaria en interés de la seguridad nacional —alcanzando incluso la vigilancia y registro de todos los contactos y relaciones de los individuos y de los lugares donde se producen y de los medios utilizados para tales fines—, el TEDH también ha subrayado que la vigilancia secreta plantea el peligro de socavar o incluso destruir la democracia con el pretexto de defenderla[556]. Además, debe tenerse en cuante la doctrina del Tribunal conforme a la cual los Estados no pueden, en nombre de la lucha contra el espionaje y el terrorismo, adoptar cualesquiera medidas que consideren apropiadas, sino que debe alcanzarse un "equilibrio proporcionado" para garantizar que no se socavase la sociedad que se estaba intentando proteger[557]. Este equilibrio es especialmente necesario cuando se trata de forzar a los prestadores de servicios de comunicaciones a que almacenen datos que ellos mismos no necesitan: "de esta manera, podría llegarse a un control continuo, generalizado y sin precedentes de todos los tipos de comunicación y movimiento de todos los ciudadanos en su vida diaria. Se almacenaría una enorme cantidad de información que sólo sería útil a efectos de investigación en un número limitado de casos"[558].

En conclusión, el hecho de que la medida de conservación de datos de las comunicaciones impuesta por la DCD supone una limitación del derecho a la *privacy* —art. 7 CDF— de los ciudadanos europeos queda suficientemente demostrada en virtud de estos argumentos.

---

[555] Cf. Sentencia del TEDH de 2 de agosto de 1984, Malone, A82 (demanda nº 8691/79).

[556] Ibíd.

[557] Cf. Sentencia Klass y otros c. Alemania, apartado. 49.

[558] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 6.

21.2 Impacto de la Directiva en el derecho a la protección de datos personales

La DCD supone una incisiva afectación del derecho fundamental a la protección de datos personales, un grupo de garantías protectoras de la intimidad recogidas ahora en la Carta de los Derechos Fundamentales y, con anterioridad, en el *Convenio nº 108 del Consejo de Europa para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal*. Respecto de la Carta, su art. 8 establece que:

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
>
> 3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

En cuanto al citado Convenio —del que la Unión Europea no es parte pero sí sus Estados miembros—, hay que advertir que, de hecho, el mismo sirvió como principal punto de referencia para la directiva de protección de datos[559]. Asimismo, el artículo 16 TFUE[560] consagra también el derecho de toda persona a "la protección de los datos de carácter personal que le conciernan".

Con la pretensión de respetar debidamente el derecho en cuestión, la DCD ha tomado como punto de partida la regulación introducida por la Directiva 95/46/CE, que exige que los Estados miembros protejan los derechos y libertades de las personas físicas en lo que se refiere al tratamiento de datos personales y, en particular, su derecho a la intimidad, para asegurar el libre flujo de datos personales en la Unión Europea. Como ya vimos, dicha protección reviste especiales caracteres en el sector de las telecomunicaciones, como consecuencia de la generalización de las comunicaciones

---

[559] Así se afirma en BIGNAMI en, Bignami, F., Privacy and Law Enforcement…, op. cit., p. 242.

[560] Publicado en DO C 83 de 30.3.2010, p. 1.

electrónicas, lo que ha supuesto la disponibilidad de un importante caudal de datos personales por parte de los proveedores de redes y servicios, con riesgo para el denominado derecho de autodeterminación informativa, tal y como se viene configurando desde el citado Convenio 108. A mayor abundamiento, el Derecho comunitario ha tratado de mitigar esos riesgos mediante la adopción de instrumentos armonizadores, como la *Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones*, derogada y sustituida por la vigente *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*, que vino a traducir los principios establecidos en la Directiva 95/46/CE en normas específicas para el sector de las comunicaciones electrónicas. Del contenido y relevancia de todas estas disposiciones nos ocupamos al principio de esta Tesis.

Así pues, las disposiciones de la DCD pretendieron aparentemente enmarcarse en esta sólida red de garantías legales que ha rodeado el derecho a la protección de datos, si bien a la postre la Directiva sigue teniendo —en palabras del SEPD— un "impacto enorme" sobre estos principios reconocidos por el Derecho comunitario[561]. Veamos en qué consiste este impacto.

En primer lugar, la DCD introduce una obligación general e inexcusable para todos los operadores de retener los datos durante al menos seis meses, un plazo mucho más largo que los plazos que son habituales para la retención por los proveedores de servicios de las comunicaciones electrónicas públicamente disponibles o por una red de comunicaciones públicas. La ya citada Directiva 2002/58/CE, en su artículo 6, estableció —y así lo sigue haciendo— que los datos sólo pueden recogerse y almacenarse por motivos relacionados directamente con la propia comunicación, incluso a efectos de facturación. Finalizadas estas funciones, los datos deben borrarse.

[561] Cf. Dictamen del SEPD…, doc. cit., punto 11.

Por el contrario, el punto de partida de la DCD es el diametralmente opuesto, al hacer obligatoria la retención por un largo período de hasta veinticuatro meses[562].

En segundo lugar, mientras la Directiva 2002/58/CE garantiza la seguridad y la confidencialidad, la introducción por la DCD de la obligación general de retener datos se traduce en la creación de bases de datos con respectos a todas y cada una de las comunicaciones de todos y cada uno de los ciudadanos, lo que implica crear un potencial riesgo de violación del derecho fundamental para los titulares de esos datos. Baste pensar en el eventual uso comercial de los mismos, o para operaciones de búsqueda aleatoria por parte de las autoridades policiales y aduaneras o de los servicios de seguridad nacional. Tal normativa corre el riesgo de facilitar las denominadas "fishing expeditions", esto es, investigaciones policiales completamente aleatorias en las que los investigadores revisan correspondencia, documentación, registros y cualesquiera enseres personales sin tener claro el tipo de prueba que buscan o el crimen que persiguen. Como ha indicado BIGNAMI, estas "fishing expeditions" constituyen una de modalidades de intrusión más "opresivas" y "detestables" que el poder público puede efectuar en la vida de los ciudadanos:

> "the vast quantity of data generated in today's electronic world—combined with the technology available to process that data—increases exponentially the risk of legitimate police searches degenerating into the aimless perusal of our private lives"[563].

De esta manera, el foco de atención y principal preocupación sobre la limitación por la DCD de este derecho debe centrarse en buena medida en que la disposición no cree lagunas en este campo, prevea estrictas salvaguardias y posea una finalidad cuidadosamente delimitada.

A este respecto, las garantías existentes en el marco jurídico actual sobre protección de datos —las ya mencionadas Directivas 95/46/CE y 2002/58/CE— deberían especificarse por lo que respecta al contexto concreto de los fines policiales de la conservación de datos relativos al tráfico, pues las mismas son vitales para asegurar que no se socave sustancialmente la protección ofrecida por la normativa de protección de

---

[562] Cf. arts. 1.1 y 6 DCD.

[563] Cf. Bignami, F., Privacy and Law Enforcement…, op. cit., p. 235.

datos, en especial el derecho a la confidencialidad del uso de los servicios públicos de comunicación electrónica[564]. Por esta razón, el GT29 concluyó que la Propuesta de Directiva debía prever estas garantías, o bien ser evaluado y adoptado juntamente con otros instrumentos jurídicos adecuados, objetivo que, como veremos, sólo ha sido parcialmente alcanzado[565].

De todo ello queda patente que el art. 8 CDF es el otro derecho fundamental clara y directamente limitado por la regulación introducida por la DCD.

22 Legitimidad del impacto de la normativa de conservación de datos en los derechos fundamentales a la protección de datos y a la intimidad

Demostrada en los términos anteriores la manera en que la obligación de conservación y el deber de cesión de los datos retenidos establecidos por la DCD constituye una limitación del derecho a la intimidad y la protección de los datos personales —que son derechos fundamentales protegidos por la Unión[566]—, resta examinar si tal afectación es o no legítima, esto es, si se produce dentro de los límites autorizados por el Derecho europeo.

Al respecto, la jurisprudencia tanto del TEDH como del TJUE[567] ha especificado en qué casos y bajo que condiciones resulta admisible —a la vista de los tratados vigentes— una injerencia de la autoridad pública en el ejercicio de los derechos fundamentales. En concreto, cualquier limitación debe ser, con arreglo al art. 52.1 CDF, "establecida por la ley y respetar el contenido esencial de dichos derechos y libertades",

---

[564] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 3.

[565] Ibíd.

[566] Como ya hemos indicado, el artículo 7 y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea garantizan el derecho de toda persona a "la protección de los datos de carácter personal que la conciernan".

[567] Cf. Casos C-331/88, Fedesa, 1990 E.C.R. I-4023, § 13; C-133/93, C-300/93, y C-362/93, 1994 E.C.R. I-04863, § 40.

de tal manera que "sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás".

De acuerdo con una conocida e inequívoca jurisprudencia, toda limitación de derechos fundamentales debe cumplir los siguientes requisitos.

En primer lugar, la medida, aun persiguiendo un fin de interés público, debe estar *establecida por la ley* y expresada de una manera precisa, de modo que provea convenientemente contra la acción arbitraria del poder público y dé a conocer a los ciudadanos la posibilidad de injerencias en su esfera de libertades[568].

En segundo lugar, la finalidad de la interferencia debe ser *legítima*, es decir, debe ser necesaria para alcanzar un objetivo de interés general o para proteger los derechos y libertades de otros y estar relacionada con alguna de las categorías reconocidas en el art. 8 CEDH: "que 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".

En tercer lugar, la injerencia en los derechos debe ser *proporcional al objetivo perseguido* para así *respetar el contenido esencial* de los derechos fundamentales en cuestión. La proporcionalidad se concreta a su vez en dos elementos: a) la búsqueda de medios alternativos, menos agresivos, para alcanzar el fin propuesto; y, b) una ponderación de la importancia del derecho en cuestión en comparación con la finalidad pública que se persigue. Si el derecho es suficientemente importante y hay medios alternativos de alcanzar el fin público, no se podrá apreciar la proporcionalidad.

En los siguientes apartados examinaremos pormenorizadamente cada una de estas condiciones, para determinar finalmente si la medida de conservación generalizada de

[568] Cf. art. 52.1 de la Carta así como *Amann v Switzerland*, App No 27798/95, 30 Eur HR Rep 843, 858 ¶ 50 (2000).

datos, introducidad por la DCD cumple o no con todos los requisitos para ser considerada legítima.

23 Previsión legal

El requisito de la previsión legal se desdobla en dos vertientes. Por un lado, la cuestión de la base legal empleada por la Unión para aprobar la norma; por otro, el de la calidad de la norma aprobada.

En cuanto a la base legal para aprobar la DCD, lo cierto es que cualquier norma comunitaria satisface las condiciones establecidas por los arts. 52.1 CDF y 8 CEDH, siempre que fuera precisa y accesible al público. No obstante, como ya se puso de manifiesto anteriormente, buena parte de los debates durante la tramitación de la DCD se centraron en la necesidad de proporcionar una base legal adecuada para la conservación de los datos de tráfico por parte de los proveedores. De otro modo faltaría la norma habilitante de la injerencia en los derechos fundamentales, por lo que tanto los organismos públicos como los agentes privados implicados por la norma estarían violando el art. 52.1 CDF, conforme al cual toda limitación del derecho fundamental debe ser precisa y previsible. Como afirmó el Tribunal de Justicia en el asunto *Österreichischer Rundfunk*, toda injerencia en Derecho con el derecho a la intimidad debe redactarse con "la suficiente precisión para permitir que los destinatarios de la Ley adapten su conducta [a fin de responder] a la exigencia de previsibilidad".

En cuanta a la calidad de la ley, se comprueba que nuestra norma regula con suficiente previsión todos los aspectos relativos a la medida impuesta, al fijar su "objetivo y ámbito" —art. 1 DCD—, las definiciones de los conceptos que emplea —art. 2 DCD—, la propia "obligación de conservar datos" —art. 3 DCD—, el "acceso a los datos" —art. 4 DCD—, las "categorías de datos que deben conservarse" —art. 5 DCD—, los "períodos de conservación" —art. 6 DCD—, la "protección y seguridad de los datos" —art. 7 DCD—, los "requisitos de almacenamiento para los datos conservados" —art. 8 DCD— y otros tantos aspectos de la medida de conservación, en abundancia suficiente para superar el canon de calidad impuesto por la jurisprudencia del TEDH.

Por lo que a nuestra investigación respecta, no cabe sino concluir que la DCD respeta el requisito de la previsión legal. Cualquier interferencia, incluida la retención y uso de los datos de tráfico para ayudar a las investigaciones penales, tenía que ser autorizada por la ley, y así se ha producido.

Por lo tanto, analizado desde ambas vertientes, no cabe sino concluir que las medidas limitadores de derechos introducidas por la DCD cumplen satisfactoriamente con el requisito de previsión legal requerido en el marco de la Unión Europea.

Al margen del análisis de los derechos fundamentales y respecto de la cuestión de la base legal *stricto sensu*, ha de decirse que la base legal contenida en la DCD reemplazaría a las normas nacionales divergentes, al especificar las circunstancias conforme a las cuales los proveedores eran requeridos a conservar los datos con fines de perseguir delitos. Aunque todos los actores implicados en la tramitación de la norma estaban de acuerdo acerca de esto último, discrepaban sin embargo ampliamente sobre si la DCD debería servir como base legal para permitir el acceso policial a los datos conservados, esto es, si la norma debía establecer las condiciones conforme a las cuales la Policía estaría autorizada a solicitar los datos a los proveedores. Tal controversia es la que subyacía a la discusión acerca de si la conservación de datos debía ser considerada una política del Primer Pilar o del Tercero, que ya expusimos en la Primera Parte de esta Tesis. El hecho es que, una vez se optó por el Primer Pilar, la Comisión y el Consejo sostuvieron que, en tal caso, la DCD no podría regular el acceso policial a los datos, ya que todo lo que tuviera que ver con la Policía venía a caer estrictamente en el ámbito del Tercer Pilar. El GT29, el SEPD y Parlamento Europeo sostuvieron lo contrario[569]. Si el asunto era regulado bien por las legislaciones internas, bien de acuerdo con el Tercer Pilar, la competencia de estos órganos supranacionales sería mínima. Finalmente, esta última opción prevaleció —si bien parcialmente— dando lugar al vigente art. 4 DCD, que regula a grandes rasgos el acceso policial a los datos. Si bien la decisión de regular sólo mínimamente las condiciones de acceso de la Policía

[569] El Parlamento, en la línea de los órganos dictaminantes, propuso una serie de enmiendas que recogía buen número de las sugerencias de éstos. Cf. Parliament Legislative Resolution, Eur Parl Doc (P6_TA (2005) 0512) 1 (Dec 14, 2005), disponible en http://www.europarl.europa.eu/sides/getDoc.do?objRefId=105467&language=MT.

representó una victoria para el Consejo, la elección del proceso de co-decisión legislativo para revisar la lista de datos de tráfico representaba otro tanto para el Parlamento.

Relacionado con la elección entre el Primer y el Tercer Pilar se presentaba el debate sobre el proceso institucional apropiado para mantener la DCD actualizada en medio de un entorno tecnológico y social rápidamente cambiante. En la Propuesta de la Comisión, como ya explicamos, la revisión de los tipos de datos de tráfico a retener había de hacerse mediante un procedimiento administrativo, a través de diversos comités, lo que en la práctica significaba una estrecha vigilancia por parte del Consejo sobre las decisiones regulatorias de la Comisión[570]. Los organismos relacionados con la protección de datos y el Parlamento objetaron. En una materia tan incisiva en materia de derechos fundamentales, les parecía mejor un genuino procedimiento legislativo de co-decisión, en el cual el Parlamento Europeo —el único órgano legislativo europeo directamente elegido por la ciudadanía— tendría ocasión de opinar y decidir. De hecho, ésta es la postura que finalmente prevaleció[571].

Algo similar acontecía con las garantías para la privacidad que la Policía tendría que respetar. En opinión del Consejo y de la Comisión, los ministerios de interior de cada país —que forman parte del Consejo—, debían ser los que decidieran su establecimiento. El requisito de la unanimidad, que otorga a cada Estado miembro un derecho de veto, así como el poder de los parlamentos nacionales para supervisar a sus ejecutivos, aseguraría que las decisiones del Consejo respetarían la voluntad del electorado europeo. Por el contrario, el Parlamento Europeo y las autoridades de protección de datos argumentaron que había de ser la cámara, en unión con el Consejo, los que decidieran sobre las garantías para la privacidad a adoptar. De este modo, el Parlamento Europeo, con legitimidad democrática directa, daría lugar a una ley que

[570] Cf. art. 5.6, Propuesta de Directiva.

[571] Cf. Dictamen del SEPD…, doc. cit., punto 60; Dictamen 4/2005, del GT29…, doc. cit., p. 9, o el Informe del Parlamento…, doc. cit., p. 34.

naciera de la deliberación parlamentaria y fuera más respetuosa con los derechos fundamentales[572].

Traemos estas cuestiones al presente apartado ya que —en el fondo— la división entre, por una parte, el Consejo y la Comisión, y por otra, el Parlamento Europeo y las autoridades de protección de datos, no tuvo como hilo conductor la necesidad de aprobar una ley que autorizara la injerencia en el derecho a la intimidad, sino por los diferentes puntos de vista acerca de qué tipo de norma era más legítima desde el punto de vista de la legalidad comunitaria.

En todo caso, como ya hemos dicho, en lo que se refiere al requisito del 52.1 CDF y del art. 8 CEDH, cualquier norma comunitaria o nacional sería satisfactoria en tanto que fuera precisa y accesible al público. El debate, en definitiva, no versaba tanto sobre la legimitad de la afectación en los derechos fundamentales como sobre la naturaleza de la democracia de la Unión Europea[573].

24 Finalidad legítima

Pasando a la siguiente condición, se ha de advertir que una medida que limita un derecho fundamental es *legítima* sólo cuando viene justificada por perseguir una finalidad pública que también lo sea. En otras palabras, para satisfacer las exigencias del art. 52.1 CDF —o del art. 8 CEDH—, la medida objeto de nuestro estudio debe responder "efectivamente a objetivos de interés general reconocidos por la Unión".

A este respecto, hemos de considerar, primeramente, que el art. 1.1 DCD establece como fin del deber de conservación de datos el de su disponibilidad en el contexto de la investigación, detección y enjuiciamiento de delitos graves, entendiendo por éstos los

[572] No obstante, debe tenerse en cuenta que no carecía de peso la opinión de que el Parlamento Europeo está hoy día más alejado de los ciudadanos que los gobiernos nacionales que se sientan en el Consejo y de los Parlamentos nacionales que controlan a sus gobiernos.

[573] Cf. Bignami, F., Privacy and Law Enforcement…, op. cit., p. 244.

que se definan en la legislación nacional de cada Estado miembro[574]. Por su parte, el art. 82 TFUE y siguientes otorgan a la Unión Europea competencias en materia de cooperación judicial en asuntos penales, entre las cuales la investigación, detección y enjuiciamiento de delitos graves del art. 1 DCD cae dentro sin duda de la finalidad pública legítima demandada por el art. 52.1 CDF.

No obstante, hay que decir que, al comienzo del debate legislativo, la finalidad de retener los datos era tremendamente amplia. El primer borrador manejado por el Consejo establecía finalidad combatir la delincuencia en general. Además, los datos conservados no sólo se usarían para investigar y perseguir los crímenes ya cometidos, sino también para *prevenir* los que en el futuro pudieran tener lugar[575]. Posteriormente, en la Propuesta de la Comisión, la finalidad se matizó ligeramente, reduciéndola a la prevención, investigación, detección y enjuiciamiento "de delitos graves, como el terrorismo y la delincuencia organizada"[576]. Como se puede comprobar con la simple lectura del considerando 21, el legislador comunitario partía de la idea de que la respuesta coordinada de los Estados miembros mediante la disponibilidad de los datos almacenados relativos a las comunicaciones electrónicas habría de servir cuando menos para dar respuesta a un denominador común: la persecución del terrorismo y la delincuencia organizada. En este sentido, la DCD fue concebida como una auténtica norma de mínimos, preocupada más por su finalidad armonizadora que por dar una respuesta jurídica única a las posibilidades procesales de la conservación de datos. Pero lo cierto es que la referencia que se hacía al terrorismo y a la delincuencia organizada, auténticos motores de toda la regulación comunitaria, ni siquiera ha quedado reflejada en el articulado de la DCD finalmente en vigor, que opta por la fórmula abierta de la concepción del delito grave según la legislación interna de los Estados miembros[577]. Son por tanto los Estados miembros quienes, con inclusión sin duda de dichas

[574] Cf. art. 1.1 DCD.

[575] La decisión de limitar el uso de los datos de tráfico a delitos graves y de excluir la finalidad preventiva puede atribuirse a la intervención del GT29 y al Parlamento Europeo. Ambos fueron extremadamente críticos con las casi ilimitadas facultades de acceso que tales finalidades conferían a las autoridades judiciales. Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 8; e Informe del Parlamento…, doc. cit., p. 33.

[576] Cf. art. 1.1 Propuesta de Directiva.

[577] Cf. art. 1.1 DCD.

concretas modalidades delictuales —tenidas por el común de las legislaciones internas como infracciones graves— tienen la libertad de decidir qué infracciones criminales pueden verse favorecidas por tan ingente fuente de conocimiento, con respeto —en todo momento y de acuerdo con su marco constitucional— al principio de proporcionalidad.

Sin embargo, debe hacerse notar que el debate durante la tramitación de la norma no se centró en la legitimidad de esta finalidad pues, desde la perspectiva tanto del CEDH como de la CDF, el uso de los datos para combatir cualquier tipo de crimen podría ser considerado legítimo[578]. En consecuencia, el propósito declarado de la DCD, a pesar de su amplitud, también cumple con el requisito de finalidad legítima, en los términos que acabamos de ver, y por tanto, la norma puede *a priori* justificar una limitación de los derechos fundamentales concernidos. De este modo, para determinar si la misma es o no legítima, el problema debe enfocarse desde el punto de vista de los problemas de proporcionalidad *stricto sensu* de la medida: cuanto mayor la importancia de la finalidad que se persigue, mayor margen para que la autoridad pública decida los medios limitadores de derechos por los que tal finalidad debe ser alcanzada.

25 Proporcionalidad *stricto sensu*

Es un principio general del Derecho europeo que toda limitación de un derecho fundamental debe ser *proporcionada al interés general*, *necesaria* y *respetuosa de unas garantías mínimas*. Una asentada jurisprudencia del TEDH ilustra con detalle estas exigencias.

Así, por ejemplo, en el asunto Copland contra Reino Unido, relativo a la interceptación por el Estado de las llamadas telefónicas, el correo electrónico y uso de internet de una persona, el Tribunal sostuvo que tal limitación del derecho a la intimidad sólo puede

[578] Incluso, en su caso, la propuesta inicial del Consejo habría satisfecho esta parte del análisis, en opinión de algún autor. Cf. Bignami, F., Privacy and Law Enforcement…, op. cit., p. 245.

considerarse necesaria sobre la base de la legislación nacional pertinente[579]. Asimismo, en el asunto S. y Marper contra Reino Unido, relativo a la conservación de perfiles de ADN o de huellas dactilares de una persona absuelta de un delito o en relación a la cual el procedimiento se haya archivado antes de dictarse condena, el Tribunal consideró que dicha restricción del derecho a la intimidad sólo puede justificarse *si responde a una necesidad social acuciante*, si es *proporcional al objetivo* perseguido y si las razones expuestas por la autoridad pública para justificarla son pertinentes y suficientes [580] . Los principios básicos de la protección de datos exigen que la conservación de datos sea proporcionada en relación con la finalidad de su recogida, y que el período de almacenamiento sea limitado[581]. En cuanto a las escuchas telefónicas, la vigilancia secreta y los servicios de inteligencia, la jurisprudencia referida considera esencial "disponer de normas claras y detalladas que regulen el ámbito y la aplicación de las medidas, así como de garantías mínimas relativas, entre otras cosas, a la duración, el almacenamiento, el uso, el acceso de terceros, los procedimientos para preservar la integridad y la confidencialidad de los datos y los procedimientos para su destrucción, aportando así las garantías suficientes contra el riesgo de abuso y arbitrariedad".

También puede citarse a este respecto la Sentencia del TJUE en el asunto Schecke&Eifert, relativo a la publicación de todos los beneficiarios de subvenciones agrícolas en internet[582], en el que el Tribunal llegó a la conclusión de que el legislador europeo no había adoptado las medidas adecuadas para conseguir un equilibrio entre el respeto de la esencia del derecho a la intimidad y el interés general —transparencia— según lo reconocido por la UE. En particular, el TJUE consideró que los legisladores no habían tenido en cuenta otros métodos que habrían sido conformes con el objetivo, ocasionando una menor interferencia con el derecho de los beneficiarios de

---

[579] Cf. Copland contra Reino Unido, sentencia del Tribunal Europeo de Derechos Humanos, 3.4.2007, p. 9.

[580] Cf. Marper contra Reino Unido, sentencia del Tribunal Europeo de Derechos Humanos, 4.12.2008, p. 31.

[581] Ibíd.

[582] Cf. C-92/09 Volker y Markus Schecke GbR contra Land Hessen y C-93/09 Eifert contra Land Hessen y Bundesanstalt für Landwirtschaft und Ernährung, 9.11.10.

subvenciones al respeto de su intimidad y a la protección de sus datos personales. Por tanto, el Tribunal declaró que los legisladores habían excedido los límites de la proporcionalidad, dado que las "limitaciones [a la protección de los datos de carácter personal] deben establecerse sin sobrepasar los límites de lo estrictamente necesario".

Volviendo nuestra atención sobre la DCD, ha se subrayarse que el cumplimiento del requisito de proporcionalidad resultó ser el punto más complejo de todos, de tal manera que algunas de las cuestiones entonces planteadas siguen abiertas en la actualidad.

Para introducir este aspecto, podemos recurrir a la concisa explicación contenida en una conocida Opinión del Abogado General Léger[583], que —partiendo de que el juicio de proporcionalidad tiene muy diferentes formulaciones según el tribunal y el juzgador— observa que dos relevante cuestiones siempre y en todo caso han de ser respondidas: en primer lugar, ¿es la acción que se juzga *adecuada* a la finalidad declarada?, y, en segundo, ¿es la acción que se juzga *necesaria* para alcanzar la finalidad perseguida o hay medios alternativos que alcanzarían la misma finalidad sin resultar tan onerosas para el derecho a la intimidad?

El requisito de *adecuación* sólo exige que la medida no sea *manifiestamente inadecuada*, tal como una sólida línea jurisprudencial del TEDH ha puesto de manifiesto[584]. Aplicada esta definición a nuestro caso, la conservación de datos —tal como está regulada por la DCD— es evidentemente adecuada para lograr el objetivo expresado en el art. 1.1 DCD, a saber: garantizar la conservación de datos el de su disponibilidad en el contexto de la investigación, detección y enjuiciamiento de delitos graves, entendiendo por éstos los que se definan en la legislación nacional de cada Estado miembro[585].

En cuanto al requisito de *necesidad*, el juicio de proporcionalidad exige inclinarse siempre hacia medidas que sean tan factibles y efectivas para los fines que persiga la autoridad pública pero que resulten menos agresivas para los derechos afectados. En consecuencia, la medida de conservación de datos sólo puede ser considerada *necesaria*

---

[583] Cf. Parlamento Europeo contra Consejo y contra Comisión, asuntos 317/04 y 318/04.

[584] Cf. caso C-331/88, Fedesa y casos C-133/93, C-300/93 y C-362/93.

[585] Cf. art. 1.1 DCD.

si se trata de la medida *menos invasiva* de entre las disponibles para lograr el objetivo expresado en el art. 1.1 DCD, que es la "investigación, detección y enjuiciamiento de delitos graves". De los tres fines, es la detección el que permite a la DCD pasar con éxito el test de necesidad, pues mientras la intervención de las telecomunicaciones de concretos sospechosos o los procedimientos "quick freeze" —de los que ya hablamos—, podrían ser suficientes para la investigación y el enjuiciamiento de delitos graves, los mismos no son alternativas adecuadas para la detección de estos delitos, ya que estos dos procedimientos requieren que el delito o al menos un potencial perpetrador haya sido ya detectado. Así pues, la detección de delitos graves hace que las medidas de conservación de la DCD puedan ser calificadas como "necesarias" a efectos del test de proporcionalidad[586].

Siguiendo con la doctrina jurisprudencial en la materia, ésta dispone que el levantamiento de la **carga de la prueba** en el juicio de proporcionalidad corresponda al poder público. El peso de esta carga puede variar mucho, dependiendo del derecho en presencia y del interés público que se persiga. En cualquier caso, cuanto más importante sea el derecho implicado, mayor habrá de ser el esfuerzo que debe hacer la autoridad pública para demostrar la necesidad de la medida. Correlativamente, cuanto más importante sea la finalidad pública que se persigue, menor será la carga que corresponde levantar al poder público[587]. Siendo este el marco general en que se desenvuelve el juicio de proporcionalidad, ha de añadirse seguidamente que, cuando el derecho implicado es —como en este caso— la protección de datos, tal juicio se guía por las más específicas garantías de la referida Convención 108. Puesto que desde el

---

[586] Cf. Dictamen del SEPD…, doc. cit., punto 20, y Dictamen 4/2005, del GT29…, doc. cit., p. 6. Como ya hemos dicho, tanto el GT29 como el SEPD sugirieron al tiempo de la tramitación de la norma que se optara por un "quick freeze procedure", conforme al cual, cada vez que la Policía tuviera un sospechoso pero no pruebas suficientes que satisfarían los requisitos necesarios para obtener autorización judicial, podrían solicitar a los proveedores de comunicaciones que almacenaran los datos de comunicaciones de esa persona. En caso de que, posteriormente, la Policía dispusiera de las evidencias exigidas para la autorización judicial, podrían acceder a tales datos. Pese a la menor intensidad de la medida, esta ponderada opción fue ignorada repetidamente por el legislador por las razones de necesidad expuestas.

[587] Opinión del Abogado General Léger, *European Parliament v Council and v Commission*, Casos 317/04 y 318/04, 96 (2006). Puede consultarse el documento en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004C0317:EN:HTML.

mero instante en que un dato trazable a un individuo es recogido y procesado es considerado una intrusión en la vida privada, todos tales datos deben ser adecuados y relevantes para alcanzar la finalidad que se persigue[588]. Asimismo, para asegurar que el procesamiento de datos personales puede alcanzar la finalidad propuesta, tales datos deben ser "exactos y si fuera necesario puestos al día"[589]. Por otra parte, el volumen de datos procesados y el tiempo durante el que es almacenado no debe ser más del necesario para alcanzar la finalidad[590]. Además, deben adoptarse medidas de seguridad que garanticen que los datos son usados sólo por los entes y para las finalidades para las que fueron originalmente recogidos[591]. Finalmente, como salvaguarda especial del derecho a la intimidad, los individuos deben tener derecho a acceder a sus datos para comprobar que son exactos y que están siendo tratados de acuerdo con la ley[592].

Volviendo sobre la cuestión acerca de cómo el poder público tiene la carga de la prueba en materia de proporcionalidad, debe recordarse que, durante la tramitación, la Comisión sostuvo que su Propuesta cumplía con el principio de proporcionalidad "ya que su impacto sobre los ciudadanos y la industria se [había] limitado al máximo"[593]: el instrumento se ocupaba solamente de los datos de tráfico procesados por los proveedores de comunicaciones electrónicas, y el contenido de las comunicaciones electrónicas estaba excluido del ámbito de la DCD. A mayor abundamiento, sostenía la institución que el respeto de los derechos y libertades fundamentales y, en especial, el derecho a la vida y la estricta limitación de la invasión de la intimidad, habían guiado "la búsqueda del equilibrio más apropiado entre todos los intereses implicados, como el contexto social y económico y los requisitos de seguridad e intimidad"[594].

En consecuencia, la Propuesta de la DCD aseguraba que se habían "tenido en cuenta las cuestiones de proporcionalidad, especialmente en lo referente a los períodos de conservación propuestos, la distinción entre datos de telefonía y de internet, la

[588] Cf. art. 5.c), Convención 108.

[589] Cf. art. 5.d), Convención 108.

[590] Cf. art. 5.e), Convención 108.

[591] Cf. art. 7, Convención 108.

[592] Cf. art. 8, Convención 108.

[593] Cf. Exposición de Motivos de la Propuesta…, doc. cit. p. 7.

[594] Ibíd.

limitación de las categorías de datos que deben conservarse, y el sistema de reembolso de costes"[595]. Además, la norma limitaba estrictamente los fines para los que podían facilitarse los datos conservados a las autoridades represivas, en tanto que la legislación sobre protección de datos sería plenamente aplicable a los datos conservados, mientras que el impacto sobre los derechos individuales y los operadores económicos se limitaba al determinar el grupo restringido de datos de tráfico que debían conservarse[596]. Además, el período de conservación más corto de los datos de tráfico generados por el uso de internet, en comparación con los datos de tráfico generados por el uso de la telefonía móvil y fija estándar —luego eliminado— tenía en cuenta las actuales prácticas comerciales reduciendo sustancialmente el volumen de datos que deben conservarse[597].

Siendo éstos los argumentos esgrimidos por la Comisión para defender la proporcionalidad de la DCD, el SEPD, sin embargo, fue mucho más exacto en su planteamiento de la cuestión, advirtiendo que la proporcionalidad de la DCD no dependía tanto de estos aspectos como de la sustancia de las disposiciones que comprendía. En concreto, para el Supervisor, la proporcionalidad vendría a ser respetada en tanto la norma cumpliera los siguientes requisitos[598]:

— los plazos tenían que reflejar las necesidades demostradas de los servicios policiales,

— la cantidad de datos a almacenar debía reflejar las necesidades demostradas de los servicios policiales, así como asegurarse de que no sea posible acceder a datos de contenido,

— la DCD debía contener medidas de seguridad adecuadas, a fin de limitar el acceso y el uso posterior, garantizar la seguridad de los datos y asegurarse de que las propias personas a las que se refieren los datos puedan ejercer sus derechos.

---

[595] Ibíd.

[596] Ibíd.

[597] Ibíd.

[598] Cf. Dictamen del SEPD…, doc. cit., punto 27.

El SEPD hizo hincapié en su Dictamen sobre la importancia de estas ponderaciones a nivel nacional[599]. En concreto, los Estados miembros no podrían, en lo que se refiere a estos tres elementos, tomar medidas nacionales adicionales que perjudicasen la proporcionalidad. El efecto de la DCD —hacía notar el Supervisor— sería el que los proveedores dispondrían de bases de datos en las que se encontraría almacenada una cantidad significativa de datos de tráfico y de localización, por lo que la Directiva tendría que asegurarse de que el acceso a estos datos y su utilización ulterior se limitasen únicamente a determinadas circunstancias y para un número limitado de fines concretos[600]. Por añadidura, las bases de datos habrían de protegerse adecuadamente, asegurándose, entre otras cosas, de que al final de los plazos de retención los datos se borrasen efectivamente[601]. Todo ello requería a su vez de medidas técnicas y organizativas que hicieran posible un nivel elevado de seguridad de los datos[602].

A resultas de todas consideraciones, ni el GT29 ni el SEPD estimaron que la Propuesta superara adecuadamente el juicio de proporcionalidad.

Así, en referencia a las dos preguntas que planteábamos al principio, hemos de indicar —acerca de la primera cuestión— que ambos órganos se mostraron escépticos acerca de si la finalidad de datos satisfaría la finalidad de lucha contra el crimen. Concretamente, ninguna de las dos instituciones creyó que el legislador hubiera demostrado con suficiente certidumbre que las comunicaciones de datos más allá de los seis meses resultarían útiles en la investigación de los delitos[603]. La evidencia en favor de la conservación de datos procedía en gran medida de estadísticas proporcionadas por la Policía británica[604], conforme las cuales los datos de tráfico de más de seis meses resultaban con frecuencia útiles en la investigación de delitos graves. Ambos organismos consideraron estas pruebas inadecuadas[605].

---

[599] Cf. Dictamen del SEPD…, doc. cit., punto 28.

[600] Cf. Dictamen del SEPD…, doc. cit., punto 29.

[601] Cf. Dictamen del SEPD…, doc. cit., punto 30.

[602] Cf. Dictamen del SEPD…, doc. cit., punto 31.

[603] Cf. Dictamen del SEPD…, doc. cit., punto 27, y Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 6.

[604] Cf. Dictamen del SEPD…, doc. cit., punto 16.

[605] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 4.

Finalmente, es oportuno terminar mencionando la opinión del CESE, que —en lo que se refería al principio de proporcionalidad y en una línea de pensamiento distinta— observaba que cualquier norma que —como la DCD— restringiera derechos fundamentales requeriría la participación mediante ley de los parlamentos nacionales, además de garantías de control judicial —*ex ante o ex post*— de índole legislativa[606]. Resultaba en consecuencia difícil imaginar —consideraba el CESE— "que la desaparición de unas «barreras invisibles» existentes a la prestación de los servicios de comunicaciones electrónicas en todo el territorio del mercado interior pueda comportar una modificación en cascada de las leyes nacionales que garantizan los derechos fundamentales, así como los sistemas nacionales de salvaguardia de los mismos"[607]. Así, pues, el Comité dudaba de que la DCD cumpliera en su totalidad con los principios de subsidiariedad y proporcionalidad, por la ausencia de razones que justificasen que un objetivo de la Unión pueda alcanzarse mejor en el plano de ésta[608].

Todo lo antedicho pone de manifiesto el hecho de que las implicaciones del principio de proporcionalidad sólo pueden ser evaluadas a la luz de sus concretas manifestaciones, que, en lo que a la DCD se refiere, se concretan a nuestro entender en los tres aspectos que estudiaremos pormenorizadamente a continuación y que han sido objeto de agitado debate tanto en sede legislativa como doctrinal. Nos referimos a la proporcionalidad de la medida de conservación generalizada de datos, la de sus plazos de su conservación y la del concreto conjunto de datos que ha de retenerse.

25.1 Proporcionalidad en el conjunto de concretas categorías de datos que se han de conservar

Examinaremos ahora la proporcionalidad de las medidas de la DCD en lo que se refiere a la cantidad de datos que han de retenerse.

---

[606] Punto 2.3.13

[607] Cf. Dictamen del CESE…, doc. cit., punto 2.3.14.

[608] Ibíd.

Al respecto, ha de señalarse que, desde un principio, resultó claro que la norma no incluiría datos de contenido, esto es, los proveedores de contenido no tendrían que crear inmensas bases de datos con conversaciones telefónicas e emails que podrían ser registrados por la Policía [609] . Igualmente, también desde el primer borrador se establecieron las seis categorías de datos que habían de ser recogidos, a saber[610]:

— datos necesarios para rastrear e identificar el origen de una comunicación;
— datos necesarios para identificar el destino de una comunicación;
— datos necesarios para identificar la fecha, hora y duración de una comunicación;
— datos necesarios para identificar el tipo de comunicación;
— datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; y,
— datos necesarios para identificar la localización del equipo de comunicación móvil.

Más adelante, dos concretos puntos de debate surgieron durante la tramitación legislativa. Algunos indicaron que las llamadas que habían sido realizadas pero no respondidas debían considerarse como una comunicación, y por tanto habían de ser objeto de conservación. Más tarde, se argumentó que datos de localización del equipo móvil debían recogerse durante todo el tiempo que durase la llamada, permitiendo así a la policía no sólo monitorizar las llamadas, sino también conocer los movimientos de los individuos. Por su parte, el GT29 recomendó la conservación de únicamente las llamadas respondidas y de los datos que permitieran la localización del sujeto solamente al inicio de la llamada[611]. Esta recomendación fue acogida por el Parlamento Europeo, si bien el Consejo y la Comisión, en cambio, la rechazaron y consiguieron que en la versión final de la Directiva las llamadas no respondidas y la localización del terminal móvil durante toda la llamada fueran conservadas, tal como ha quedado reflejado en los arts. 3.2 y 5.f).2 DCD[612].

---

[609] Cf. art. 3 de la Propuesta de Directiva.

[610] Cf. Anexo de la Propuesta de Directiva.

[611] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 10.

[612] Cf. Parliament Report…, doc. cit., p. 35.

Por nuestra parte, hemos de apuntar que la evidencia de que la selección de los concretos datos que han de ser retenidos en virtud de la DCD no es una decisión neutra. Informaciones tales como la identidad de los emisores y receptores de las comunicaciones, la duración y frecuencia de éstas, la localización física, etc. son elementos que invaden la vida privada de las personas y, en muchos casos, también pueden dañar otros derechos como el secreto profesional o la asistencia jurídica debida, por lo que su selección por el legislador y, posteriormente, por el Juez, debe someterse a una razonado test de proporcionalidad, en atención a las circunstancias generales y específicas concurrentes[613].

En este sentido, y por lo que respecta a la selección hecha en abstracto por el legislador europeo, debe criticarse el que la lista de datos a retener sea una lista cerrada y obligatoria en cada uno de sus puntos, en lugar de una de máximos de la cual los Estados pudieran exonerar aquellos que tengan a bien. No es de extrañar, por tanto, que el GT29 se haya mostrado a este respecto favorable a la limitación del conjunto de datos que deben conservarse por lo que se refiere al uso de internet, así como que, en general, los datos que deben conservarse se limiten a los recogidos por los proveedores para fines técnicos y de facturación[614].

25.2 Proporcionalidad en los períodos de conservación de los datos

Siendo difícil encontrar una alternativa real a la conservación generalizada de los datos de tráfico y localización, tal como ha quedado regulada por la DCD, la cuestión se desplaza a otro aspecto de las medidas de conservación, a saber: si los períodos de conservación del art. 6 se prolongan por el plazo estrictamente necesario para garantizar la finalidad del art. 1 DCD, o por el contrario, son más largos de lo realmente preciso.

El plazo de conservación de los datos se encuentra estrechamente vinculado a la propia medida de conservación y plantea la necesidad de ponderación entre la finalidad

[613] Cf. Dictamen del CESE…, doc. cit., punto 2.4.2.

[614] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 2.

perseguida —el aseguramiento de la eventual puesta a disposición de los datos conservados, cediéndolos a los agentes facultados— y el gravamen que para el derecho a la protección de los datos de carácter personal supone la prolongación en el tiempo del tratamiento de los datos. Si bien podrían parecer más justificadas las previsiones de distintos plazos de conservación en virtud de la finalidad a que se adscriba la cesión —vg. represión de delitos sin especificaciones o represión de delitos concretos especialmente graves— no ha sido el caso de la DCD.

La cuestión podría quedar resuelta satisfactoriamente analizando la antigüedad de los datos que en la práctica de los Estados sirven para la "investigación, detección y enjuiciamiento de delitos graves". Por desgracia, hasta la fecha no se ha realizado ningún estudio empírico a nivel europeo que demuestre hasta qué punto los datos retenidos por cierto plazo son necesarios[615]. No es posible, en consecuencia, determinar con certeza si uno, dos o más años son o no necesarios.

No obstante, conviene advertir que el documento inicial elaborado por el Consejo establecía un período de entre uno y tres años[616]. La Comisión consideró este período desproporcionado y lo redujo considerablemente en su Propuesta: los datos de las llamadas se habrían de conservar durante un año, en tanto que los correos electrónicos y protocolos de VoiP durante seis meses[617]. Tras negociaciones con el Consejo y las demás partes interesadas, el período de retención en la versión finalmente aprobada se en fijó en un período de entre seis meses a dos años para todas las categorías y tipos de datos. Como bien ha observado BIGNAMI, esta determinación alcanzada por el Consejo —preocupado por las cuestiones de eficacia y seguridad ciudadana— y el Parlamento y los organismos de protección de datos —más preocupados por la protección de la intimidad—, es el justo medio entre ambas posturas: el plazo es un año más corto que

[615] Nótese además que muy pocos Estados miembros han proporcionado cifras a la Comisión conforme al deber establecido al efecto por el art. 10 DCD, como ha lamentado el GT29 en su informe 1/2010, disponible en http://ec.europa.eu/ justice/ policies/ privacy/ docs/ wpdocs/ 2010/ wp172_ en.pdf. También se ha hecho eco de esta carencia la propia Comisión en su Informe (p. 19).

[616] Cf. art. 1.2 de la Propuesta de Directiva.

[617] Cf. art. 7 de la Propuesta de Directiva.

lo pretendido inicialmente por el Consejo, y un año más largo que la posición mantenida por el Parlamento[618].

En todo caso, de acuerdo con las argumentaciones esgrimidas al respecto durante la tramitación de la DCD, el mejor parámetro de la proporcionalidad de los períodos máximos para la conservación obligatoria y general de los datos marcados en la DCD sólo puede venir dado que una justificación precisa de los mismos y respaldada claramente con pruebas.

Durante la elaboración de la DCD, tanto la Comisión como la Presidencia del Consejo concedieron importancia a un estudio de la Policía del Reino Unido que demostraba que aunque el 85% de los datos de tráfico requeridos por la Policía tenían un máximo de seis meses de antigüedad, en tanto que los datos de entre seis meses y un año se utilizaban en investigaciones complejas de delitos más graves[619]. En este sentido, el plazo de retención previsto en la Propuesta —de un año para datos telefónicos — se suponía que reflejaban estas prácticas de los servicios policiales.

Pese al plazo de un año y los datos estadísticos suministrados, el SEPD no se mostró convencido de que tales cifras representasen las pruebas de la necesidad de la retención hasta un año de los datos de tráfico, puesto que "el hecho de que en algunos casos la disponibilidad de los datos del tráfico y/o de localización ayudara a resolver un delito no significa automáticamente que esos datos sean necesarios, en general, como instrumento para los servicios policiales" [620]. Sin embargo, no podían ignorarse las cifras, pues representaban por lo menos "una tentativa seria de demostrar la necesidad de la retención"[621]. Por otra parte, las cifras indicaban claramente que no se requería un plazo de retención de más de un año desde la perspectiva de las prácticas corrientes de los servicios policiales.

---

[618] Cf. BignamI, F., Privacy and Enforcement…, op. cit., p. 248.

[619] Cf. Documento de la Presidencia británica de la Unión Europea, de 7 de septiembre de 2005, *Liberty and security: striking the right balance* (Libertad y seguridad: mantener un equilibrio adecuado).

[620] Cf. Dictamen del SEPD…, doc. cit., punto 17.

[621] Ibíd.

Por su parte, y en la misma línea, el GT29 hizo hincapié en que debía regularse un período de conservación general que fuera lo más breve posible y lo más cercano al período de conservación para cuyos fines originales los prestadores de servicios de comunicaciones registraron los datos. Como ya indicamos, ya con ocasión del fallido proyecto de Decisión marco, el GT29 había manifestado que la retención obligatoria de los datos de tráfico, bajo las condiciones previstas en el proyecto, no resultaba aceptable porque el análisis que aportaron los proponentes mostró que la mayoría de los datos de tráfico exigidos por los servicios policiales no superaba los seis meses. En el caso de la DCD, el mismo organismo mostró su preocupación por el hecho de que la iniciativa de la Comisión Europea podría en definitiva dar lugar al establecimiento de períodos de conservación máximos más extensos que los previstos en el pasado, sobre lo cual el GT29 se había expresado desfavorablemente —la última vez, en el Dictamen nº 9/2004 adoptado el 9 de noviembre de 2004—.

Sin embargo, en todo caso, debe subrayarse que cualquier estudio que se realizara acerca de qué períodos de conservación son proporcionados demostraría que siempre quedan delitos para cuya averiguación los datos deben guardarse durante dos, cuatro, ocho o más años. Esto pone de manifiesto que, en realidad, la cuestión de cuánto tiempo los datos pueden ser conservados para que su conservación pueda ser considerada "necesaria" y no vulneradora de los derechos de la Carta es, en realidad y predominantemente, una cuestión de proporcionalidad *stricto sensu* más que de necesidad.

25.3 Proporcionalidad en la medida de conservación generalizada de datos.

Los conceptos de necesidad y proporcionalidad de la medida de conservación de datos han jugado un papel de primer orden desde los comienzos del debate sobre la conveniencia de su adopción. Así, por ejemplo, el fallido proyecto de Decisión marco debe parte de su fracaso al hecho de que el GT29 sostuviera —en un informe fechado el 9 de noviembre de 2004— que la retención obligatoria de los datos de tráfico, bajo las condiciones previstas en el proyecto, no resultaba aceptable, entre otras cosas por la imposibilidad de los proponentes de facilitar cualquier prueba en lo que se refiere a la

necesidad de la retención a efectos de orden público[622]. En concreto, el análisis que aportaron mostró que la mayoría de los datos de tráfico exigidos por los servicios policiales no superaba los seis meses, plazo durante el cual —según la legislación europea de telecomunicaciones— las compañías solían conservar la información a los permitidos efectos de facturación y prestación del servicio, lo que hacía inútil la medida[623].

Sin embargo, la necesidad de la DCD —y por ende, la determinación de su proporcionalidad— podía en cambio venir dada, según apuntó el SEPD, por los velozmente cambiantes desarrollos de la conservación de datos por los propios proveedores [624] . En concreto, el Supervisor hizo notar que las compañías de telecomunicaciones no utilizaban siempre las posibilidades de que disponían conforme a la Directiva 2002/58/CE para retener datos de tráfico a efectos de facturación, dado que en un número cada vez mayor de casos no se realizaba en absoluto la retención de datos a tales efectos —vg. las tarjetas de prepago para comunicaciones desde teléfonos móviles, suscripciones a tarifas planas, etc.[625]—. En esos cada vez más frecuentes supuestos, los datos de tráfico y de localización no se almacenaban en absoluto, sino que se borraraban inmediatamente después de la comunicación. Lo mismo ocurría con las llamadas infructuosas. Esto podía tener, a juicio del dictaminante, un impacto sobre la eficacia de los servicios policiales que sí justificaba la necesidad de establecer una medida de conservación generalizada[626].

---

[622] Nos referimos al ya expuesto Proyecto de Decisión marco sobre la conservación de los datos tratados y almacenados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o el suministro de datos en redes públicas de comunicaciones a efectos de la prevención, investigación, descubrimiento y represión de la delincuencia y de las infracciones penales, con inclusión del terrorismo, presentada por la República Francesa, Irlanda, el Reino de Suecia y el Reino Unido el 28 de abril de 2004 (CNS/2004/0813). El texto íntegro en su publicación oficial es accesible en el siguiente enlace: http://register.consilium.eu.int/pdf/es/04/st08/st08958.es04.pdf

[623] Cf. Dictamen del SEPD…, doc. cit., punto 14.

[624] Cf. Dictamen del SEPD…, doc. cit., punto 15.

[625] Cf. Dictamen del SEPD…, doc. cit., punto 18.

[626] Ibíd.

Por otra parte, un segundo argumento en favor de la proporcionalidad de la DCD venía dada por las perturbaciones en el funcionamiento del mercado interior que se había generado —y podría aumentar— por la adopción de medidas legislativas, en los Estados miembros de conformidad con el artículo 15 DPCE[627]. Por ejemplo, como indicamos en la Primera Parte de esta Tesis, gobiernos como el italiano habían por entonces publicado normas que obligaban a los proveedores a almacenar datos telefónicos durante largos períodos —cuatro años en el caso de Italia[628]—.

En tercer lugar, el SEPD hacía notar que los métodos de trabajo de las autoridades policiales hacían que el uso de apoyo técnico se hubiera vuelto más importante, de manera tal que estos progresos requerían que las autoridades dispusieran de instrumentos "adecuados y formulados con precisión para que puedan trabajar con el debido respeto a los principios de la protección de datos"[629]. La misma opinión fue mantenida por el GT29, que observó que los datos conservados en virtud de la DCD podían constituir una herramienta útil para los investigadores. El Dictamen advertía, no obstante, de la existencia de "otras medidas útiles" que debían tenerse en cuenta a efectos de investigación, y que incidían en menor grado sobre los derechos fundamentales de los ciudadanos, poniendo por ejemplo el procedimiento *quick freeze* —procedimiento de congelación rápida—, que ya explicamos en un apartado anterior[630]. Sin embargo, el Supervisor contraargumentaba al respecto que este instrumento —que en sí mismo tiene efectivamente menos impacto sobre los derechos— podía no ser siempre suficiente, en especial por no seguir la pista de las personas implicadas en el terrorismo u otros delitos graves que no hayan sido

---

[627] Cf. Dictamen del SEPD…, doc. cit., punto 19.

[628] Cf. Decreto Legislativo n. 196, Codice in materia di protezione dei dati personali, publicado el 29 de julio de 2003 en Gazzetta Ufficiale, n. 174, Supplemento Ordinario, n. 123. El texto de la norma es accesible en: http://www.camera.it/parlam/leggi/deleghe/testi/03196dl.htm.

[629] Cf. Dictamen del SEPD…, doc. cit., punto 20.

[630] Recuérdese que en este sistema ni los proveedores de comunicación ni los prestadores de servicios de internet están obligados a almacenar datos relativos al tráfico. De este modo, en casos justificados, las autoridades policiales consultan a las empresas y piden que se almacenen ciertos datos. Después de que esos datos se hayan almacenado, las autoridades tienen algunas semanas para recoger pruebas a fin de obtener una orden judicial. Posteriormente, con esta orden, pueden acceder a los datos.

sospechosas previamente de ninguna actividad delictiva[631]. De hecho, a la vista del aumento de la preocupación por los atentados terroristas, el SEPD compartía el punto de vista de que la seguridad física tiene, en cuanto tal, una importancia máxima para nuestras sociedades. A su entender, los gobiernos tenían la obligación, en caso de ataques contra la ciudadanía, de demostrar que conceden la mayor consideración a esta necesidad de protección y de investigar si tienen que reaccionar introduciendo nuevas medidas legislativas. El deber para los gobiernos—tanto a nivel nacional como europeo— de "proteger a la sociedad y para demostrar que hacen todo lo necesario para asegurar la protección, inclusive mediante la adopción de nuevas medidas, legítimas y eficaces, como consecuencia de sus investigaciones", podía entenderse así como una justificación de la proporcionalidad de la medida[632].

Además, no puede dejar de considerarse que las razones que justifican la proporcionalidad de la DCD están sujetas a los más diversos cambios, dado que la medida se ordena a perseguir delitos en un ámbito en constante evolución como es el tecnológico. La introducción de medios de vigilancia general de los ciudadanos puede dar lugar a estrategias por parte del terrorismo y de la delincuencia organizada para no utilizar ciertos medios. Esto daría lugar a la necesidad de desarrollar nuevos métodos de vigilancia aún más estrictos, iniciándose así una espiral de posibles infracciones de los derechos fundamentales de los ciudadanos que sería difícil detener, al tiempo que cambiaría el carácter de la sociedad que tratamos de proteger. De ahí la necesidad de que las consideraciones de proporcionalidad deban al menos evaluarse periódicamente y publicarse los resultados.

No deja de resultar relevante —y así hemos de hacerlo constar— que a pesar de todas estas consideraciones, tanto el GT29 como el SEPD se mostraban contrarios a la adopción de la DCD. En el caso del primero, las circunstancias que justificaban la conservación de datos y su proporcionalidad, si bien se afirmaba por la Comisión que

[631] Cf. Dictamen del SEPD…, doc. cit., punto 20. Sin embargo, el SEPD consideraba "necesarias más pruebas para determinar si éste es realmente el caso".

[632] Cf. Dictamen del SEPD…, doc. cit., punto 21. Aunque con menor convencimiento, el GT29 también reconocía que algunas circunstancias de nuestras sociedades habían cambiado en relación con los riesgos que suponían las amenazas terroristas, y era consciente de que algunos datos son a veces útiles y pueden utilizarse justificadamente en determinadas investigaciones.

se basaban "en las peticiones de las autoridades competentes de los Estados miembros", no parecía al entender del órgano "apoyarse en pruebas claras", por lo que, en consecuencia, las condiciones propuestas no parecían convincentes "de momento"[633].

Algo similar indicaba el SEPD, que se mostró "no convencido" de la necesidad de la retención de datos de tráfico y de localización a efectos policiales[634]. En concreto, recordando la importancia del principio jurídico establecido por la Directiva 2002/58/CE de que los datos de tráfico deben borrarse en cuanto el almacenamiento ya no sea necesario para fines que no estén relacionados con la propia comunicación, consideraba el Supervisor que las cifras facilitadas no probaban que el marco jurídico existente no ofreciera los instrumentos necesarios para proteger la seguridad física, ni que los Estados miembros ejercieran plenamente sus competencias conforme a la legislación europea para cooperar según les garantiza el marco jurídico vigente —pero sin los resultados necesarios—[635].

En una última concesión, sin embargo, concluía el Supervisor que si el Parlamento Europeo y el Consejo, tras haber sopesado cuidadosamente los intereses en juego, llegaban a la conclusión de que la necesidad de la conservación de los datos de tráfico y de localización está suficientemente demostrada, la retención sólo podía justificarse conforme al Derecho comunitario en la medida en que se otorgaran las salvaguardias adecuadas, de conformidad con los criterios que acabamos de exponer[636].

26 Conclusiones de esta Segunda Parte

Al disponer la conservación generalizada de numerosas categorías de datos externos de las comunicaciones, la DCD ha introducido en el Derecho de la Unión Europea una medida que limita los derechos fundamentales a la intimidad y a la protección de datos personales de todos los ciudadanos europeos que usan diariamente servicios telefónicos

---

[633] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 7.

[634] Cf. Dictamen del SEPD…, doc. cit., punto 22.

[635] Ibíd.

[636] Cf. Dictamen del SEPD…, doc. cit., punto 23.

e internet. La legitimidad de esta limitación sólo puede establecerse si se cumplen tres requisitos establecidos por una sólida jurisprudencia del TJUE y TEDH sobre medidas limitadores de derechos fundamentales.

En primer lugar, la medida debe estar *establecida por la ley* y expresada de una manera precisa, de modo que provea convenientemente contra la acción arbitraria del poder público y dé a conocer a los ciudadanos la posibilidad de injerencias en su esfera de libertades[637]. La DCD cumple este requisito, en tanto que una directiva es una norma comunitaria que satisface las condiciones establecidas por los arts. 52.1 CDF y 8 CEDH, siempre que sea precisa y accesible al público. La norma regula con detalle todos los aspectos relativos a la medida que pretende imponerse, al especificar su objetivo y ámbito, las categorías de datos que deben conservarse, los períodos de conservación, los requisitos de almacenamiento para los datos conservados y otros tantos aspectos en abundancia suficiente para superar el canon de calidad impuesto por la jurisprudencia europea.

En segundo lugar, la finalidad de la medida limitadora de derechos fundamentales debe ser *legítima*, es decir, debe ser necesaria para alcanzar un objetivo de interés general o para proteger los derechos y libertades de otros y estar relacionada con alguna de las categorías reconocidas en los arts. 52.1 CDF u 8 CEDH. La DCD cumple también este requisito: su art. 1.1 DCD establece como fin del deber de conservación de datos el de su disponibilidad en el contexto de la investigación, detección y enjuiciamiento de delitos graves[638]. Esta finalidad es legítima en tanto que se enmarca expresamente dentro de las competencias otorgadas por el art. 82 TFUE a la Unión en materia de cooperación judicial en asuntos penales.

En tercer lugar, la injerencia en los derechos fundamentales efectuada por la DCD debe ser *proporcional al objetivo perseguido* para así *respetar el contenido esencial* de los derechos implicados. Esta proporcionalidad se concreta en dos elementos: a) la búsqueda de medios alternativos, menos agresivos, para alcanzar el fin propuesto; y, b)

---

[637] Cf. art. 52.1 de la Carta así como *Amann v Switzerland*, App No 27798/95, 30 Eur HR Rep 843, 858 ¶ 50 (2000).

[638] Cf. art. 1.1 DCD.

una ponderación de la importancia del derecho en cuestión en comparación con la finalidad pública que se persigue. En cuanto al primer elemento, no existe un medio menos agresivo que la conservación generalizada de datos para lograr la detección de delitos graves, que es la primera finalidad citada por el art. 1.1 DCD. Los procedimientos "quick freeze" podrían ser suficientes para la investigación y el enjuiciamiento de los mismos, pero no para su detección. El segundo elemento comporta valorar los elementos concretos de la medida —qué concretos datos son almacenados y durante cuánto tiempo— para determinar si son los estrictamente necesario para garantizar la finalidad del art. 1 DCD, o por el contrario, van más allá de lo realmente preciso. La cuestión podría quedar resuelta satisfactoriamente analizando la antigüedad y el tipo de datos que en la práctica de los Estados sirven para la "investigación, detección y enjuiciamiento de delitos graves". Por desgracia, hasta la fecha no se ha realizado ningún estudio empírico a nivel europeo que demuestre hasta qué punto los datos retenidos por cierto plazo son necesarios. No es posible, en consecuencia, determinar con certeza este punto. Ante la falta de información al respecto, es de criticar que la lista de datos a retener hecha en abstracto por el legislador europeo sea una lista cerrada y obligatoria en cada uno de sus puntos, en lugar de una de máximos de la cual los Estados pudieran exonerar aquellos que tengan a bien, disminuyendo así la injerencia en los derechos fundamentales de los ciudadanos.

TERCERA PARTE. LEY 25/2007, DE 18 DE OCTUBRE, DE CONSERVACIÓN DE DATOS RELATIVOS A LAS COMUNICACIONES ELECTRÓNICAS Y A LAS REDES PÚBLICAS DE COMUNICACIONES

27 Presentación, precedentes legislativos y tramitación de la ley

Al abordar el estudio en profundidad de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[639], un afán de sistematicidad nos invita a comenzar explicando su estructura. Así, lo primero que cabe señalar es que la norma consta de una exposición de motivos, diez artículos divididos en tres capítulos, una disposición adicional, una disposición transitoria, una disposición derogatoria y cinco disposiciones finales[640]. Al examen detallado de todos estos elementos dedicaremos esta parte de la presente Tesis.

El objeto de la norma en presencia consiste, en lo formal, en la transposición de la Directiva 2006/24/CE —de la que hemos tratado anteriormente— y, en lo sustantivo, en la introducción en nuestro ordenamiento interno de la obligación para los operadores que prestan servicios de comunicaciones electrónicas de captar y conservar los datos generados en el marco de sus servicios de comunicaciones electrónicas de manera que estén disponibles por el plazo de doce meses para la averiguación y represión de delitos graves[641].

Tal deber general de retención de datos de tráfico electrónico no es completamente novedoso en nuestro Derecho, pues ya el art. 12 de la Ley 34/2002, de 11 de julio, de

---

[639] Publicada en BOE núm. 251, de 23 de octubre de 2007.

[640] Cf. Exposición de Motivos, apartado II, párrafo primero.

[641] Cf. art. 1 y 5 LCD.

servicios de la sociedad de la información y de comercio electrónico[642] —en adelante, LSSI— previó un régimen similar que no llegó a entrar en vigor por falta del necesario desarrollo reglamentario.

Además, hemos de hacer notar que el contenido de dicha regulación la ubica, por una parte, dentro del Derecho de las telecomunicaciones —en tanto que establece un conjunto de obligaciones jurídico-públicas que los operadores deben cumplir—, y, por el otro, del Derecho procesal penal, dado que tales obligaciones se ordenan a la persecución y enjuicimiento de delitos graves. El resultado es una normativa de Derecho público que estable una importante excepción en el marco de los derechos de los usuarios de las telecomunicaciones y que además comporta una grave afectación de derechos fundamentales de creciente relevancia en nuestros días, tales como la intimidad, la protección de datos y el secreto de las comunicaciones. Dejando esta concreta cuestión para más tarde, expondremos a continuación el marco jurídico previo en el que ha hecho aparición la LCD, primero con respecto al Derecho de las telecomunicaciones, y después en lo que se refiere al ordenamiento procesal penal vigente en nuestro país.

27.1 Marco jurídico previo

Los aspectos centrales del sector de las telecomunicaciones se regulan en España por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones[643] —en adelante, LGT—, que comprende la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados[644]. Esta Ley, junto con su

[642] Publicada en BOE núm. 166, de 12 de julio de 2002.

[643] Publicada en BOE núm. 264, de 4 de noviembre de 2003. Tres grandes monografías sobre régimen legal español de telecomunicaciones destacan en nuestra literatura, a saber: De la Quadra Salcedo, T., Derecho de la Regulacion Economica, Tomo IV: Telecomunicaciones, Iustel, Portal Derecho, 2009; Cremades, J., y Rodriguez-Arana Muñoz, J., Comentarios a la Ley General de Telecomunicaciones, La Ley, 2004; y, Garcia de Enterria, E., Comentarios a la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, Civitas Ediciones, 2004.

[644] Cf. art. 1 LGT.

necesario desarrollo reglamentario[645], incorporó al ordenamiento jurídico español el contenido de la abundantísima normativa comunitaria en la materia[646], respetando plenamente los principios recogidos en ella aunque adaptándolo a las peculiaridades propias del Derecho y de la situación económica y social de nuestro país[647].

Para enmarcar mejor nuestras consideraciones, nos limitaremos a señalar que la LGT regula principalmente las siguientes materias: aspectos generales de la explotación de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia[648]; obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas[649]; evaluación de la conformidad de equipos y aparatos[650]; dominio público

---

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

[646] La Unión Europea ha dirigido sus esfuerzos durante muchos años a consolidar un marco armonizado de libre competencia en las telecomunicaciones alcanzado entre los Estados miembros. Este esfuerzo ha desembocado en la aprobación de un nuevo marco regulador de las comunicaciones electrónicas, compuesto por diversas disposiciones comunitarias. Se trata, hasta la fecha, de la Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas; la Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas; la Directiva 2002/22/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas; 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; 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; la Directiva 2002/77/CE, de la Comisión, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas; y, finalmente, la Decisión n. o 676/2002/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea. La LGT traspone las citadas directivas.

[647] Cf. Apartado I, Exposición de Motivos, LGT.

[648] Cf. Título II, LGT.

[649] Cf. Título III, LGT.

[650] Cf. Título IV, LGT.

radioeléctrico[651]; Administración de las telecomunicaciones[652]; tasas en materia de telecomunicaciones[653]; y, por último, inspección y régimen sancionador de la propia normativa[654].

No de menor interés resulta el que entre los principales objetivos de la LGT[655] se cuentan expresamente el fomento de la competencia efectiva en los mercados de

---

[651] Cf. Título V, LGT.

[652] Cf. Título VI, LGT.

[653] Cf. Título VII, LGT.

[654] Cf. Título VIII, LGT.

[655] El tenor literal del artículo reza así: "Artículo 3. Objetivos y principios de la Ley. Los objetivos y principios de esta Ley son los siguientes:

a) Fomentar la competencia efectiva en los mercados de telecomunicaciones y, en particular, en la explotación de las redes y en la prestación de los servicios de comunicaciones electrónicas y en el suministro de los recursos asociados a ellos. Todo ello promoviendo una inversión eficiente en materia de infraestructuras y fomentando la innovación.
b) Garantizar el cumplimiento de las referidas condiciones y de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas, en especial las de servicio universal.
c) Promover el desarrollo del sector de las telecomunicaciones, así como la utilización de los nuevos servicios y el despliegue de redes, y el acceso a éstos, en condiciones de igualdad, e impulsar la cohesión territorial, económica y social.
d) Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones, como la numeración y el espectro radioeléctrico, y la adecuada protección de este último, y el acceso a los derechos de ocupación de la propiedad pública y privada.
e) Defender los intereses de los usuarios, asegurando su derecho al acceso a los servicios de comunicaciones electrónicas en adecuadas condiciones de elección, precio y calidad, y salvaguardar, en la prestación de éstos, la vigencia de los imperativos constitucionales, en particular, el de no discriminación, el del respeto a los derechos al honor, a la intimidad, a la protección de los datos personales y al secreto en las comunicaciones, el de la protección a la juventud y a la infancia y la satisfacción de las necesidades de los grupos con necesidades especiales, tales como las personas con discapacidad. A estos efectos, podrán imponerse obligaciones a los prestadores de los servicios para la garantía de dichos derechos.
f) Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.
g) Promover el desarrollo de la industria de productos y servicios de telecomunicaciones.
h) Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea".

telecomunicaciones, la promoción del desarrollo del sector y el acceso a estos servicios, la contribución al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea y el impulso a la neutralidad tecnológica en la regulación[656]. También es objetivo de la LGT —lo que resulta de gran relevancia para nuestro estudio, y por eso lo subrayamos aquí— la defensa de los intereses de los usuarios[657], la cual debe llevarse a cabo "asegurando su derecho al acceso a los servicios de comunicaciones electrónicas", así como la salvaguarda, en la prestación de éstos, "de los imperativos constitucionales, en particular, el de no discriminación, el del respeto a los derechos al honor, a la intimidad, a la protección de los datos personales y al secreto en las comunicaciones, el de la protección a la juventud y a la infancia y la satisfacción de las necesidades de los grupos con necesidades especiales, tales como las personas con discapacidad"[658].

A los efectos anteriores, concluye el art. 3.e) LGT, "podrán imponerse obligaciones a los prestadores de los servicios para la garantía de dichos derechos", tarea que lleva a cabo la LGT en sus arts. 33 a 38, que comprenden el Capítulo III del Título III bajo la ya expresiva rúbrica de *Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas*. De este grupo de normas nos ocuparemos a continuación —así como en otras partes del presente trabajo— ya que es precisamente en el área regulada por estos seis artículos en donde las disposiciones de la LCD vienen a encuadrarse como una excepción a sus principios generales[659]. Veamos a renglón seguido de qué tratan.

El art. 33 LGT establece un deber general de protección del secreto de las comunicaciones por parte de los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas

---

[656] Cf. art. 3 LGT.

[657] Cf. art. 3.e) LGT.

[658] El art. 3.e) LGT se hace eco así de lo dispuesto en el art. 20 de nuestra Constitución.

[659] De hecho, en la Disposición Transitoria Única de la LCD —*Vigencia del régimen de interceptación de telecomunicaciones*— el legislador creyó oportuno aclarar que las normas dictadas en desarrollo de estos artículos "continuarán en vigor en tanto no se opongan a lo dispuesto en la propia Ley".

disponibles al público[660]. De esta manera, las compañías dedicadas a la explotación de estas redes tienen la obligación expresa de garantizar el secreto de las comunicaciones "de conformidad con los artículos 18.3 y 55.2 de la Constitución" y "debiendo adoptar las medidas técnicas necesarias" para preservar tal finalidad. Como es bien sabido, el art. 18.3 CE es el que garantiza en nuestra carta magna el secreto de las comunicaciones y "en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial", en tanto que el art. 55.2 CE previene la posible suspensión de este derecho de acuerdo con una ley orgánica, con la necesaria intervención judicial y el adecuado control parlamentario, para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas[661].

En relación con esto, el art. 33 LGT añadía —en su redacción previa a la entrada en vigor de la LCD— la existencia de un deber adicional para los operadores de adoptar a su costa "las medidas que se establezcan reglamentariamente para la ejecución de las interceptaciones dispuestas conforme a lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia". En estas dos últimas normas citadas —sobre las que volveremos pronto— se recogía y recoge una buena porción del régimen conforme al cual puede efectuarse en nuestro Estado de derecho la

---

[660] Transcribimos aquí el texto original del artículo, tal como fue publicado el 4 de noviembre de 2003 y estuvo en vigor hasta la Ley 25/2007, de 18 de octubre: "Artículo 33. Secreto de las comunicaciones. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

Asimismo, los operadores deberán adoptar a su costa las medidas que se establezcan reglamentariamente para la ejecución de las interceptaciones dispuestas conforme a lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia".

[661] No estará de más recordar que el art. 55.2 CE dispone que "una Ley Orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas".

interceptación de las comunicaciones con fines de descubrimiento y comprobación de hechos delictivos[662] o para el cumplimiento de las funciones asignadas al CNI[663].

Con la entrada en vigor de la LCD, el art. 33 LGT recibió una nueva y mucho más amplia redacción a través de su Disposición Final Primera, que le añadió nueve nuevos apartados[664] que contienen numerosos detalles sobre el régimen de interceptación de las comunicaciones desde la perspectiva de las obligaciones que atañen a los proveedores. De acuerdo con la Exposición de Motivos[665], las modificaciones incluidas buscan adaptar la LGT al contenido de la LCD; sin embargo, debe señalarse que lo que lo que realmente llevan a cabo los nuevos apartado es incorporar a la LGT las previsiones sobre intervención de las comunicaciones que con anterioridad se incluían en los artículos 84.i), 86.2, 87.2 y 3, 88, 89.2 , 95 y 96 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el *Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios* —en adelante, RLGT[666]—, así como una ligera pero relevante modificación de las previsiones contenidas en el contenido original del artículo 33 LGT. Tal regulación complementa técnicamente la del art. 579 LECrim[667], que se ocupa de la vertiente procesal[668].

---

[662] Cf. art. 579.1 LECrim.

[663] Cf. art. único, apartado 1, de la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

[664] El tenor del apartado primero, más o menos coincidente con el anterior, se ha dividido ahora en dos apartados.

[665] Cf. Exposición de Motivos, apartado II.

[666] Critica GONZÁLEZ LÓPEZ que el legislador ha incorporado literalmente a la LGT aquellos aspectos que ha querido, olvidando algunos esenciales para la comprensión del conjunto, y sin especificar qué partes del reglamento continúan vigentes (ya que sólo es posible acudir a la previsión de la Disposición Derogatoria Única de que "quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley"). El resultado es una regulación legal insuficiente que obliga a acudir al reglamento como medio para su interpretación. Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 35.

[667] El régimen de interceptación de las comunicaciones electrónicas es una materia netamente diferente del régimen de conservación. Dada su complejidad y lejanía con el objeto de nuestro estudio, estimamos

Regulado así el principal medio de injerencia en el derecho al secreto de las comunicaciones, los demás artículos se centran de reforzar las garantías de este derecho y el modo en que debe ser respetado por las compañías de telecomunicaciones en el desarrollo de sus actividades.

Así, la LGT extiende su preocupación por la privacidad a la regulación de las redes de comunicaciones electrónicas en el interior de los edificios[669] y a las condiciones para el cifrado en las redes y servicios de comunicaciones electrónicas[670]. Por su parte, el art. 35 LGT explicita las precauciones y garantías que han de observarse cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general. Entre las mismas, y a efectos de nuestra materia, hemos de destacar el hecho de que la norma establezca expresamente que cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan no pueden ser "ni almacenados ni divulgados" y deberán ser "inmediatamente destruidos"[671]. Así pues, resulta meridiano que la destrucción es el deber y principio conforme al cual los operadores deben actuar en caso de tener que acceder al contenido de las comunicaciones por motivos de mantenimiento técnico.

---

conveniente limitarnos a remitirnos a la lectura de la actual redacción del artículo 33 LGT, tras lo que el apartado uno de la Disposición Final Primera ha añadido.

[668] Como señala GONZÁLEZ LÓPEZ, la inclusión en un texto legal de la mayor parte de la regulación de la intervención de las comunicaciones contenida en el RLGT supone una indudable mejora en el aún deplorable panorama normativo español relativo a esta materia y, por tanto, un avance en la superación de la defectuosa técnica legislativa que ha sido objeto de reproche por parte de la doctrina". Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 33. Al respecto también, Cabezudo Rodríguez, N., "La Administración de Justicia ante las nuevas tecnologías. Del entusiasmo a la desconfianza, pasando por el olvido", Revista Jurídica de Castilla y León, n. 7, octubre 2005, p.188.
Por el contrario, la regulación en el indicado reglamento de los requisitos operacionales y técnicos para el cumplimiento por los operadores de las resoluciones judiciales que ordenen la intervención de las comunicaciones fue considerado correcto por RODRÍGUEZ LAINZ. Cf. Rodríguez Lainz, J.L., "Identificación... (y II)", op. cit., p.1.

[669] Cf. art. 37 LGT.

[670] Cf. art. 36 LGT.

[671] Cf. art. 35.1.b) LGT.

El cuidado con que el legislador español ha venido proveyendo al secreto de las comunicaciones en favor de los usuarios de las telecomunicaciones se manifiesta aún con mayor elocuencia en el art. 38 LGT que, sin perjuicio de todo lo dispuesto en la Ley 26/1984, de 19 de julio, *General para la Defensa de los Consumidores y Usuarios*[672], reconoce una serie de derechos de los consumidores y usuarios finales de estos servicios[673].

De la extensa regulación contenida en este art. 38 LGT, se deduce el derecho del abonado a decidir y disponer como desee acerca del uso y destino de los datos de tráficos que generen sus comunicaciones, lo que, por una parte, no es más que una consecuencia de los derechos tanto al secreto de las comunicaciones como a la protección de datos, y por otra y simultáneamente, se traduce en un principio general consistente en el derecho de los abonados a los servicios de comunicaciones electrónicas a que sus datos de tráfico no puedan ser accedidos, captados, conservados, mostrados ni tratados por parte de los operadores sin que medie su previo consentimiento informado. Este principio encuentra su concreción, por ejemplo, en el explícito derecho de los usuarios a que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación, tal como establece el art. 38.3.a) LGT. "Los datos de tráfico —se indica a renglón seguido— necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnacion de la factura del servicio o para que el operador pueda exigir su pago". Además, el principio se concreta en el derecho a que los datos de tráfico de los abonados sean utilizados con fines comerciales o para la prestación de servicios de valor añadido "únicamente cuando hubieran prestado su consentimiento informado para ello"[674], así como a recibir facturas no desglosadas cuando así se solicite[675]. Tampoco ha de pasar inadvertido el que las compañías no pueden legalmente proceder al

---

[672] Cf. art. 38.8 LGT.

[673] Sobre este régimen en nuestro Derecho, cf. Alenza García, J. F., et alii, Comentarios a las normas de protección de los consumidores (RDL 1/2007) y otras leyes y reglamentos vigentes en España y en la Unión Europea, Colex, Madrid, 2011.

[674] Cf. art. 38.3.b) LGT.

[675] Cf. art. 38.3.c) LGT.

tratamiento de los datos de localización distintos a los datos de tráfico salvo cuando se hayan hecho anónimos o previo consentimiento informado y —lo que es también relevante— "únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado"[676]. El art. 38.3 LGT también reconoce otros derechos que, básicamente, hacen visible el derecho del abonado a disponer como desee —y en la medida que sea técnicamente posible— de los datos de tráfico que generen sus comunicaciones como, por ejemplo, la potestad para el abonado de ocultar a terceros ciertos datos de tráfico. En concreto, nos referimos al derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada, o de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada[677].

Para mayor refuerzo del derecho a la protección de datos en el ámbito de las telecomunicaciones y de la LGT, dentro del conjunto de preceptos referido prevé su art. 34 la obligación para los operadores de garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal conforme a la legislación vigente —es decir, la LOPD y su desarrollo reglamentario—, adoptando las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, "con el fin de garantizar los niveles de protección de los datos de carácter personal que sean exigidos por la normativa de desarrollo de esta ley en esta materia".

De todo lo que acabamos de exponer se echa de ver cómo la entrada de la LCD en este marco regulatorio supuso la irrupción de una amplia e incisiva excepción a todas las previsiones que concretaban el meritado principio general de libre disposición de los datos por parte de los abonados. Ante la gravedad de la afectación[678], no es de extrañar que el legislador se viera obligado a añadir a través de la Disposición Final Primera,

---

[676] Cf. art. 38.3.d) LGT.

[677] Cf. art. 38.3.f) y g) LGT.

[678] Así como para mayor claridad en la integración de estas normas.

apartado segundo de la LCD, un nuevo párrafo al art. 38.5 LGT, que ahora advierte que lo establecido en las dichas letras —a) y d) del apartado 3— se entiende "sin perjuicio de las obligaciones establecidas en la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones"[679]. Este nuevo inciso vino además a sustituir a otro —dado por la redacción original— en virtud del cual lo dispuesto en el párrafo a) del apartado 3 se entendía sin perjuicio de lo dispuesto en el art. 12 LSSI. Este artículo —ahora derogado por el apart. 1 de la Disposición Derogatoria Única de la LCD[680]— nos sirve de pasarela entre esta breve exposición de la normativa sobre telecomunicaciones en el que se enmarca la LCD —que damos por concluida— y el del Derecho procesal penal, que abordaremos después.

27.2 El derogado artículo 12 LSSI

Con la entrada en vigor de la LSSI, su artículo 12 estableció por vez primera en el Derecho español un deber general de retención de datos de tráfico relativos a las comunicaciones electrónicas[681]. Conforme al mismo, los operadores de redes y

---

[679] Para hacer más exhaustiva nuestra exposición, debemos señalar que estos poderes de disposición del abonado respecto de sus datos de tráfico conocen otras excepciones por parte del art. 38.5. Así, el apartado indica que los usuarios finales no podrán ejercer los derechos reconocidos en los párrafos d) y f) del apartado 3 cuando se trate de llamadas efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen reglamentariamente, en especial a través del número 112. Del mismo modo, y por un período de tiempo limitado, los usuarios finales no podrán ejercer el derecho reconocido en el párrafo f) del apartado 3 cuando el abonado a la línea de destino haya solicitado la identificación de las llamadas maliciosas o molestas realizadas a su línea.

[680] El tenor literal del precepto dice así: "Disposición Derogatoria Única. Derogación normativa. 1. Quedan derogados los artículos 12, 38.2.c y d y 38.3.a de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. 2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley".

[681] El texto original de la norma, tal como fue publicada el 12 de julio de 2002, decía así:

"Artículo 12. Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.

1. 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 deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de

servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos debían retener por un período máximo de doce meses los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información[682] para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional[683]. La idea del legislador se asemejaba en muchos aspectos a la que finalmente consagró la LCD, pero se distanciaba en algunos aspectos importantes, como el hecho de que incluyera también a los prestadores de servicios de alojamiento de datos o el que los datos

---

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.

2. Los datos que, en cumplimiento de lo dispuesto en el apartado anterior, deberán conservar los operadores de redes y servicios de comunicaciones electrónicas y los proveedores de acceso a redes de telecomunicaciones serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.

Los prestadores de servicios de alojamiento de datos deberán retener sólo aquéllos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.

En ningún caso, la obligación de retención de datos afectará al secreto de las comunicaciones.

Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos.

3. Los datos se conservarán 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 los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales.

4. 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 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".

[682] Cf. art. 12.1 LSSI, ahora derogado.

[683] Cf. art. 12.3 LSSI, ahora derogado.

retenidos estuvieran a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requiriesen[684].

Como ya hemos dicho, los datos a retener ex art. 12.1 LSSI eran los de conexión y tráfico que se hubieran generado u originado en el transcurso de las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, siendo el período máximo de dicho almacenaje o retención de doce meses, y efectuándose el mismo bajo los términos y condiciones establecidos en la propia LSSI así como en la normativa futura que la desarrollase. El precepto detallaba que, si se trataba de operadores de redes y servicios de comunicaciones electrónicas o de proveedores de acceso a redes de telecomunicaciones, los datos a conservar serían exclusivamente aquellos necesarios en orden a la localización del equipo terminal empleado por el usuario para la transmisión de la información —entre ellos, sin duda, la IP del ordenador que usara dichos servicios—. Los prestadores de servicios de alojamiento de datos —como, vg., una empresa de *hosting*— habrían retener sólo aquéllos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio[685]. Estos datos se conservarían —indicaba el art. 12.3 LSSI— 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 cuando así los requiesen. Especificaba el mismo artículo que la comunicación de la información a las Fuerzas y Cuerpos de Seguridad se haría con sujeción a lo dispuesto en la normativa sobre protección de datos personales —esto es, la LOPD y su reglamento—.

Como límite a toda esta regulación, el art. 12.2 LSSI indicaba que en ningún caso, la obligación de retención de datos afectaría al secreto de las comunicaciones, así como que los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios no podrían utilizar los datos retenidos para fines distintos de

---

[684] Pueden hallarse comentarios a esta derogada norma en Maestre, J. A., y Sánchez-Almeida, C., La ley de internet: régimen jurídico de los servicios de la sociedad de la información y comercio electrónico, Servidoc, Madrid, 2002; López Sánchez, J. P., "Retención de datos en las comunicaciones electrónicas", en Economist & Jurist, Vol. 13, Nº 95, 2005, pp. 19 y ss.

[685] Cf. art. 12.2 LSSI, ahora derogado.

los indicados, u otros que estuvieran permitidos por la Ley, y deberían adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos.

En todo caso, la omisión del necesario desarrollo reglamentario —previsto en el art. 12.4 LSSI— en el que habían de detallarse extremos tan relevantes como las categorías de datos a conservar, el plazo de conservación para cada supuesto, o las condiciones de almacenamiento, custodia y cesión, hizo que todas estas previsiones permanecieran inaplicadas durante años hasta, finalmente, su derogación expresa por la LCD[686].

27.3 Marco procesal penal de la LCD

Una vez expuesto con concisión el marco regulatorio en el que la norma objeto de nuestro estudio se encuadró desde la perspectiva del Derecho de las telecomunicaciones, hemos de volver ahora nuestra mirada al Derecho procesal penal, que es el otro ámbito implicado en esta materia. Esta rama del Derecho es la que justifica la finalidad de la LCD, pues la obligación de conservar datos se ordena a su uso en la detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales[687].

Lo primero que debemos destacar es que el legislador español ha mostrado tradicionalmente cierta reticencia o falta de disposición en el establecimiento de una regulación pormenorizada de la injerencia sobre contenidos de las comunicaciones, incluso con anterioridad a la era digital. Antes de la aprobación del malogrado art. 12 LSSI, nuestro legislador se había limitado a dar una nueva redacción al art. 579

[686] Correlativamente, la Disposición Derogatoria Única de la LCD también derogó los arts. 38.2.c) y d) LSSI, que establecían como infracción muy grave de la LSSI "el incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12" y "la utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él".

[687] Cf. art. 1 LCD.

LECrim[688] a través de la Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal [689], para legalizar el régimen de la intervención de las comunicaciones telefónicas. Desde luego, nuestro país tampoco ha destacado en ser pionero en la regulación de los datos de tráfico o relativos a las comunicaciones electrónicas como posible fuente de investigación criminal. Y es que, como ha señalado RODRÍGUEZ LAINZ[690], España ha ido siempre a remolque bien de las iniciativas, bien de las imposiciones de la Unión Europea y su prolija regulación del sector de las telecomunicaciones, a pesar no obstante de haber tenido buenas oportunidades para ello, tales como la ratificación del Convenio 185 del Consejo de Europa sobre la cibercriminalidad, aprobado en Budapest el 23 de noviembre de 2001[691]. Al menos, eso sí, nuestro legislador ha sabido dar un amplio desarrollo a una legislación comunitaria muy preocupada por los riesgos del anonimato en las redes de telecomunicaciones y la potencialidad de ser instrumento idóneo para la realización de actividades criminales a través de la red.

---

[688] El artículo 579, en su redacción según Ley Orgánica 4/1988, de 25 de mayo, establece: "1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

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

4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación".

[689] Publicada en BOE núm. 126, de 26 de mayo de 1988.

[690] Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 15.

[691] Recientemente ratificado por el Estado español el 20 de mayo de 2010

Vale la pena recorrer los pasos que ha dado el legislador español hasta llegar al actual texto normativo objeto de nuestro estudio.

El antecedente más remoto en esta materia —aparte de la previsión en términos generales[692] de los arts. 8.2 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950, y 9.2 del Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal— ha de encontrarse sin duda en el art. 13.1 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de la que el art. 15.1, penúltimo inciso[693], de la Directiva 2002/58/CE, no es más que una derivación o consecuencia para evitar las extraordinarias trabas que podrían deducirse de la estricta aplicación de los principios de salvaguardia de la protección de la privacidad y la confidencialidad de las comunicaciones establecidos en esta última normativa[694]. Por tal motivo —reconoce el considerando undécimo de la citada Directiva—, se excluye del ámbito normativo de la Directiva la regulación interna de los Estados miembros de posibilidades de exceptuación de los derechos concretamente tutelados, sin más limitaciones que el sometimiento a los principios de protección de los Derechos Humanos, exigiendo, eso sí, el respeto del mandato del Convenio de Roma, la jurisprudencia emanada del Tribunal Europeo de Derechos Humanos y la garantía positiva de la protección de tales derechos impuesta por el art. 6 del Tratado de la Unión Europea.

---

[692] Citamos aquí normas europeas e internacionales pues ambas forman parte de nuestro ordenamiento interno: las primeras en virtud de nuestro compromiso comunitario; las segundas, tras cumplir los requisitos del art. 96 CE.

[693] "Los Estados miembros —dispone el precepto— podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos [de tráfico, se sobreentiende] se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado".

[694] Al respecto, cf. Poullet, Y., y Dinant, J. M., "Hacia nuevos principios de protección de datos en un nuevo entorno TIC", EN IDP: revista de Internet, derecho y política; revista d'Internet, dret i política, Nº. 5, 2007, pp. 33-46. Texto accesible en http://www.uoc.edu/idp/5/dt/esp/poullet_dinant.pdf.

El Convenio Europeo sobre Cibercriminalidad, por contra, apenas tuvo incidencia en la decisión del legislador de regular la obligación de retención de datos de tráfico a los efectos de su eventual utilización para finalidades públicas superiores. Su articulado establece deberes concretos de retención en el marco de investigaciones criminales singulares, en los que la retención se ordena por una autoridad estatal con competencia para ello, con eficacia *ex nunc*[695]. Los arts. 16 y 17 del mencionado Convenio regulan modalidades concretas de injerencia como son la conservación inmediata —*expedited preservation of stored computer data*— y conservación inmediata y revelación parcial de datos de tráfico trascendentales para la investigación —*expedited preservation and partial disclosure of traffic data*—, así como la interceptación, en tiempo real, tanto de datos de tráfico —*real-time collection of traffic data*— como de contenidos de comunicaciones —*interception on content data*— en los arts. 20 y 21. La única novedad que aportaba el Convenio de Budapest a este respecto era la distinción entre la retención de datos de tráfico o datos conservados en terminales informáticos previa a una injerencia sobre contenidos, o como técnica independiente de investigación, y la interceptación conjunta de comunicaciones y datos de tráfico asociados a las mismas[696]. La retención era entendida como una medida preambular de investigación en la que se interesaba del Estado requerido la actuación inmediata tendente a evitar que tan valiosa información pudiera perderse, bien por la acción fugaz del sujeto investigado, bien

[695] Acerca del Convenio sobre Cibercriminalidad y su impacto en nuestro Derecho, cf. Pavón Pérez, J. A., "La labor del Consejo en Europa en la lucha contra la cibercriminalidad. El protocolo adicional al convenio nº 185 sobre cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos", en Anuario de la Facultad de Derecho, Nº 21, 2003, pp. 187-204.

[696] Estas cuestiones y problemática relacionada han sido analizadas en Morón Lerma, E., y Rodríguez Puerta, M. J., "Traducción y breve comentario del convenio sobre cibercriminalidad", en Revista de derecho y proceso penal, Nº. 7, 2002, pp. 167-200; Díaz Gómez, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest", en "Revista electrónica del Departamento de Derecho de la Universidad de La Rioja", REDUR, Nº. 8, 2010, pp. 169-203.

porque tales datos no pudieran ser objeto de un lícito almacenamiento y ulterior utilización[697].

Finalmente, y como ya vimos en capítulos anteriores, la Unión Europea tomó el liderazgo legislativo en la materia hasta cristalizar sus esfuerzos en la Directiva 2006/24/CE, que adoptada el 15 de marzo de 2006, entró en vigor el 3 de mayo de ese mismo año —veinte días después de su publicación en el Boletín Oficial de la Unión Europea, el 13 de abril—. La norma debía ser transpuesta antes del 15 de septiembre de 2007, como disponía explícitamente su art. 15.1. España disponía por tanto del sensato plazo de dieciocho meses desde la adopción de la Directiva para implementarla en el ordenamiento nacional interno[698], pese a lo cual, llegó tarde al cumplimiento de tal plazo.

27.4 Tramitación de la LCD

En un primer momento, hay que reconocer que el Gobierno español actuó sin aparente demora para dar cumplimiento al mandato de la Directiva 2006/24/CE, teniendo preparado su Anteproyecto de Ley —ya intitulado "de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones"— en el mes de septiembre de 2006. El texto, en su versión fechada el 18 de diciembre de 2006,

---

[697] Eso sí, como reconoce LEZERTÚA, en los trabajos y negociaciones preliminares del Proyecto de Convenio sobre la Cibercriminalidad del Consejo de Europa, en las primeras versiones se llegó a discutir sobre la posibilidad del establecimiento de obligaciones de almacenamiento temporal de datos por parte de los prestadores de servicios. Sin embargo, en la larga negociación se acabó cediendo a la presión de las asociaciones de internautas y sobre todo de las entidades dedicadas a la fabricación de componentes informáticos o a la prestación de servicios de la denominada sociedad de la información, optándose por la línea de la actuación concreta antes apuntada. Cf. Lezertúa, M., "El Proyecto de Convenio sobre el Cybercrimen del Consejo de Europa"; en: Internet y Derecho Penal. Cuadernos de Derecho Judicial, Escuela Judicial-CGPJ. Madrid, 2001, pág. 55.

[698] Nuestro país no cumplió dicho plazo, dado que la Ley 25/2007, de 18 de octubre, llevó fecha de 18 de octubre, fue publicada al día siguiente y entró en vigor el 8 de noviembre de 2007. Se constata así un retraso de casi dos meses en la *puesta en vigor* —usando el lenguaje del art. 15.1 de la Directiva — de las disposiciones legales que dan cumplimiento a la Directiva.

constaba de una exposición de motivos, diez artículos divididos en tres capítulos, una disposición adicional, una disposición transitoria, una disposición derogatoria y cuatro disposiciones finales.

De acuerdo con lo dispuesto en el artículo 22 de la Ley 50/1997, de 27 de noviembre, del Gobierno[699], el Anteproyecto se acompañó de una memoria justificativa y de una memoria económica, así como de un informe sobre impacto por razón de género. También se recabó el parecer de diversas organizaciones y entidades del sector de las telecomunicaciones, directamente afectado por las medidas proyectadas, y emitieron informe el Consejo General del Poder Judicial y la Agencia Española de Protección de Datos. El Anteproyecto fue asimismo informado por la Secretaría General Técnica de los Ministerios de Justicia, del Interior y de Industria, Turismo y Comercio.

---

[699] Dispone el art. 22 —*De la iniciativa legislativa del Gobierno*— que:

"1. El Gobierno ejercerá la iniciativa legislativa prevista en los artículos 87 y 88 de la Constitución mediante la elaboración, aprobación y posterior remisión de los proyectos de Ley al Congreso de los Diputados o, en su caso, al Senado.

2. El procedimiento de elaboración de proyectos de ley a que se refiere el apartado anterior, se iniciará en el ministerio o ministerios competentes mediante la elaboración del correspondiente Anteproyecto, que irá acompañado por la memoria, los estudios o informes sobre la necesidad y oportunidad del mismo, un informe sobre el impacto por razón de género de las medidas que se establecen en el mismo, así como por una memoria económica que contenga la estimación del coste a que dará lugar. En todo caso, los Anteproyectos de ley habrán de ser informados por la Secretaría General Técnica.

3. El titular del Departamento proponente elevará el Anteproyecto al Consejo de Ministros a fin de que éste decida sobre los ulteriores trámites y, en particular, sobre las consultas, dictámenes e informes que resulten convenientes, así como sobre los términos de su realización, sin perjuicio de los legalmente preceptivos.

4. Una vez cumplidos los trámites a que se refiere el apartado anterior, el titular del Departamento proponente someterá el Anteproyecto, de nuevo, al Consejo de Ministros para su aprobación como Proyecto de Ley y su remisión al Congreso de los Diputados o, en su caso, al Senado, acompañándolo de una Exposición de Motivos y de la Memoria y demás antecedentes necesarios para pronunciarse sobre él.

5. Cuando razones de urgencia así lo aconsejen, el Consejo de Ministros podrá prescindir de los trámites contemplados en el apartado tercero de este artículo, salvo los que tengan carácter preceptivo, y acordar la aprobación de un Proyecto de Ley y su remisión al Congreso de los Diputados o, en su caso, al Senado.

La memoria justificativa elaborada por el Gobierno español ponía de manifiesto que con la ley proyectada se trataba de incorporar al ordenamiento jurídico interno la Directiva 2006/24/CE[700]. A partir de la necesidad de velar por la seguridad de los ciudadanos, en relación con el crecimiento de las posibilidades de las comunicaciones electrónicas, señalaba que el objeto de la norma proyectada era dotar a los miembros de los cuerpos policiales autorizados de mejores mecanismos para investigar la comisión de delitos —*sic*, la comisión de delitos en general—, mediante la obtención de los datos relativos a las comunicaciones relacionadas con la investigación. A tal efecto, se fijaban obligaciones de conservación de tales datos por parte de los operadores "buscando —explicitaba— el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones".

Añadía la memoria que la norma proyectada respetaba la jurisprudencia constitucional relativa al secreto de las comunicaciones, a través de dos garantías: en primer lugar, porque la obligación de conservación no alcanzaba a datos reveladores del contenido de las comunicaciones; y, segundo, porque la cesión de aquellos datos que afecten al secreto de las comunicaciones exigiría siempre una autorización judicial previa. Por otra parte —se decía— el legislador optaba por habilitar la cesión de estos datos para *cualquier tipo* de delito, "a fin de no privar a las autoridades judiciales de un mecanismo de investigación con el que actualmente cuenta, de acuerdo con la configuración constitucional del derecho al secreto de las comunicaciones".

Por su parte, la memoria económica que elaboró el Gobierno afirmaba que la aplicación de la proyectada ley supondría repercusiones económicas para la Administración Pública y los sujetos obligados. Así, en relación con la primera, sería necesaria la realización de un sistema informático para el almacenamiento y gestión, por parte de los agentes facultados, de la información recibida de los sujetos obligados, así como el establecimiento de canales de comunicación de datos con los mismos. Los costes totales en inversiones reales implicarían asimismo la implantación de dos sistemas informáticos gemelos para las Direcciones Generales de la Policía y de la Guardia

[700] Extraída del punto segundo de los Antecedentes del Dictamen del Consejo de Estado.

Civil, que se estimaban en 3.070.000 euros, y los gastos corrientes de mantenimiento de los sistemas supondrían, aproximadamente, el 12% de los gastos de inversión.

En cuanto a la incidencia económica sobre el sector, el Gobierno indicaba que los costes para los sujetos obligados eran de dos tipos: los relativos a adaptaciones técnicas en sus redes para el cumplimiento de las obligaciones de conservación y cesión de datos, y los referentes a actividades administrativas relacionadas con la gestión de las peticiones y la transmisión o entrega de la información solicitada a los agentes facultados. Tras apuntar que el problema se centraba en los primeros, la memoria se limitó a señalar que se "tendría en consideración la necesaria proporción entre los objetivos a conseguir y los costes en que se incurra".

Por último, el informe sobre impacto por razón de género señalaba escuetamente que el Anteproyecto "no afecta[ba] a la igualdad entre hombres y mujeres".

Frente a estas memorias del Gobierno y sus órganos, resulta de mayor interés las aportaciones realizadas por los órganos de Estado dictaminantes. De este modo, y de conformidad con lo dispuesto en el art. 108.1.e) de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial[701], el Pleno del Consejo General del Poder Judicial aprobó

---

[701] Cf. Artículo 108 (redacción según Ley Orgánica 16/1994, de 8 de Noviembre): "1. El Consejo General del Poder Judicial deberá informar los Anteproyectos de leyes y disposiciones generales del Estado y de las Comunidades Autónomas que afecten total o parcialmente a alguna de las siguientes materias:

a) Determinación y modificación de demarcaciones judiciales y de su capitalidad en los términos del artículo 35 de esta Ley.
b) Fijación y modificación de la plantilla orgánica de Jueces, Magistrados, secretarios y personal que preste servicios en la Administración de Justicia.
c) Estatuto Orgánico de Jueces y Magistrados.
d) Estatuto Orgánico de los secretarios y del resto del personal al servicio de la administración de justicia.
e) Normas procesales o que afecten a aspectos jurídico-constitucionales de la tutela ante los Tribunales ordinarios del ejercicio de Derechos Fundamentales y cualesquiera otras que afecten a la constitución, organización, funcionamiento y gobierno de los Juzgados y Tribunales.
f) Leyes Penales y Normas sobre Régimen Penitenciario.
g) Aquellas otras que le atribuyan las Leyes.

informe el 18 de octubre de 2006 sobre el texto del *Anteproyecto de Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*[702]. El Informe se abría con unas consideraciones sobre los antecedentes, sobre su función consultiva y sobre la estructura y contenido del Anteproyecto. A continuación exponía unas consideraciones generales sobre el fundamento normativo comunitario del texto sometido a consulta y, en particular, sobre el derecho al anonimato y a la confidencialidad en relación con los datos personales generados y tratados en los procesos de comunicación por medios electrónicos, y sobre las nuevas obligaciones de los operadores de servicios de comunicaciones electrónicas —conservación de datos y cesión—.

Las consideraciones particulares sobre el texto proyectado se referían, en primer lugar, a diversos elementos de la obligación de retención de datos —delimitación objetiva y subjetiva, duración, destinatarios y seguridad—. Se sugería asimismo la sustitución de la expresión "agentes facultados", terminología que no se corresponde con nuestro ordenamiento procesal ni sectorial sobre seguridad pública, a lo que se añadía que los "agentes facultados" no debían ser quienes formularan el requerimiento correspondiente, sino los destinatarios de los datos, mientras que la orden de entrega debía provenir de la autoridad judicial que autorizaba su cesión. Tras manifestar su conformidad y la correcta incorporación que reflejaban otros artículos del Anteproyecto, sugería que se aclarase, en el artículo 6, que la referencia a la Policía Judicial debía comprender no sólo a los miembros de las unidades orgánicas de Policía Judicial, sino también a los agentes de las Fuerzas y Cuerpos de Seguridad del Estado

---

2. El Consejo General del Poder Judicial emitirá el informe en el plazo de treinta días. Cuando en la orden de remisión se haga constar la urgencia del informe, el plazo será de quince días.

3. El Gobierno remitirá dicho informe a las Cortes Generales en el caso de tratarse de Anteproyectos de Leyes.

4. El Consejo General será oído con carácter previo al nombramiento del Fiscal General del Estado".

[702] El texto del Anteproyecto tuvo entrada en el Registro del Consejo General del Poder Judicial con fecha 20 de septiembre de 2006. La Comisión de Estudios e Informes, en su sesión del día 28 de septiembre de 2006, designó Ponente al Excmo. Señor D. Luis Aguiar de Luque y acordó solicitar prórroga del plazo de urgencia inicialmente concedido, y en su reunión de fecha 11 de octubre de 2006, aprobó el presente informe, acordando su remisión al Pleno del Consejo General del Poder Judicial. (cf. *Antecedentes*, Informe)

que, sin participar de dicho encuadramiento orgánico, ejercen funciones de Policía Judicial.

En segundo término, en cuanto al procedimiento de cesión y la exigencia de autorización judicial previa, se ponía de manifiesto por el CGPJ cómo, en la jurisprudencia constitucional, "no sólo es secreto el contenido del mensaje comunicado, sino también aquellos datos que configuran la comunicación en su vertiente externa", por lo que se estimaba acertada la exigencia de autorización judicial para ceder, a los agentes de la Policía Judicial o del CNI, los datos de tráfico y los datos de localización generados y tratados por los operadores del servicio y de la red. Sin embargo, el Consejo criticaba que el artículo 7 del Anteproyecto exigiera que la autorización judicial hubiera de concretarse en una comunicación o comunicaciones determinadas —puesto que, en muchos casos, no podría determinarse de antemano qué comunicaciones de las entabladas por el imputado pueden tener relevancia para el buen fin de la instrucción—; se prefería, por ello, que la norma hiciera una remisión a lo previsto en la Ley de Enjuiciamiento Criminal. Concluía el Informe valorando favorablemente el régimen transitorio y de derogaciones expresas[703].

Por su parte, la Agencia Española de Protección de Datos emitió informe sobre el texto del Anteproyecto con fecha 30 de octubre de 2006. El documento comenzaba con una referencia a las normas comunitarias y nacionales relativas a la materia afectada por el Anteproyecto. En cuanto a su contenido, consideraba que el artículo 1 debía limitar su objeto en relación con los supuestos de investigación, detección y enjuiciamiento de delitos "graves", tal y como hace la Directiva 2006/24/CE, y teniendo en cuenta que el Tribunal Constitucional exige la gravedad del delito como presupuesto objetivo para la adopción de medidas que afectan al secreto de las comunicaciones. El hecho de que el Código Penal no contemple una categoría especial de delitos calificados como graves —añadía— no impedía que la gravedad del delito pueda ser analizada en cada supuesto

[703] En lo relativo al registro de los titulares de tarjetas prepago, entendía el órgano de gobierno del Poder Judicial que, siendo el registro de estos datos previo a la activación del teléfono o terminal móvil, su cesión no precisaba verse sometida al régimen más riguroso de licencia judicial previa, lo que debería explicitarse; otra cosa es que, activada la tarjeta, se aplicara el régimen general de la ley para los datos de tráfico y localización que se generasen y tratasen a partir de ese momento.

concreto. El resto de las disposiciones del Capítulo I eran a su entender fiel reflejo de lo establecido en la Directiva.

La Agencia también consideraba conformes a la Directiva los artículos 4 y 5.1, y proponía una nueva redacción del artículo 5.2 y del artículo 6 —en ambos casos, por razones de mayor claridad—, indicando que lo dispuesto en el Anteproyecto había de entenderse sin perjuicio de las habilitaciones legales para la comunicación de los datos regulados por el Anteproyecto a otros órganos u organismos, al amparo del artículo 11.2.a) LOPD. Sugería un cambio de redacción en el artículo 7 y, en relación con el artículo 8 —sobre protección y seguridad de los datos—, señalaba que las obligaciones exigidas por el artículo 7 de la Directiva aparecían expresamente recogidas en la Ley Orgánica 15/1999 y sus normas de desarrollo. Al resultar aplicable dicha ley orgánica en cuanto a los restantes principios reguladores del derecho fundamental a la protección de datos de carácter personal, se ponía de manifiesto que una remisión parcial como la contenida en los tres primeros apartados del artículo 8 podría inducir a la confusión de considerar que aquella ley orgánica era aplicable únicamente en los supuestos mencionados en esos tres apartados. Proponía, de acuerdo con ello, una redacción alternativa[704].

El Informe de la AEPD terminaba señalando, en relación con la Disposición Final Primera, que sería más lógico incluir la regla propuesta como art. 38.9 LGT en el

---

[704] Sobre la Disposición Adicional Única, exponía la AEPD que la exigencia de identificación de los titulares de las tarjetas de prepago estaba recogida en las legislaciones de otros Estados europeos y que no podía considerarse que el tratamiento de estos datos fuera contrario al principio de proporcionalidad previsto en el artículo 4.1 de la Ley Orgánica 15/1999; ahora bien —añadía— la llevanza del libro-registro previsto supondría un tratamiento de datos que en todo punto debía resultar conforme a lo dispuesto en la citada ley. En cuanto al mantenimiento del régimen allí previsto desde la fecha de activación de la tarjeta y durante la vigencia de la misma, la Agencia llamaba la atención sobre el hecho de que los datos generados en el año siguiente a la desactivación no aparecerían vinculados al adquirente; por ello —indicaba—, si la voluntad del precepto es distinta, debía aclararse —y, en concreto, debía determinarse cuál sería el plazo de conservación de los datos en el libro-registro para su comunicación a los agentes facultados—. Proponía asimismo aclarar que la obligación de llevanza del libro-registro únicamente resultaría exigible respecto de quienes adquieran las tarjetas con posterioridad a la fecha en que sea exigible la llevanza. A partir de todo ello, proponía una nueva redacción de la Disposición Adicional Única.

apartado 5 del precepto, que se refiere a las especialidades en la aplicación del régimen previsto en al artículo 38.3 LGT.

Asimismo, durante la tramitación de la LCD, diversas asociaciones y empresas del sector de las telecomunicaciones, directamente afectadas por el contenido de la proyectada ley, presentaron escritos de alegaciones a la misma, que fueron incorporadas al expediente[705]. Dado su número, intentaremos exponer su contenido con la mayor concisión.

En primer lugar, Vodafone España, S. A. elaboró una nota en la que manifestaba que el plazo de veinticuatro horas para la entrega de la información, previsto en el artículo 7.3, era demasiado ajustado, dado el volumen de datos que había que manejar. Proponía así un plazo de entrega de cuarenta y ocho horas para datos relativos a los últimos tres meses y de setenta y dos horas para datos de una antigüedad superior a nueve meses. Manifestaba asimismo reservas sobre los términos de la Disposición Final Cuarta. Por una parte, se preguntaba cuándo se iba producir el desarrollo por orden ministerial allí previsto, y proponía que el plazo de seis meses para adaptarse a la ley se modificara para que los seis meses empezaran a contar a partir de la publicación de las órdenes ministeriales de desarrollo —puesto que dependían de ese desarrollo para la puesta en marcha de su sistema—; por otra, mostraba su preocupación por el hecho de que el sistema de entrega fuera diferente según el agente facultado perteneciera al Ministerio del Interior o al Ministerio de Defensa[706].

Por su parte, Ono, S.A.U. y la Asociación de Operadores de Cable presentaron escrito de alegaciones, en el que señalaban la necesidad de que se detallasen con claridad, y de forma homogénea a lo largo del texto, los agentes facultados para solicitar los datos, incluyendo la exigencia de autorización previa en todos los casos; subrayaba la importancia de establecer un plazo mínimo de ejecución de las órdenes judiciales de

---

[705] A su contenido nos referimos a través de lo expuesto en el punto quinto de los Antecedentes del Dictamen del Consejo de Estado.

[706] En cuanto a la Disposición Adicional Única, se apuntaba la falta de especificación del formato del libro-registro, y se llamaba la atención sobre el hecho de que para la entrega bastara requerimiento del agente facultado, sin especificar dónde se iba a solicitar la información, sugiriendo que hubiera un único punto de contacto entre la empresa y los agentes facultados.

cesión de cuarenta y ocho o setenta y dos horas, según que la antigüedad de los datos fuera inferior o superior a tres meses —plazos que podrían ser ampliados por la orden judicial correspondiente—; apuntaba que el Anteproyecto se extralimitaba en su objeto al extenderse más allá de los supuestos de delitos graves a que se refiere la directiva de cuya incorporación se trataba; consideraba que debían aclararse algunas cuestiones sobre los datos objetos de conservación y sobre los conceptos de "llamada infructuosa" y de "llamada no conectada". Entendía asimismo que el plazo de conservación de los datos que se fijara en la ley debía ser objetivo e inamovible, excluyéndose la posibilidad de modificación posterior; en concreto, proponía un plazo de doce meses para la conservación de datos relativos a servicios de internet y un plazo de seis meses para servicios de voz. Por último, indicaba que el plazo de seis meses de adecuación a las obligaciones establecidas en la ley debía estar condicionada a la entrada en vigor de las órdenes ministeriales que la desarrollaran, previstas en la Disposición Final Cuarta.

Otro de los escritos de alegaciones al que hemos de referirnos es el presentado por la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC), que comenzaba sus observaciones con una referencia a los antecedentes y a la constitucionalidad de la norma proyectada, si bien consideraba que debía incorporarse, de forma expresa y para todos los casos de cesión a un agente facultado, la exigencia de autorización judicial, y que había de recabarse informe de la Agencia Española de Protección de Datos. Proponía suprimir las distintas referencias a la responsabilidad penal en que podían incurrir los operadores, y que el coste del cumplimiento de la ley no se dejara a las exclusivas expensas de los operadores. En este sentido, sugería la creación de un "fondo nacional de ayuda a la conservación de datos de las comunicaciones electrónicas". Planteaba igualmente una nueva redacción de la Disposición Final Tercera a fin de que la ampliación del plazo de conservación de datos no quedara a la absoluta discrecionalidad del Gobierno, como también que el plazo de entrega se fijase, con carácter general, en tres días —sin perjuicio de que la autorización judicial pudiera fijar uno distinto, no inferior a un día—. Aludía también a los problemas que podría suscitar la entrada en vigor de la ley que, decía, debería producirse a los seis meses de su publicación, si bien se añadía que "lo más problemático [...] se halla[ba] en la obligación de efectuar la cesión de datos en dos formatos electrónicos distintos, según convenga al Ministerio del Interior o al Ministerio de Defensa".

Por su parte, Telefónica, en las observaciones que formuló, distinguió entre unos comentarios generales más relevantes y unos comentarios específicos a diferentes artículos. Entre los primeros incluyó su disponibilidad a prestar toda la colaboración precisa unida a la aspiración de que fuera la Administración la que asumiera todos los costes que ello supondría. También consideraba que el plazo de conservación de datos debía limitarse a seis meses y que el de entrega de los datos no podía fijarse, con carácter general, en veinticuatro horas, lo que consideraba inasumible técnica y organizativamente, sugiriendo que se exigiera la entrega "en el menor plazo de tiempo posible". En cuanto a la obligación de conservar los datos de llamadas infructuosas, proponía que alcanzara exclusivamente a aquellas cuyos datos fueran actualmente guardados para la prestación de un servicio por los operadores. Entre los comentarios específicos, se criticaba que no se limitara la ley a los supuestos de delitos "graves" —como hacía la Directiva objeto de incorporación—, que se evitase la exigencia de conservar los datos cedidos de forma indefinida, que se trasladara a la Disposición Adicional Única la concreta y estricta definición de "agente facultado" contenida en el artículo 6, la unificación del régimen sancionador en el establecido en la LGT y de las competencias sancionadoras en el Ministerio de Industria[707]. Terminaba proponiendo que se incluyera en el texto de la ley un artículo con definiciones o una remisión a la Directiva.

Finalmente, el último de los escritos de alegaciones a los que hemos de hacer mención es el de la Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España, quien en sus observaciones generales apuntaba que la posible incidencia de la norma proyectada en el derecho fundamental a la intimidad aconsejaba su tramitación como ley orgánica y manifestaba su inquietud por el impacto financiero que la industria afectada pudiera tener que soportar como consecuencia de

[707] Añadía, respecto de los servicios de telefonía tarjetas de prepago, que debía suprimirse la obligación de llevar un libro-registro en el que constara la identidad de los clientes de tarjetas prepago y veía razonable que se ampliara a dieciocho meses el plazo que se establecía para que los operadores estuvieran en disposición de cumplir las obligaciones previstas en la ley. Insistía, por otra parte, en que la petición de los datos de identificación del titular de una tarjeta prepago con origen en una comunicación —listado de llamadas— estaba protegido por el secreto de las comunicaciones, por lo que el requerimiento de información debería realizarse mediante mandamiento judicial.

ella. Entendía asimismo que el Anteproyecto debía rediseñar las obligaciones de los operadores realizando un análisis coste-beneficio y calibrando de forma precisa la eficacia de unas medidas muy costosas de implementar, a lo que se añadía la propuesta de que se incluyera una mención explícita a los mecanismos de reembolso asociados a las nuevas obligaciones y la sugerencia de que se incorporase al texto un anexo con definiciones. A continuación se formulaban observaciones al articulado y, entre ellas, que se limitase el ámbito de aplicación al acordado en el ámbito comunitario, ceñido a los delitos graves, que se aplicase el aludido análisis coste-beneficio —en particular, en relación con las llamadas infructuosas y con el período de conservación de los datos—, que se restringiera el ámbito de los agentes facultados mediante la exigencia, en todo caso, de autorización judicial, cohonestando las previsiones del artículo 6 y de la Disposición Adicional Única, como también las de los artículos 8 y 9, y que el plazo de entrega se extendiera hasta las cuarenta y ocho o setenta y dos horas en función de la antigüedad de los datos[708]. Sobre la Disposición Adicional Cuarta se preguntaba cuándo se iba a producir el desarrollo mediante orden ministerial allí previsto y cuál iba a ser la vinculación de esa fecha a la entrada en vigor de la ley —lo que tenía especial importancia para desarrollar los sistemas internos—, proponiendo que el sistema de entrega fuera común para los agentes facultados, a fin de evitar mayores costes y agilizar su implementación. Terminaba el documento proponiendo que fueran los responsables del requerimiento del servicio los que asumieran su coste.

Una vez expuestas las alegaciones, dictámenes e informes presentados por instituciones y particulares, el principal y sin duda más determinante documento en la tramitación de la LCD, fue —como no puede ser de otra manera— el Dictamen del Consejo de Estado[709]. El 22 de febrero de 2007 la multisecular institución aprobó su *Dictamen sobre el Anteproyecto de Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones* —n. expediente 32/2007—, que formulado de conformidad con lo dispuesto en el artículo 21.2 de la Ley Orgánica

[708] En relación con la Disposición Adicional Única, se afirmaba que se trataba de una medida enormemente costosa para los operadores, pero de dudosa eficacia, y se apuntaban algunas imprecisiones que convenía aclarar.

[709] Disponible en: http://www.boe.es/aeboe/consultas/bases_datos_ce/doc.php?coleccion=ce&id=2007-32

3/1980, de 22 de abril, del Consejo de Estado, impone la consulta dicho órgano en pleno en relación con los Anteproyectos de leyes que hayan de dictarse en ejecución, cumplimiento o desarrollo de tratados, convenios o acuerdos internacionales y del derecho comunitario europeo[710]. La relevancia e impacto de dicho Dictamen en la ley en estudio aconsejan, en pro de una mejor sistematicidad y claridad expositiva, que distribuyamos la explicación de su contenido a lo largo de nuestro análisis sobre el articulado de la Ley.

Así pues, finalmente, precluidas todas estas fases preparatorias, la tramitación legislativa del Proyecto dio comienzo en el Congreso de los Diputados mediante su presentación por parte del Gobierno el 16 de marzo

de 2007. La tramitación parlamentaria como Proyecto de Ley 121/000128, que se preveía casi rutinaria, experimentó sin embargo los avatares de un imprevisto interés parlamentario sobre la materia, que condujeron a importantes cambios sobre el proyecto inicial, en aspectos tales como la elevación a rango normativo de ley de las previsiones que ya se contenían en el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el *Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, sobre el deber de colaboración de operadores concernidos en materia de interceptación legal de comunicaciones, la consolidación de la normativa específica sobre registro de adquisición de tarjetas telefónicas de prepago*[711], que viera ya la luz en el Proyecto de Ley presentado a las Cortes, y sobre todo, la opción por la determinación de los delitos que podrían ser investigados aprovechando la información

---

[710] De conformidad con la redacción dada por la Ley Orgánica 3/2004, de 28 de diciembre

[711] Cf. Mendoza Losana, A. I., "El nuevo Reglamento del servicio universal de telecomunicaciones: análisis de las novedades introducidas por RD 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios", en Estudios sobre telecomunicaciones y derecho de consumo (coord. por Angel Carrasco Perera), Aranzadi, 2005, págs. 265-306; y Zoco Zabala, C., "Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de SITEL con el artículo 18.3 CE", en Indret: Revista para el Análisis del Derecho, , Nº. 4, 2010, p. 17, disponible en http://www.indret.com/pdf/781_es.pdf

almacenada, asumiendo finalmente el concepto de delito grave por el que aboga la Directiva[712].

Tras pasar por el trámite de enmiendas —setenta y siete fueron las presentadas por los diferentes grupos parlamentarios—, se aprobó un texto el 21 de junio de 2007. A continuación tuvo lugar la tramitación del proyecto legislativo ante el Senado, que aprobó el texto el 2 de octubre, también tras su correspondiente trámite de enmiendas. La norma fue finalmente votada por el Congreso de los Diputados en sesión plenaria de 4 de octubre y publicada en el Boletín Oficial del Estado el 19 de octubre de 2007.

Transcurrido el plazo común de los veinte días de *vacatio legis*[713], la LCD entró en vigor el 8 de noviembre de 2007. Al transponer la Directiva 2006/24/CE, la norma previó tanto la derogación de los arts. 12, 38.2 c) y d) y 38.3 a) LSSI —ya comentada[714]— como la modificación de los arts. 33, 38.5, 53 y 54 LGT —en los términos que expondremos más adelante—.

Accesoriamente, ha de indicarse que la Disposición Final Segunda clarifica la competencia estatal en la materia, al disponer que "esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones"[715]. Por su parte, la Disposición Final Tercera —desarrollo reglamentario—, habilita al Gobierno a

---

[712] Señala RODRÍGUEZ LAINZ que "la nueva ley supuso, no obstante, que el art. 12 de la LSSICE no llegara a ver la luz en cuanto a su normatividad, al ser derogada, antes de que su necesario desarrollo reglamentario tuviera lugar, por mandato de la Disp. Derogatoria única, parágrafo primero de la LCDCE". Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 8.

[713] Cf. art. 5 del Código Civil.

[714] De conformidad con la Disposición Derogatoria Única: "1. Quedan derogados los artículos 12, 38.2 c) y d) y 38.3 a) de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. 2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley".

[715] Según su tenor literal: "Disposición final segunda. Competencia estatal. Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21.ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones".

dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en la propia Ley[716].

Entrando a valorar todo el proceso que acabamos de describir y, en general, la transposición del contenido de la Directiva 2006/24/CE por parte del legislador español, podemos afirmar que la misma fue llevada a cabo por parte del Gobierno sin el cuidado y precisión necesarios. Esta falta ya fue puesta de manifiesto en varias ocasiones en el Dictamen del Consejo de Estado, que reprochó al Gobierno ciertas omisiones en la preparación del borrador. Así, por ejemplo, en el expediente del Anteproyecto se acompañaron "alegaciones presentadas por el sector" pero no figuraban la totalidad de las que habían sido consultadas, si bien constaba que dicho Anteproyecto había sido objeto de una reunión en el seno del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información y que se había concedido un plazo para que las organizaciones o entidades allí representadas pudieran remitir observaciones sobre su contenido[717]. Tampoco se dejaron constancia en el expediente de las razones que llevaron al órgano instructor a aceptar o rechazar en cada caso las propuestas, sugerencias y observaciones formuladas por los distintos órganos y entidades que habían emitido su parecer sobre el Anteproyecto, a lo que se añadía la ausencia del texto o textos sobre los que han informado aquellos —esto es, las versiones anteriores de la norma proyectada[718]—. El Consejo de Estado no dejó de insistir[719] en la conveniencia, "cuando no necesidad, de que quede constancia de tales razones en este tipo de expedientes; ha de tenerse en cuenta la virtualidad que ello puede tener para los ulteriores informes y, sobre todo que, una vez aprobado como proyecto de Ley, ha de ser remitido a las Cortes Generales, acompañando los "antecedentes necesarios para pronunciarse sobre él (artículo 22.4 de la Ley del Gobierno)"[720].

---

[716] El texto dice así: "Disposición final tercera. Desarrollo reglamentario. Se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley".

[717] Apartado I, Dictamen del Consejo de Estado.

[718] Ibíd.

[719] Como ya ha hecho en otras ocasiones; por ejemplo, en el Dictamen 2467/2006, de 21 de diciembre.

[720] Ibíd.

Estas ausencias resultan especialmente graves y perjudiciales en un caso como el que ocupa nuestro examen, en el que la memoria justificativa se limitó a hacer una rápida referencia, de carácter general, a la necesidad y oportunidad del Anteproyecto, en función de la necesaria incorporación de la Directiva 2006/24/CE, añadiendo una exposición de su estructura y contenido pero sin detenerse a explicar —siquiera en relación con las cuestiones más relevantes o más debatidas— las razones que llevaron a adoptar una concreta solución frente a otras posibles o de las que se han propuesto en los distintos informes incorporados al expediente.

Directamente relacionado con lo anterior, llama la atención la ausencia de datos relativos a los efectos económicos que las medidas previstas habían de tener sobre los sujetos obligados y que, en definitiva, han sido evidentemente repercutidos sobre todos los usuarios. Como ya vimos, aunque en la memoria económica se incluyó un tercer epígrafe sobre la "incidencia económica sobre el sector", su contenido se reducía prácticamente a distinguir entre los costes de adaptaciones técnicas y los de actividades administrativas —sin cuantificar unos ni otros— y a concluir que se tendría "en consideración la necesaria proporción entre los objetivos a conseguir y los costes en que se incurra". En este sentido, en distintos escritos de alegaciones u observaciones se plantearon —y así lo hemos hecho constar— alternativas en relación con la configuración legal de algunas de las medidas previstas —plazos de conservación, plazos de entrega, medidas sobre tarjetas prepago, sobre "llamadas infructuosas", etc.—, aludiendo a los elevados costes que suponían algunas exigencias previstas en el Anteproyecto, y no impuestas por la norma comunitaria, o a las diferencias de coste, en función de la concreta configuración legal, de algunas de las medidas previstas, en las que cuantiosas inversiones tendrían una escasa utilidad marginal.

A este respecto, es claro que para que las Cortes Generales pudieran haber tenido en cuenta la proporción que existe entre una determinada exigencia y el coste que habría de tener para los sujetos obligados —con eventual repercusión en los usuarios finales—, el máximo representante del pueblo español[721] debería haber contado con una información económica más detallada. Tal negligencia ha repercutido sin duda alguna

[721] En palabras del art. 66.1 CE.

en la calidad de la Ley 25/2007, de 18 de octubre, y en el equilibrio, prudencia y acierto de sus disposiciones.

Finalmente, hemos de señalar que la Directiva fue adoptada el 15 de marzo de 2006, entró en vigor el 3 de mayo de ese mismo año —veinte días después de su publicación en el Boletín Oficial del Estado el 13 de abril[722]— y debía ser transpuesta antes del 15 de septiembre de 2007, pues así lo disponía explícitamente su art. 15.1[723]. España disponía de dieciocho meses desde la adopción de la Directiva para implementarla en el ordenamiento nacional. Sin embargo, nuestro país no cumplió dicho plazo, dado que la Ley 25/2007, de 18 de octubre, llevó fecha de 18 de octubre, fue publicada al día siguiente y entró en vigor el 8 de noviembre de 2007. Se constata así un retraso de casi dos meses en la "puesta en vigor" —usando el tenor literal del art. 15.1 de la Directiva[724]— de las disposiciones legales que dan cumplimiento a la norma europea.

Concluida con estas explicaciones la presentación de los antecedentes, tramitación y marco legislativo de la norma objeto de este estudio, sólo nos cabe proceder a valorar con el mayor detalle posible el contenido de su articulado.

28 Objeto de la ley

28.1 Presentación del objeto de la Ley

Obviamente, la LCD nace de la necesidad de incorporación de la DCD, "cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley" —afirma su Preámbulo[725]—. El adjetivo "principal" es aquí relevante pues, como ya observara GONZÁLEZ LÓPEZ, el alcance de la norma no se limita a dicha

[722] Cf. Diario Oficial de la Unión Europea, L105, de 13 de abril de 2006, páginas L105/54 a L105/63.

[723] De acuerdo con su tenor literal, "los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar el 15 de septiembre de 2007". Cf. art. 15.1 Directiva 2006/24/CE.

[724] Ibíd.

[725] Cf. Exposición de Motivos, apart. I, doc. cit.

transposición[726]. Por un lado, junto a la regulación de la conservación generalizada de datos relativos a las comunicaciones electrónicas, la LCD se ocupa también del procedimiento de su cesión[727] y crea un régimen especial —sin base en la DCD— para los servicios de telefonía mediante tarjetas de prepago[728]. Por otro, la Ley también realiza diversas modificaciones de la LGT. Como ha señalado el mismo autor[729], esta reforma no sólo adapta dicha ley general a la LCD, sino que incorpora a aquélla previsiones referentes a la intervención de las comunicaciones con anterioridad ya presentes en el RLGT, elevando su contenido a rango de ley, lo que resulta más conveniente dado que el mismo conecta directamente con el derecho fundamental del art. 18 CE.

Volviendo nuestra atención sobre el articulado, el artículo 1 de la LCD —formado por tres apartados agrupados bajo la rúbrica "objeto de la Ley"— se ocupa de definir el propósito de la norma transpuesta, indicando que la misma tiene por objetivo la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales[730]. Por su parte, la Exposición de Motivos identifica como objeto de la norma "la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados". Si bien el texto habla de "retener", el art. 1.1 LCD usa más correctamente el término "conservar", referido a una conservación generalizada de datos ya tratados, que es una modalidad diferente de la "retención" en el sentido que le atribuye el Consejo de Europa en el Convenio sobre Cibercriminalidad como "obtención en tiempo

[726] Cf. González López, J. L., Comentarios a la Ley 25/2007…, op. cit., p. 2.

[727] Cf. arts. 6 y 7 LCD.

[728] Cf. Disp. Adic. Única, LCD.

[729] Cf. González López, J. L., Comentarios a la Ley 25/2007…, op. cit., pp. 2 y 3.

[730] Cf. art. 1.1 LCD.

real de ciertas categorías de datos", y que se distingue a su vez de la "preservación", que es la "conservación particularizada de datos ya tratados"[731].

Asimismo, aclara el art. 1.2 LCD que la Ley se aplica "a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado", términos con los que la norma viene a disponer el sometimiento a la LCD tanto de las comunicaciones electrónicas realizadas por los particulares —sean personas físicas, empresas, instituciones, etc—, como de las Administraciones Públicas. En este sentido, el art. 1.2 de la LCD no hace sino transcribir, casi literalmente, el contenido del art. 1.2 de la Directiva[732].

El apartado tercero y último excluye expresamente del ámbito de aplicación de la LCD "el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas"[733], reflejo fiel del inciso final del art. 1.2 de la Directiva.

Así pues, el tipo de medida ante la que nos hallamos viene a configurarse como lo que se ha dado en denominar técnicamente como "conservación generalizada de datos". PÉREZ GIL la describe como aquella que opera cuando la comisión delictiva es meramente hipotética y no consta sospecha inicial ni indicio alguno, de manera que lo que se trata es de "congelar" datos que, una vez archivados, podrán ser elevados a la categoría de fuentes de prueba "aunque eso suceda únicamente en un porcentaje infinitesimal de ocasiones"[734]. En aguda observación del mismo autor, tal tipo de

---

[731] Acerca de esta distinción, González López, J. J., "Retención de datos de tráfico de las telecomunicaciones y proceso penal", en VV.AA., Estudios jurídicos sobre la Sociedad de la Información y nuevas tecnologías. Libro con motivo del XX Aniversario de la Facultad de Derecho, Servicio de Publicaciones de la Universidad de Burgos. Burgos 2005, pp. 375-394.

[732] Dispone el precepto que "la presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas".

[733] Cf. art. 1.3 LCD.

[734] Cf. Pérez Gil, J., "Entre los hechos y la prueba: reflexiones acerca de la adquisición probatoria en el proceso penal", Revista jurídica de Castilla y León, n.º14, enero 2008, p.234. Citado por González López, J. J., en Comentarios a la Ley 25/2007…, p. 10.

herramientas supone una quiebra para el monopolio estatal de la persecución del delito, al tratarse de la "externalización" —*outsourcing*— de partes esenciales de la tarea de prevenir y perseguir el delito que comporta la obligación de conservación impuesta a los operadores[735].

En el caso español, el concreto instrumento legal configurado por la LCD y enunciado por este primer artículo presenta en concreto dos finalidades, una inmediata y otra mediata[736]. La primera consiste en el deber para los operadores de conservar las categorías de datos enunciadas en la ley, que opera como presupuesto de la finalidad mediata, a la que también alude el artículo 1.1 LCD: la eventual cesión a los agentes facultados con fines de "detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales".

El art. 1.1 LCD introduce un buen número de los elementos en torno a los cuales gira la mayor parte de esta regulación, que iremos examinando pormenorizadamente a lo largo de estas páginas.

Fijaremos por ahora nuestra atención en el concepto de "detección" de los delitos graves, empleado por el art. 1.1 LCD entre sus finalidades y cuyo significado parece referirse a la utilización de los datos con fines preventivos —por oposición al término "investigación"—, pero del que no se concreta su alcance. La idea de "detección" induce a pensar que el hallazgo de los delitos será susceptible de efectuarse inindiciariamente, esto es, al margen de la existencia de indicios de delito o con apoyo en simples sospechas sin base fáctica suficiente[737]. En este sentido, se referiría a lo que PEDRAZ PENALVA ha definido como la "detección de las circunstancias y condiciones criminógenas, dirigiéndose a los delincuentes ocasionales o potenciales", es decir, como una de las actividades incluidas en el concepto de "prevención"[738]. Ahora bien, por otra parte, también cabría interpretar el término "detección" como referido a las

---

[735] Cf. Pérez Gil, J., "Entre los hechos...", op. cit., pp. 235 y 236.

[736] El mérito de esta distinción corresponde a González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 10; o también en Los datos de tráfico..., op. cit., p. 415.

[737] Así lo ha recalcado González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 11.

[738] Cf. Pedraz Penalva, E., "Notas sobre policía y justicia penal", Revista jurídica de Castilla y León, nº. 14, enero 2008, pp. 23, 77 y 78.

actividades preventivo-policiales de aseguramiento de fuentes de prueba de carácter preprocesal, y no a las preventivas de la comisión de delitos, lo que parece sugerir la propia secuencia detectar, investigar y enjuiciar empleada por el art. 1.1 LCD[739].

28.2 El concepto de delito grave en la LCD

Una interpretación literal del art. 1.1 LCD puede llevarnos fácilmente a equívoco acerca de cuál es el verdadero ámbito de aplicación de la norma que examinamos. En concreto, nos referimos a la correcta delimitación de la noción de "delito grave" que maneja la LCD, cuyas medidas de conservación —conforme al tenor del precepto— miran a la exclusiva finalidad de detectar, investigar y enjuiciar "delitos graves contemplados en el Código Penal o en las leyes penales especiales"[740].

Lo primero que nos sugiere la redacción del art. 1.1 LCD es que la misma no hace sino transcribir fielmente lo dispuesto en la Directiva 2006/24/CE, que se refiere a "los delitos graves, tal como se definen en la legislación nacional de cada Estado miembro"[741]. La opción del legislador europeo de incluir en el ámbito de aplicación de la medida la generalidad de los delitos graves ya ha sido objeto de nuestra reflexión al comentar la Directiva, y a esa parte nos remitimos en lo que toca a su conveniencia y acierto. No obstante, debemos recordar aquí que el legislador comunitario partía de la idea de que la respuesta coordinada de los Estados miembros mediante la disponibilidad de los datos almacenados relativos a comunicaciones electrónicas habría de servir cuando menos para dar respuesta a un denominador común: la persecución del terrorismo y la delincuencia organizada, como se puede comprobar con la simple lectura de su considerando 21[742]. Pero la referencia que se hacía al terrorismo y a la

---

[739] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 11.

[740] Cf. art. 1.1 LCD *in fine*.

[741] Concretamente: "que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro". Cf. art. 1.1 *in fine*, Directiva 2006/24/CE.

[742] El Considerando 21 se refiere a "los objetivos de la presente Directiva, a saber, armonizar las obligaciones de los proveedores de conservar determinados datos y asegurar que éstos estén disponibles

delincuencia organizada —sin duda los genuinos detonantes de la regulación comunitaria— no se reflejó en el articulado de la Directiva, que optó finalmente por la fórmula abierta del delito grave según la legislación interna de los Estados miembros. En este sentido, la Directiva ha acabado por presentarse como una auténtica norma de mínimos, más preocupada por su finalidad armonizadora que por dar una respuesta jurídica única a las posibilidades procesales de la retención de datos, tal como también sugiere el propio considerando 21[743]. Son los Estados miembros quienes en definitiva deben decidir qué infracciones criminales pueden verse favorecidas por tan eficaz fuente de conocimiento.

El legislador español, al implementar lo previsto en la norma europea, pretendió en una primera hora separarse de lo dispuesto textualmente en la Directiva y extender el objeto de la medida a cualquier delito. De este modo, el artículo 1.1 del Anteproyecto, al definir el objeto de la Ley, autorizaba la cesión de los datos conservados cuando fueran requeridos "con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales". En la Exposición de Motivos, se advertía que el legislador había optado por habilitar la cesión de estos datos para cualquier tipo de delito "a fin de no privar a las Autoridades Judiciales de un mecanismo de detección e investigación con el que actualmente cuentan de acuerdo con la configuración constitucional del derecho al secreto de las comunicaciones"[744], así como porque era "imposible saber con precisión cuando se inicia una investigación penal cuál será la calificación final de los hechos delictivos"[745]. En cuanto a la primera explicación, la implicación del principio del menor rigor en la afectación del derecho al secreto de las comunicaciones, y por ende de la protección de datos de carácter personal —los dos derechos afectados por la LCD—, pudo sin duda haber pesado en la

---

con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la normativa nacional de cada Estado miembro, como el terrorismo y la delincuencia organizada".

[743] En este sentido, el Considerando 21 expone que dado que los objetivos de la presente Directivason armonizar las obligaciones de los proveedores de conservar determinados datos "no pueden ser alcanzados de manera suficiente por los Estados miembros y, debido a la dimensión y los efectos de la presente Directiva, pueden lograrse mejor a nivel comunitario, la Comunidad puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado".

[744] Cf. Exposición de Motivos, párrafo sexto del apart. I.

[745] Ibíd.

opinión del Ejecutivo al redactar el Anteproyecto, liberándose a su vez de la complicación que suponía el tener que realizar un estudio serio y riguroso del catálogo concreto de infracciones criminales cuya investigación pudiera verse beneficiada por tan poderosa fuente de conocimiento. La segunda justificación tampoco parece muy convincente, puesto que el hecho de que cuando se inicia la investigación penal resulte difícil determinar cuál será la calificación final de los hechos ilícitos no supone sino el intento de apoyarse en una circunstancia evidente para obviar que precisamente el control judicial previo está destinado, entre otros aspectos, a asegurar que los indicios de delitos requeridos para limitar el derecho al secreto de las comunicaciones satisfacen la exigencia de gravedad y, en definitiva, se ajustan al principio de proporcionalidad. Ambas explicaciones resultaban en consecuencia desacertadas.

En todo caso, el notable apartamiento de la norma a transponer no pasó inadvertida en la tramitación legislativa, y sobre él llamaron la atención varias instituciones. En particular, la Agencia Española de Protección de Datos consideraba que "tanto la Directiva 2006/24/CE como la jurisprudencia del Tribunal Constitucional parecen exigir la gravedad del delito como requisito previo a la adopción de medidas tales como la intervención de las comunicaciones o, en el caso de la Directiva, la comunicación de datos de tráfico y localización"; y concluía, por ello, que la comunicación de los datos debe limitarse a los fines de investigación, prevención y detección de delitos "graves"[746].

Más que la constitucionalidad o no de esta decisión, parece que fue finalmente un criterio de buena política legislativa el que malogró el intento. En concreto, dado que el objeto de la Directiva se proponía "armonizar las disposiciones de los Estados miembros relativas a las obligaciones" en materia de conservación y cesión con fines penales, la extensión de sus previsiones a la persecución de cualquier delito hacía un

[746] El GT29, en su Dictamen 3/2006, enunció entre las garantías exigibles la limitación de la conservación a los delitos graves, entendiendo que "cualquier otro uso de los mismos debería excluirse o estar rigurosamente limitado sobre la base de unas garantías concretas". De hecho, tal opinión constituye una relajación de los requisitos exigidos por este mismo órgano en su anterior Dictamen 4/2005, en que se sostiene que "Los datos sólo deberán conservarse con el fin específico de luchar contra el terrorismo y la delincuencia organizada, en vez de considerarse cualesquiera otras "infracciones graves" indeterminadas". Al respecto, cf. González López, J. J., Los datos de tráfico..., op. cit., pp. 426 y 427.

mal servicio a esta finalidad. No cabe olvidar que la Directiva 2006/24/CE había sido aprobada para armonizar disposiciones dictadas por los distintos Estados miembros en aplicación del artículo 15.1 DPCE[747], que al permitir ya este tipo de medidas[748], había dado lugar a una pluralidad de regulaciones nacionales cuya homogeneización a nivel europeo se estimaba conveniente. Aunque finalmente la Directiva 2006/24/CE no ha alcanzado el objetivo propuesto, por los diversos motivos que ya apuntamos, la decisión del legislador español de extender las medidas a cualquier delito no habría sido sino una contribución directa a este fracaso del objetivo europeo común.

La redacción finalmente aprobada acabó así refiriéndose sólo a los "delitos graves". No ha faltado algún autor[749] que ha dado por sentado que no cabe sino interpretar tales términos de manera literal, esto es, acudiendo a lo que el Código Penal establezca formalmente como delitos de tal denominación. De acuerdo con este criterio, la interpretación literal de la previsión del art. 1.1 LCD nos llevaría a cubrir un abanico delictivo muy extenso pero de sencillísima delimitación. El art. 13.1 del vigente

---

[747] 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). El mencionado artículo dispone que "los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, 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 del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros 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. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea".

[748] Y en el que tiene su origen el art. 12 LSSI.

[749] Como por ejemplo RODRÍGUEZ DELGADO, para quien "la opción adoptada por el legislador de englobar todos los delitos graves dentro del objeto de la Ley excede en cierta medida los delitos para los que se pensó la directiva, en especial delitos de terrorismo, tráfico de armas y explosivos, y a mi entender, delitos informáticos". Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 10.

Código Penal —en la redacción dada por la Ley Orgánica 15/2003, de 25 de noviembre[750]— define como "delitos graves" aquéllos que son castigados con "penas graves", que son las descritas en su art. 33.2[751], a saber:

a) "La prisión superior a cinco años.
b) La inhabilitación absoluta.
c) Las inhabilitaciones especiales por tiempo superior a cinco años.
d) La suspensión de empleo o cargo público por tiempo superior a cinco años.
e) La privación del derecho a conducir vehículos a motor y ciclomotores por tiempo superior a ocho años.
f) La privación del derecho a la tenencia y porte de armas por tiempo superior a ocho años.
g) La privación del derecho a residir en determinados lugares o acudir a ellos, por tiempo superior a cinco años.
h) La prohibición de aproximarse a la víctima o a aquellos de sus familiares u otras personas que determine el juez o tribunal, por tiempo superior a cinco años.
i) La prohibición de comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el juez o tribunal, por tiempo superior a cinco años.
j) La privación de la patria potestad".

Cualquier delito castigado con alguna de estas penas tiene carácter de delito grave y, por tanto, de acuerdo con una interpretación literal del art. 1.1 LCD, su detección, investigación o enjuiciamiento podría beneficiarse automáticamente de las medidas habilitadas por la LCD, en tanto que aquellos delitos no comprendidos en esta relación quedarían consecuentemente excluidos de tal posibilidad.

Creemos que este criterio interpretativo merece ser ampliamente cuestionado. Una comprensión meramente literal de lo que haya de entenderse por "delito grave" no resulta admisible por resultar tanto insuficiente como meridianamente inadecuada.

En primer lugar, la interpretación literal del concepto de "delito grave" ex art. 1.1 LCD es insuficiente porque nos llevaría a usar las medidas de la LCD sólo para perseguir aquellos delitos castigados con penas superiores a cinco años de prisión, y quedaría

---

[750] Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. BOE núm. 283 de 26 de noviembre de 2003, pp. 41842 a 41875.

[751] Cf., entre otros, Ormazábal Sánchez, Guillermo, Los deberes de conservación…, op. cit., p. 5. Así también se sobreentiende en RODRÍGUEZ DELGADO, al sostener que "la opción adoptada por el legislador de englobar todos los delitos graves dentro del objeto de la Ley excede en cierta medida los delitos para los que se pensó la directiva, en especial delitos de terrorismo, tráfico de armas y explosivos, y a mi entender, delitos informáticos". Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 10.

prohibida su aplicación en campos de la investigación criminal ciertamente idóneos, tales como la posesión y difusión de pornografía infantil, el tráfico de sustancias estupefacientes que no causaran grave daño a la salud, los delitos contra el patrimonio de cierta trascendencia social —piénsese en los atracos a bancos, etc.—, la protección del patrimonio histórico, etc[752].

En segundo lugar, el recurso estricto a lo dispuesto en los arts. 13.1 y 33.2 CP resulta claramente inadecuado en tanto que nos hace aplicar un criterio arbitrario para saber cuando las herramientas de la LCD pueden ser empleadas. Como es sabido, la razón efectiva por la que el actual sistema penal español considera como delitos graves los castigados con penas superiores a cinco años —y no a tres, como sucedía anteriormente[753]— no depende de la gravedad sustantiva de los hechos, sino que —de acuerdo con la explicación que nos da la Exposición de Motivos de la Ley Orgánica 15/2003, de 25 de noviembre, origen de la actual redacción de los comentados preceptos— el motivo por el cual el legislador ha fijado el parámetro en la prisión superior a cinco años descansa en la mera simplificación de normas procesales. En concreto, se buscó diferenciar los delitos cuyo enjuiciamiento corresponde a las Audiencias Provinciales frente a los que competen a los Juzgados de lo Penal[754]. Es

---

[752] Argumento también esgrimido por RODRÍGUEZ LAINZ. Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 8.

[753] El art. 33.2 del Código Penal, en su redacción anterior a la reforma, disponía que "son penas graves:

a) La prisión superior a tres años.

b) La inhabilitación absoluta.

c) Las inhabilitaciones especiales por tiempo superior a tres años.

d) La suspensión de empleo o cargo público por tiempo superior a tres años.

e) La privación del derecho a conducir vehículos a motor y ciclomotores por tiempo superior a seis años.

f) La privación del derecho a la tenencia y porte de armas por tiempo superior a seis años.

g) La privación del derecho a residir en determinados lugares o acudir a ellos o la prohibición de aproximarse a la víctima, o a aquellos de sus familiares u otras personas que determine el Juez o Tribunal, o de comunicarse con ellos, por tiempo superior a tres años".

[754] Indica el apart. II.b) de la Exposición de Motivos que "se establece en cinco años la duración de la pena que permite distinguir entre la grave de prisión y la menos grave, con lo que se consigue una regulación armonizada con la distribución de competencias entre el Juzgado de lo Penal y la Audiencia Provincial prevista en la Ley de Enjuiciamiento Criminal, de modo que la Audiencia Provincial conocerá

decir, realmente el propósito del legislador no fue elevar el concepto de gravedad de la pena —y por tanto del delito grave—, sino, manteniendo en esencia la misma correlación que la establecida en el texto inicial del Código Penal de 1995, con una visión más procesal que material, identificar el delito grave como aquél que es enjuiciable ante las Audiencias Provinciales[755]. Si el legislador optó definitivamente por el camino fácil, esto es, por trasladar la voz delito grave utilizada en la Directiva 2006/20/CE, es obvio que no pretendía establecer una relación directa, racional y excluyente entre las medidas de investigación provistas por la LCD y los delitos que son de conocimiento exclusivo de las Audiencias Provinciales o de la Sala de lo Penal de la Audiencia Nacional. Admitir lo contrario resultaría bastante paradójico, toda vez que los restantes delitos "no graves", incluidos parte de los delitos contra la salud pública, y en general delitos relacionados con el crimen organizado —vg. tráfico de inmigrantes, contrabando— o que emplean la red para su expansión o garantía de la impunidad de sus autores —vg. difusión de pornografía infantil, estafas vía telemática, etc.—, y que pueden sin ningún género de duda ser objeto de una plena interceptación de los contenidos de comunicaciones, quedan prácticamente excluidos del recurso a la interceptación de los datos de tráfico conservados en virtud de la LCD. En consecuencia, no cabe sino rechazar el criterio de la estricta literalidad para interpretar qué ha de entenderse por "delito grave" conforme al art. 1.1 LCD.

---

de los delitos castigados con penas graves y los Juzgados de lo Penal de los delitos castigados con penas menos graves".

[755] Añade Rodríguez Lainz al respecto que "a igual conclusión se llegaría comparando la postura del legislador en la concepción de la gravedad de la pena a los efectos de la decisión judicial sobre una medida tan grave como es la privación provisional de la libertad en el curso de un proceso penal, en una norma tramitada casi en paralelo con el anterior texto modificador del Código Penal. Con la actual redacción del art. 503.1,1º de la Ley de Enjuiciamiento Criminal, el delito grave, justificador de tan grave medida restrictiva de la libertad personal del imputado, pasaría a ser aquél castigado con pena igual o superior a la de dos años de prisión, incluso superable a la baja si el imputado contara con antecedentes penales no cancelados o que pudieran serlo derivados de delitos dolosos (art. 503.1,1.º,2). La pena igual o superior a la de dos años de prisión es un criterio de especial peso a la hora de decidir el ingreso en prisión provisional de un imputado o acusado". Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 8.

La cuestión de fondo —y otro punto débil de la presente norma— radica en el hecho de que nuestro legislador, cediendo bien al afán de armonización de la Directiva, bien a su propia desidia, se ha apartado u olvidado del régimen legal y constitucional conforme al cual se regulan en España las injerencias en los derechos fundamentales en el proceso penal. Esto nos obliga a posponer la correcta delimitación del concepto de delito grave manejado por el art. 1.1 LCD para la Cuarta Parte de esta Tesis, en la que abordaremos el correcto encaje de la medida central de la LCD en nuestro ordenamiento, lo que a su vez nos permitirá concretar cuáles son verdaderamente los delitos cuya detección, investigación y enjuiciamiento pueden valerse de este instrumento de lucha contra la criminalidad.

29 Sujetos obligados

El art. 2 LCD —bajo la rúbrica de "sujetos obligados"— establece que son destinatarios de las obligaciones relativas a la conservación de datos impuestas en la norma los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en LGT[756]. En efecto, esta última ley regula los requisitos para poder acceder a la condición de operador[757] y ofrece en su Anexo II las definiciones legales acerca de lo que ha de entenderse por "operador", "servicio de comunicaciones electrónicas", y "red de comunicaciones electrónicas", entre otros muchos términos.

Así, se entiende por *operador* la "persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas

[756] La remisión expresa por parte de la LCD a la LGT se nos antoja como una solución técnica positiva en la medida que permite una gran capacidad de adaptación a la constante evolución del Derecho de las telecomunicaciones.

[757] Cf. arts. 5 y 6 LGT y 4 RLGT. En relación con esta forma de determinar los sujetos obligados por remisión a la definición contenida en otra ley, el Consejo de Estado sugería "una reflexión sobre si pueden existir operadores que presten servicios de los previstos en la Directiva y que, por no prestarlos en los términos establecidos en dicha ley, quedan excluidos de las obligaciones que se prevén en el Anteproyecto".

disponibles al público y ha notificado a la Comisión del Mercado de las Telecomunicaciones el inicio de su actividad"[758]. Por servicio de comunicaciones electrónicas, "el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos; quedan excluidos, asimismo, los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas" [759]. Finalmente, son redes de comunicaciones electrónicas, "los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluida internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada" [760]. A su vez, las Directivas Marco sobre telecomunicaciones, y en concreto la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas[761], también contienen deficiones de estos términos, de la que la LGT ha tomado las dos últimas definiciones transcribiéndolas casi literalmente[762].

---

[758] Cf. apartado 21, Anexo II, LGT.

[759] Cf. apartado 28, Anexo II, LGT.

[760] Cf. apartado 25, Anexo II, LGT.

[761] Publicada en Diario Oficial de la Unión Europea, núm. L 108, de 24 de abril de 2002, pp. 0033 – 0050.

[762] De acuerdo con esta normas, se entiende por *servicio de comunicaciones electrónicas* "el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte

No obstante, al pretender delimitar el ámbito subjetivo de la LCD, ha de tenerse igualmente en cuenta que la condición de operador o prestador del servicio de comunicaciones electrónicas o la explotación de redes públicas de comunicaciones se ve condicionada en el Derecho español por la previa notificación fehaciente a la Comisión del Mercado de las Telecomunicaciones, con anterioridad al inicio de la actividad, y al sometimiento a las condiciones previstas para el ejercicio de la actividad que pretendan realizar[763]. En consecuencia, es dentro de tales condiciones donde deben entenderse aplicables las obligaciones impuestas por la LCD, que además se integra en la disciplina común de la legislación sobre telecomunicaciones al introducirse dentro del catálogo de infracciones y sanciones precisamente incumplimientos relacionados con dichos concretos deberes. De este modo, la identificación de quiénes son los obligados en la LCD se simplifica en la práctica significativamente, pues los mismos habrán de cumplir en todo caso con la necesaria inscripción en el Registro de operadores previsto por el art. 7 LGT[764]. De este modo, en caso de que surgiera alguna

---

de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos" —art. 2.c) Directiva 2002/21/CE—. Por otra parte, se considera "red de comunicaciones electrónicas" los "sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas —de conmutación de circuitos y de paquetes, incluido internet— y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada" —art. 2.a) Directiva 2002/21/CE—. Por último, se entiende por "red pública de comunicaciones electrónicas" aquella "red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público" —art. 2.d) Directiva 2002/21/CE—.

[763] Cf. art. 6.2 LGT, conforme al cual "los interesados en la explotación de una determinada red o en la prestación de un determinado servicio de comunicaciones electrónicas deberán, con anterioridad al inicio de la actividad, notificarlo fehacientemente a la Comisión del Mercado de las Telecomunicaciones en los términos que se determinen mediante real decreto, sometiéndose a las condiciones previstas para el ejercicio de la actividad que pretendan realizar".

[764] Dispone el art. 7 LGT que "en él [el Registro de operadores, dependiente de la Comisión del Mercado de las Telecomunicaciones] deberán inscribirse los datos relativos a las personas físicas o jurídicas que

duda sobre este ámbito, el criterio seguro de interpretación radica en si existe o no la certificación del Registro de operadores.

Además, para redondear nuestro intento de delimitación subjetiva, debe indicarse que el carácter de acceso público a las redes y servicios de comunicaciones electrónicas referido por el art. 2 LCD deja fuera del deber de conservación a los explotadores de redes y prestadores de servicios de comunicaciones electrónicas en régimen de autoprestación, es decir, a las redes privadas, que como se colige del último inciso del art. 6.2 LGT[765], están excluidos del régimen general de la prestación de servicios de telecomunicaciones.

En otro orden de cosas, se constata que el ámbito subjetivo cubierto por la LCD resulta más restringido que el proyectado por el art. 12 LSSI[766], pues a los operadores de redes y servicios se añadían los prestadores de servicios de alojamientos de datos, si bien estos tenían que conservar sólo los datos que permitieran identificar "el origen de los datos alojados y el momento en que se inició la prestación del servicio"[767]. En todo caso, la exclusión de estos prestadores de servicios de alojamiento supone una importante restricción al campo de investigación que pretende facilitarse con la LCD: la

---

hayan notificado su intención de explotar redes o prestar servicios de comunicaciones electrónicas, las condiciones para desarrollar la actividad y sus modificaciones".

[765] De acuerto con el art. 6 (*Requisitos exigibles para la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas*), apart. 2 *in fine*, quedan exentos de la obligación de notificación a la Comisión del Mercado de las Telecomunicaciones y de sometimiento a las condiciones previstas para el ejercicio de la actividad que pretendan realizar "quienes exploten redes y se presten servicios de comunicaciones electrónicas en régimen de autoprestación".

[766] Derogado por la Disp. Derog. Única de la LCD, el art. 12.1 LSSI disponía, respecto del deber de retención de datos de tráfico relativos a las comunicaciones electrónicas, que "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 deberán 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".

[767] Cf. art. 12.2 LSSI, cuyo párrafo tercero rezaba así: "Los prestadores de servicios de alojamiento de datos deberán retener sólo aquéllos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio".

trazabilidad de comunicaciones. Como señala RODRÍGUEZ LAINZ[768], buena parte de la actividad terrorista internacional se difunde mediante el alojamiento temporal de información —no sólo mediática o publicitaria de sus fines ilícitos—, sino también sobre consignas u órdenes concretas que suelen enmascararse en sus contenidos publicados en servidores o prestadores de servicio de alojamiento de datos. Al no existir posibilidad de acceder a tales fuentes de información —en concreto, las relacionadas con el origen de los datos alojados—, no se podrá acceder a la información necesaria para descubrir a sus autores, como no sea incidiendo de forma específica, tras la obtención de la oportuna autorización judicial, sobre los accesos que realicen en el futuro sobre la fuente originaria de los datos almacenados, lo que disminuye exponencialmente las posibilidades de éxito de la investigación[769].

No obstante, GÓNZALEZ LÓPEZ mantiene una opinión diferente al respecto, defendiendo que, conforme a la definición de "servicio de comunicaciones electrónicas", al art. 1.2 LGT, y a la interpretación que el G29 proporciona, los proveedores de servicios quedan incluidos en el ámbito de la LCD "cuando sus servicios consistan total o principalmente en el transporte de señales a través de redes de comunicaciones electrónicas, que es, en definitiva, lo que interesa en relación con el objeto de la LCD, siendo la pretensión de extender el deber de almacenamiento a los contenidos (implicando al administrador) contraria a la exclusión del contenido material que la propia LCD hace"[770].

En estrecha relación con esta materia, debemos hacer ahora algunas consideraciones sobre el *ámbito de aplicación territorial* de la LCD, sobre el que no existe una referencia específica en la propia norma. Parece que el mejor criterio al respecto es acudir al principio del sometimiento a la legislación nacional sobre telecomunicaciones

---

[768] Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad…, op. cit, p. 11.

[769] Explica el citado autor que las organizaciones terroristas internacionales suelen alquilar por días, si no por horas, servicios de alojamiento accesibles al público en cualesquiera ubicaciones geográficas de todo el planeta, que van rotando de forma casi aleatoria. Al no conservarse tales datos de acceso bastará con la variación constante de los alojamientos temporales para que se impida cualquier acceso lícito a su origen, como no sea obteniendo precisamente de forma previa la información sobre el origen; información que sin duda se mostrará como extremadamente dificultosa en su obtención. [Ibíd.]

[770] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 14.

que inspira el art. 6.1 LGT[771]. Esto es, aquellos operadores que lícitamente pueden concurrir en el mercado nacional de las telecomunicaciones —y por tanto están sometidos a la disciplina de la LGT—, son a los que incumbirá igualmente cumplir con los deberes de la LCD. La obligación, por tanto, parece fácilmente delimitable en este punto.

Sin embargo, pueden resultar dudosos aquellos supuestos en que la sede física del almacenamiento de datos se localice fuera de nuestro territorio nacional. En este sentido, no hay que olvidar que el párrafo segundo del art. 6.1 LGT[772] impone a las personas físicas o jurídicas que exploten redes o presten servicios de comunicaciones electrónicas a terceros el deber de designar una persona responsable a efecto de notificaciones domiciliada en España, sin perjuicio de lo que puedan prever los acuerdos internacionales. De este modo, la sede física del prestador puede estar sometida a una legislación extranjera, respecto de la que solamente en el ámbito de la Unión Europea —y en tanto en cuanto la Directiva 2006/24/CE haya sido debidamente transpuesta—, se podrá garantizar el cumplimiento de su obligación de conservación y cesión.

En los demás casos, la situación será mucho más compleja, pues no existe en el área de la conservación de datos una norma similar a la vigente en el campo de la interceptación legal de comunicaciones, donde el deber de colaboración, definido por la prestación del servicio en el territorio nacional, queda expresamente definido en el art.

---

[771] El tenor literal del precepto dispone: "Artículo 6. Requisitos exigibles para la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas.

1. Podrán explotar redes y prestar servicios de comunicaciones electrónicas a terceros las personas físicas o jurídicas nacionales de un Estado miembro de la Unión Europea o con otra nacionalidad, cuando, en el segundo caso, así esté previsto en los acuerdos internacionales que vinculen al Reino de España. Para el resto de personas físicas o jurídicas, el Gobierno podrá autorizar excepciones de carácter general o particular a la regla anterior.

En todo caso, las personas físicas o jurídicas que exploten redes o presten servicios de comunicaciones electrónicas a terceros deberán designar una persona responsable a efecto de notificaciones domiciliada en España, sin perjuicio de lo que puedan prever los acuerdos internacionales".

[772] Cf. anterior nota a pie.

85.1 RLGT[773], imponiéndose el deber de colaboración aun cuando solamente se preste en España el acceso a una red pública de comunicaciones, y el equipamiento susceptible de emplearse para realizar la interceptación se encuentre bajo la jurisdicción de otro Estado[774].

30 Datos objeto de conservación

Los datos que han de ser objeto de conservación por parte de los operadores se especifican en el artículo 3 LCD, que es el más extenso de la Ley y que prácticamente no hace sino reproducir lo dispuesto en el artículo 5 de la Directiva 2006/24/CE.

De este modo, nuestra Ley, al abordar dicha enumeración, sigue de cerca los pasos de la norma comunitaria y enuncia primero los datos necesarios para identificar el origen de una comunicación, para continuar seguidamente con los del destinatario, fecha y duración, tipo de comunicación y equipo de comunicación. En concreto, las categorías de datos que el art. 3 LCD manda conservar son las siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

> 1º. Con respecto a la telefonía de red fija y a la telefonía móvil: i) Número de teléfono de llamada. ii) Nombre y dirección del abonado o usuario registrado.

---

[773] En este sentido, indica el art. 85.1 RLGT (*Sujetos obligados y obligación de colaborar*) que "estarán obligados a seguir los procedimientos y adoptar las medidas a las que se refiere el artículo 83 los operadores que presten o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público o de establecer o explotar redes públicas de comunicaciones en España, con independencia de la naturaleza, ámbito territorial y momento en que tuvo efecto su habilitación.
Los operadores a los que se refiere el párrafo anterior estarán obligados a cumplir lo establecido en este capítulo, aun en el caso de que sólo presten en España acceso a una red pública de comunicaciones electrónicas, y todo aquel equipamiento susceptible de emplearse para realizar la interceptación se encuentre bajo la jurisdicción de otro Estado".

[774] Se cuenta además con un estimable mecanismo de cooperación judicial: el Acto del Consejo de la Unión Europea de 29 de mayo de 2000, por el que se celebra, de conformidad con el art. 34 del Tratado de la Unión Europea, el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, arts. 18 a 20.

2º. Con respecto al acceso a internet, correo electrónico por internet y telefonía por internet: i) La identificación de usuario asignada. ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía. iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1º. Con respecto a la telefonía de red fija y a la telefonía móvil: i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas. ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2º. Con respecto al correo electrónico por internet y la telefonía por internet: i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por internet. ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1º. Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.

2º. Con respecto al acceso a internet, al correo electrónico por internet y a la telefonía por internet: i) La fecha y hora de la conexión y desconexión del servicio de acceso a internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado. ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por

internet o del servicio de telefonía por internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1º. Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).

2º. Con respecto al correo electrónico por internet y a la telefonía por internet: el servicio de internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1º. Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.

2º. Con respecto a la telefonía móvil: i) Los números de teléfono de origen y destino. ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada. iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada. iv) La IMSI de la parte que recibe la llamada. v) La IMEI de la parte que recibe la llamada. vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3º. Con respecto al acceso a internet, correo electrónico por internet y telefonía por internet: i) El número de teléfono de origen en caso de acceso mediante marcado de números. ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1º. La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2º. Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

Del examen de este listado, y su comparación con el establecido en la Directiva, se constata que el listado de datos que han de ser objeto de conservación es un fiel trasunto —de "mimético" lo ha calificado algún autor[775]— del art. 5 de la norma comunitaria, del que solamente difiere en pequeñas modificaciones de finalidad aparentemente didáctica o de simple redundancia.

Así, vemos que el apartado c.1) de la Directiva se refiere a los "datos necesarios para identificar la fecha, hora y duración de una comunicación: 1) con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la comunicación", mientras que la norma española añade la fecha y hora del comienzo y fin de la comunicación y "en su caso", del servicio de mensajería o del servicio multimedia[776].

Algo similar ocurre con los datos necesarios para identificar el tipo de comunicación. Mientras el texto de la Directiva[777] meramente se refiere a "datos necesarios para identificar el tipo de comunicación: 1) con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado", el artículo español especifica muchísimo más: "datos necesarios para identificar el tipo de comunicación. 1. Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de

[775] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 4.

[776] Cf. art. 3.1.c).1 LCD.

[777] Cf. art. 5.1.d).1) LCD.

mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia)".

En tercer lugar, el apartado e) del art. 5.1 de la Directiva establece la retención de los datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación con respecto a la telefonía móvil, entre los que se incluye —letra vi— "en el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio". La norma española, por su parte, menciona expresamente las tarjetas prepago "en el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera"[778].

Los aspectos que merecen atención sobre el objeto del deber de conservación recogido en el art. 3 LCD y, concretamente, acerca del concepto de dato que maneja la LCD, son los mismos señalados en la Parte Primera de esta Tesis, por lo que nos remitimos a lo dicho allí con mayor detalle. No obstante, conviene advertir, en relación con nuestro Derecho interno, que la LCD abandona con esta regulación el clásico concepto de dato de tráfico[779] al que trasciende por dos frentes.

---

[778] Cf. art. 3.1.e.2) LCD. En el apartado 1.e.2º.vi) del Anteproyecto se había sustituido la referencia comunitaria a "servicios anónimos de pago por adelantado" por "servicios con tarjeta prepago". Esta sustitución era un error, que luego fue corregido tras advertirlo el Consejo de Estado en su Dictamen. De un lado, si existían o se creaban "servicios anónimos de pago por adelantado" distintos del de la tarjeta prepago, la norma española no incluiría todos los datos que exige la norma comunitaria; de otro lado, la previsión no era ajena a la regulación que introduce la disposición adicional única, pero, a juicio del Consejo de Estado, la existencia de un registro sobre las adquisiciones de tarjetas prepago no impedía que el servicio pudiera calificarse como "servicio anónimo de pago por adelantado". Para evitar problemas derivados de las dudas que pudieran albergarse sobre este extremo, se sugería la inclusión de la mención de ambos en el apartado 1.e.2.vi) del artículo 3, como así ha sucedido. Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.A.

[779] Para el art. 64.a) del RLGT, es dato de tráfico "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones o a efectos de su facturación". A efectos de una investigación, la dimensión económica del dato de tráfico resulta evidentemente ajena. Tan es así, que en el listado de datos objeto del deber de conservación la idea de la facturación es absolutamente ajena.

En primer lugar, el abandono de la idea de dato de tráfico como elemento *dinámico*, en el sentido de su captación en el curso de una comunicación intervenida judicialmente: el legislador no diferencia entre el dato de tráfico captado conforme se está generando y el dato de tráfico almacenado como dato de carácter personal[780].

En segundo lugar, la LCD utiliza un *amplio* concepto de dato, que incide no solamente en los componentes esenciales del dato de tráfico —terminales conectados, identificación de los usuarios y datación de la comunicación—, sino también en los que por regla general no serían sino servicios de valor añadido[781] —en concreto, la localización del usuario— cuando tal localización no fuera indispensable para el buen fin de la comunicación o a efectos de su facturación, así como en relación con una serie de datos tendentes a perfilar la persona física o jurídica titular o usuaria del servicio. No en vano, el concepto de dato utilizado por la Directiva 2006/24, en su art. 2.2.a) no puede ser más explícito a tal respecto, al referirse a los "datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario"; concepto que es reproducido en el art. 1.2 LCD. Los datos de tráfico clásicos se entremezclan así con datos de carácter personal ajenos a éstos, sometiéndose unos y

[780] Un mismo dato de tráfico puede conceptuarse como un elemento dinámico —esto es, como un elemento externo de una comunicación que está teniendo lugar— o como un elemento estático —un dato que es almacenado cuando la comunicación se da por concluida (sincrónico o diacrónico serían nomenclaturas más exactas)—. En tanto que elemento estático, el dato queda protegido por el derecho fundamental a la protección de datos de carácter personal. En tanto que elemento dinámico, ese mismo dato quedará protegido por el derecho fundamental al secreto de las comunicaciones. Volveremos sobre esta cuestión al exponer pormenorizadamente las implicaciones constitucionales de la LCD.

[781] Para el art. 2.g) de Directiva 2002/58/CE es servicio de valor añadido "Todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación". En el considerando décimo octavo se recogen como ejemplos de servicios de valor añadido las recomendaciones sobre tarifas menos costosas, orientación vial —mapas de carreteras según localización por GPS—, información sobre tráfico, previsiones meteorológicas e información turística; en todos se parte de la base de la necesaria compartición de datos de tráfico de la comunicación que permitan la prestación, conforme a tal información tratada previamente o conjuntamente con la comunicación —en el ejemplo de los mapas de carretera el GPS o localizador ubica al vehículo en el punto en que se encuentra, manejando, tratando tal información, para orientar su circulación conforme al mapa de carreteras utilizado—.

otros al mismo régimen jurídico en tanto en cuanto son objeto de almacenamiento para su eventual utilización ulterior.

Adicionalmente, debemos señalar que del listado de datos, ninguno de ellos tiene una relación concreta y directa con el concepto de red pública de comunicaciones, como no sea el que las comunicaciones transitan por éstas. La red pública de comunicaciones, y los datos que pudieran concernirle directamente, solamente interesan a la investigación criminal en cuanto que permitan facilitar información sobre el tránsito de una determinada comunicación hasta llegar a su destino —estrechamente unido al concepto de trazabilidad—; información que siempre estará asociada a los concretos datos de tráfico de comunicaciones que se deben conservar, o que podrán obtenerse a través de la colaboración del proveedor de servicios que facilite un servicio de itinerancia al prestador principal, como refiere el art. 85.2.2 RLGT[782].

Un aspecto relevante del listado del art. 3 LCD —señalado por GÓNZALEZ LÓPEZ[783]— es el apartamiento u olvido por parte del legislador español de la doble dimensión formal y material que la jurisprudencia constitucional[784] constata en el contenido de cada comunicación, lo que no impide que se identifique el contenido —dimensión material— con lo que el art. 1.3 LCD viene a referirse como "la información consultada utilizando una red de comunicaciones electrónicas". Como ya dijimos, esta distinción puede plantear dificultades derivadas de la complejidad de la delimitación entre contenido "formal" y "material" de la comunicación, como en el caso de los datos de localización geográfica, cuya adscripción a uno u otro tipo de contenido es suceptible de variar. La necesidad de minimizar estos eventuales problemas es lo que invita a que la relación de datos a retener del art. 3 LCD deba considerarse taxativa, sin que quepa su aplicación flexible o analógica. Así lo defiende GONZÁLEZ LÓPEZ, para quien otra posibilidad supondría "incurrir en una inseguridad jurídica en cuanto al alcance de la

[782] "Asimismo cualquier otro proveedor de servicios de comunicaciones electrónicas disponibles al público que acuerde facilitar servicio de itinerancia con un proveedor estará obligado a colaborar con éste en el cumplimiento de los requisitos de este capítulo".

[783] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 4.

[784] Véanse la Parte Cuarta de la presente Tesis y las sentencias y doctrina allí expuestas.

medida totalmente inadmisible"[785]. En este sentido, concurrimos con el autor citado en que la enumeración de los concretos datos a retener debe valorarse positivamente[786].

Una vez determinada la tipología de datos que han de ser conservados por los operadores de telecomunicaciones, el art. 3 LCD contiene un segundo, último y breve apartado conforme al cual "ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley", transposición fiel del apartado segundo del art. 5 de la Directiva 2006/24/CE. Al respecto, hemos de señalar que estamos ante el común denominador de todos los datos objeto de obligada conservación, que es la no injerencia en el derecho al secreto de las comunicaciones ni la conservación de contenidos de comunicaciones —que implica al derecho a la intimidad—, a través de una auténtica norma de cierre. Se puede entender así que este párrafo es eminentemente un recordatorio, una mera aclaración llevada a cabo por el legislador, ya que el objeto de la obligación de conservar viene establecido positivamente, enumerando todos y cada uno de los datos susceptibles de dicha obligación. En la misma línea, entiende RODRÍGUEZ DELGADO que aunque se trate de una previsión prescindible, "sirve de recordatorio de la existencia, sean cuales fueran los fines de la Ley 25/2007, de 18 de octubre, del derecho fundamental del secreto de las comunicaciones que la Constitución recoge en el artículo 18.3"[787]. Además, tal como ha venido interpretándose la afectación de la LCD por el legislador y la doctrina, la reserva del derecho al secreto de las comunicaciones como derecho fundamental de naturaleza formal parece erigirse en principio esencial del deber de conservación, a la vez que en clave de bóveda para la constitucionalidad del empleo de la forma de ley ordinaria; cuestión sobre la que posteriormente volveremos en la Cuarta Parte de esta Tesis.

[785] Ibíd.

[786] Ibíd.

[787] Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 8.

31 Obligación de conservar datos

El auténtico núcleo de la normativa en estudio radica —junto con el art. 1 LCD— en la previsión del art. 4 LCD[788], cuyos tres apartados, agrupados bajo la rúbrica "obligación de conservar datos", establecen el deber general para los operadores obligados de conservar los datos procedentes de las comunicaciones electrónicas, adoptando las medidas necesarias para garantizar que los datos especificados en el art. 3 LCD se conserven de conformidad con lo dispuesto en la propia Ley y en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate —bien telefónica o por internet—. Indica el párrafo segundo del art. 4.1 LCD que en ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el art. 38 LGT. Con estas palabras, el precepto incorpora lo dispuesto en el art. 3 de la Directiva, realizando las adaptaciones oportunas para enmarcarlo en el ordenamiento español y, en particular, sustituyendo la referencia a distintos artículos de la Directiva 2002/58/CE por lo dispuesto en el art. 38 LGT. La obligación central de conservar los datos de tráficos va acompañada a su vez de una obligación correlativa, que le da

---

[788] Transcribimos aquí el tenor literal del precepto:

"Artículo 4. Obligación de conservar datos.

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados".

sentido: los arts. 6 y 7 LCD obligan a los operadores a ceder a las autoridades facultadas los datos obtenidos en virtud de lo que se establece en el art. 4 LCD.

Así las cosas, podemos indicar —siguiendo a RODRÍGUEZ DELGADO[789]— que el deber general de conservación comporta una doble carga para los sujetos obligados: en primer lugar una obligación de captar y almacenar lo captado; en segundo lugar, la imposibilidad para estos proveedores de aprovechar o utilizar los registros generados. Examinado desde el punto de vista del ordenamiento interno español, no podía ser de otra manera. La conducta de captar, guardar y no destruir los registros creados por las comunicaciones electrónicas o telefónicas supone una amplísima excepción a los principios generales del Derecho de las telecomunicaciones reflejados en el ya tratado Cap. III del Tít. III de la LGT que, para proteger los derechos a la intimidad, la protección de datos de carácter personal y el secreto de las comunicaciones, sustrae a los proveedores la facultad de disponer de estos datos a su antojo, sometiendo cualquier tratamiento al consentimiento previo e informado[790] del cliente, y de igual modo, consagra el derecho —deber para las compañías— a que se hagan anónimos o se cancelen cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Como ya vimos, el meritado art. 38 LGT recoge en nuestro ordenamiento los derechos de los consumidores y usuarios finales en relación con los datos de tráfico y de localización, y se ocupa de especificar los concretos supuestos y las condiciones exactas en que las compañías pueden usar de los datos generados por sus servicios: son los "supuestos de autorización" a los que se refiere el art. 4.1 LCD[791].

Así, aunque los abonados a los servicios de comunicaciones electrónicas tienen el derecho "a que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación", el art. 38.3.a) LGT dispone que los datos de tráfico necesarios a efectos de la facturación de los abonados y

---

[789] Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 7.

[790] Cf. art. 38.3 LGT.

[791] A saber, el segundo párrafo del precepto dispone que "cada Estado miembro definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del Derecho de la Unión o del Derecho internacional público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos".

los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnacion de la factura del servicio o para que el operador pueda exigir su pago. Además, los abonados tienen derecho a que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido "únicamente cuando hubieran prestado su consentimiento informado para ello"[792] y a que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico "cuando se hayan hecho anónimos o previo su consentimiento informado" y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado[793].

En todo caso, se echa de ver que el legislador ha apostado decididamente por la implicación de los operadores de telecomunicaciones en su deber de colaboración con la investigación criminal, imponiéndoles un complejo y costoso deber de facilitación de medios tecnológicos y humanos en las labores de almacenamiento y facilitación de información sobre comunicaciones; y lo ha hecho —en expresión de RODRÍGUEZ LAINZ[794]— *cerrando el círculo* del deber de facilitación de medios, que ahora afecta no sólo a la información que podría obtenerse de comunicaciones que tuvieran lugar desde la recepción de la orden judicial de interceptación —las clásicas intervenciones telefónicas de contenidos, que evolucionaron a las solicitudes mixtas de contenidos y datos de tráfico—, sino también al nuevo deber de conservación de datos a los efectos de su posible ulterior utilización procesal o a los efectos de las necesidades de investigación del Centro Nacional de Inteligencia.

Previamente a la aprobación de la LCD, el art. 33 LGT aportaba un título con rango de ley que imponía a los operadores un concreto deber de colaboración en la ejecución de interceptaciones de comunicaciones dictadas al amparo del art. 579 LECrim[795]. Pero en

---

[792] Cf. art. 38.3.b) LGT.

[793] Cf. art. 38.3.d) LGT.

[794] Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 15.

[795] Según la redacción dada por la Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal, "1. Podrá el Juez acordar la detención de la correspondencia privada, postal y

el campo de la información asociada con el tráfico de las comunicaciones o datos de carácter personal relacionados con éstas, la situación, sin embargo, se mostraba especialmente preocupante, pues o se accedía a la información almacenada legítimamente en bases de datos de los operadores al amparo del art. 11.2.d) LOPD[796], o se les imponía, respecto de los restantes datos, y desde el momento de recepción de la orden judicial, deberes de captación, conservación y cesión, que si encontraban una base legal en su obtención en el mencionado precepto, podían suponerles una carga tecnológica o económica que carecía de cobertura legal.

De hecho, sólo a partir de 2005, cuando se aprueba el Reglamento de la LGT[797] —que desarrolló el mandato de la redacción originaria del art. 33.2 LGT y de su Disposición Final Tercera— existió una determinación normativa —si bien de rango

---

telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

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

4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación".

[796] Dispone el art. 11.2.d) LOPD que el consentimiento exigido será preciso "cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas".

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

reglamentario— que especificase cuáles habían de ser tales concretos deberes de colaboración. De esta manera, se estableció una concreta norma de derecho positivo sobre el tratamiento de los datos de tráfico como posible fuente de información para la investigación criminal o del CNI.

Así pues, desde dos años antes de la entrada en vigor de la LCD, existía ya una base normativa para el acceso a unos datos de carácter personal relacionados con el tráfico de comunicaciones que afectaba a aspectos tan importantes como eran las características del medio de comunicación utilizado por el sujeto concernido, identificación del abonado o usuario, ubicación del punto de terminación de red o de terminal, código de identificación, para el supuesto que accediera a la red a través de claves, así como cualquier otra identidad[798], pero la limitación era evidente, puesto que únicamente se debería facilitar aquella información que se almacenaba, que era la generada por el tránsito de comunicaciones y en tanto en cuanto ésta fuera necesaria para encarrilar la comunicación o la conservada a los efectos comerciales y de facturación o conservada dentro de los estrechos márgenes del principio del consentimiento del usuario o abonado.

Aquí radica precisamente y en buena medida el mérito de la Ley objeto de nuestro estudio: en la extensión del ámbito del deber de colaboración a una actuación preventiva, más allá del concepto clásico de la protección de datos de carácter personal, que tiene su propia fuente en unos datos que han de ser conservados por los operadores por mandato legal. Ya no será necesario, con la LCD, imponer al operador un deber de colaboración, almacenando, o incluso captando, unos datos a los que no podría acceder, ni someter a tratamiento o cesión, como no fuera por imposición de una autoridad judicial. La información, simplemente, debe conservarse durante un plazo de tiempo delimitado, a los efectos de que resulte útil para alguno de los fines públicos superiores concretamente tasados. Pero el mérito va aún más allá, cuando por fin tan concretos

[798] El art. 84.i) del RLGT define la identidad como "Etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso".

deberes de colaboración en el ámbito de la injerencia sobre comunicaciones han adquirido el carácter de norma con rango de ley formal, evitando en buena parte el riesgo de superación de los límites de la potestad reglamentaria.

De hecho, la LCD ha recogido una serie de fuentes de investigación que en buena parte fueron anticipadas por la práctica jurisdiccional y avaladas por la jurisprudencia tanto del Tribunal Supremo como del Tribunal Constitucional. Así, la técnica de la captación de datos relativos a comunicaciones —en este caso, de datos de tráfico— como fuente para el inicio de una investigación sobre contenidos —fundada en la utilización de determinado terminal asociado con sospechosos del tráfico de estupefacientes— encontró un primer apoyo en la STS 306/2002, de 25 de febrero[799].

Por su parte, la información del tráfico de las llamadas emitidas como fuente de prueba, bien con origen en la información facilitada —una vez éstas tuvieron lugar— por los prestadores del servicio de telefonía, bien de la información obtenida de los teléfonos móviles intervenidos a los detenidos, cuenta también con numerosos precedentes jurisprudenciales. Al primer ámbito pertenece la interesante STS 1330/2002, de 16 de julio, en la que el *continuum* del tráfico de llamadas telefónicas que fuera descubierto mediante la petición del listado de llamadas emitidas y recibidas desde el teléfono móvil del patrón de una patera en peligro de naufragio permitió discriminar la

[799] Según la jurisprudencia citada se deduce que los agentes de autoridad en principio no pueden abrir la agenda del teléfono móvil de un sospechoso; aunque, si que tienen varias posibilidades: a) que, el sospechoso preste su consentimiento libremente; en este supuesto no habrá problema alguno; convendría que los agentes le hicieran firmar la autorización; b) que, el sospechoso se encuentre detenido en calabozos policiales; en este supuesto es necesario que preste su consentimiento en presencia de su letrado. Convendría que los agentes hicieran firmar la autorización al letrado y al detenido; c) que, el sospechoso, sea o no detenido se niegue a que los agentes puedan ver la agenda del móvil (registro de llamadas entrantes y salientes); en este caso los agentes pueden pedir al sospechoso que les entregue el teléfono e incluso utilizar la fuerza mínima imprescindible para ello; a continuación deberán practicar unas diligencias poniendo en conocimiento del juez los indicios existentes de que el sospechoso es el autor de unos hechos delictivos, explicado la necesidad de la práctica de la diligencia; el juez deberá abrir procedimiento judicial (generalmente diligencias previas) y a continuación resolver mediante un Auto motivado si la autoriza o no; lo siguiente, en caso de que el juez admita la necesidad de la prueba, sería que el secretario judicial, como fedatario público, diera fe del contenido de la agenda, a partir de este momento la información se podría poner a disposición de los agentes.

intervención organizativa de la persona que estaba dirigiendo la operación de inmigración clandestina desde el territorio español[800]. Al segundo, la trascendental STC 70/2002, de 3 de abril, así como las SSTS 316/2000, de 3 de marzo, 1235/2002, de 27 de junio, 934/2003, de 24 de junio, 1231/2003, de 25 de septiembre, 1023/2004, de 24 de septiembre, 1206/2004, de 6 de octubre, y la 912/2004, de 16 de julio, en la que la ocupación en poder del condenado de un teléfono móvil robado a una víctima de delito de violación y el examen del tráfico de llamadas relacionado con personas del círculo de aquél sirvieron de prueba irrefutable para la imputación al mismo del referido delito. En conclusión, la captación de datos de tráfico conjuntamente con contenidos, como técnica de investigación adicional a ésta, contaba con una larga lista de resoluciones tanto del Tribunal Constitucional como del Tribunal Supremo con anterioridad a la aprobación de la LCD.

Tras su entrada en vigor, las nuevas herramientas a disposición de los agentes facultados y de la autoridad judicial o del CNI abarcan ya a todo el espectro de posibilidades de actuación, desde la preambular, tomando como fuente los datos almacenados por mandato de la norma, como la actuación conjunta en el contexto de una interceptación de comunicaciones. Considera RODRÍGUEZ LAINZ que, en este último supuesto "la información se captará y cederá en origen, en el mismo momento en que los datos de tráfico recabados se vayan generando. Unos se someterán a la disciplina de la LCD —en tanto que no se llegue a afectar al contenido de las comunicaciones— y otros a la disciplina del art. 579 LECrim, pero en ambos casos bajo el imperio de unos mismos principios constitucionales, sin otra diferencia que el mayor rigor en la protección de los derechos fundamentales concernidos cuando se afecta a los contenidos que cuando se incide sobre los datos de tráfico de éstas o sobre datos relacionados con comunicaciones ya ultimadas"[801].

---

[800] O también la STS 130/2007, de 19 de febrero, que proclamó la ilicitud de técnicas policiales de captura o muestreo de frecuencias para acceder a los datos identificadotes de terminales de comunicaciones de sospechosos; así como la STC 26/2006, de 30 de enero, en un supuesto en el que se llegó a rechazar por el Juez instructor la intervención de contenidos, aceptándose la injerencia sobre datos de tráfico como fuente para avanzar en la línea de investigación abierta.

[801] Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 12.

En otro orden de cosas, hemos de hacer algunas consideraciones sobre las consecuencias prácticas que han tenido las medidas impuestas por el art. 4.1 LCD. Aunque la obligación de conservar, y por tanto almacenar lo conservado, parece a primera vista bastante fácil de cumplir, ya que tan sólo requiere que el programa informático que elabora los datos de tráfico de la comunicación —origen, destino, fechas, etc.— almacene los datos, este almacenamiento sin embargo ha supuesto una modificación de los programas gestores de estos datos, que deben realizar una función que antes no desempeñaban, y por otro lado, ha generado la necesidad de nuevos e ingentes espacios de almacenamiento. Por añadidura, la imposibilidad para los operadores de aprovechar o utilizar los registros generados ha dado lugar a la coexistencia de dos regímenes diversos. El primero, basado en una norma legal —la LCD— que impone una concreta restricción de determinados derechos relacionados con la protección de datos de carácter personal al objeto de su posible utilización para específicos fines públicos. El segundo, plenamente integrado en la normativa general sobre protección de datos de carácter personal —la LOPD— y su concreta aplicación en el tráfico de comunicaciones electrónicas —la LGT—. Como ya hemos visto, el art. 38 LGT desarrolla el derecho de los abonados y usuarios en relación con los datos de tráfico generados y limita las posibilidades de conservación a las estrictas necesidades técnicas y comerciales, abriendo la puerta del principio del consentimiento en contados aspectos y siempre bajo el estricto sometimiento al principio de la utilidad y conservación mientras que el servicio prestado así lo demande.

Como es obvio, esta situación es susceptible de crear ámbitos de compleja coexistencia entre el extenso deber de conservación *ministerio legis* y las posibilidades de conservación a efectos de tránsito y facturación o al amparo del consentimiento del usuario o abonado. Dicha coexistencia, además, casa difícilmente con las exigencias de calidad y seguridad en la conservación de tales datos a los efectos de lo establecido en la LCD. Si los datos de tráfico deben ser tratados y utilizados por el operador en tanto en cuanto son precisos para asegurar el buen fin de una comunicación, "es difícilmente defendible —advierte RODRÍGUEZ LAINZ[802]— permitir que unos datos que deben ser conservados sin que puedan ser manipulados o usados para fines distintos a los

[802] Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 12.

previstos en la Ley[803] puedan ser utilizados por el operador concernido para fines comerciales o de facturación. La coexistencia, si es que queremos respetar el mandato de la ley, y a la vez garantizar mínimos estándares de seguridad en su conservación a los efectos de su ulterior utilización en una investigación criminal o de inteligencia, debe evitarse a toda costa". Esto hace necesario establecer mecanismos que permitan la conservación independiente de los datos de tráfico para los fines de la LCD, y su tratamiento para legítimos fines comerciales o de facturación; y ello solamente puede conseguirse mediante la generación de ficheros independientes, unos bajo el imperio de la LCD y otros bajo el mandato de la LGT y de la LOPD.

No obstante, parece que la suposición de la que parte la LCD[804] es la conservación en un mismo registro de los datos destinados a satisfacer ambas finalidades: la eventual puesta a disposición de los agentes facultados y la de facturación y adecuada gestión del servicio por parte de los operadores. Según el párrafo segundo del art. 4.1 LCD, "en ningún caso, los sujetos obligados, podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones". La referencia aquí a los "registros generados" puede entenderse hecha a aquéllos que los operadores generen para sus propios fines de facturación. Sin embargo, la sede normativa en que se hace esta alusión nos invita a sostener, con GONZÁLEZ LÓPEZ[805], que el legislador se está refiriendo a los registros generados para satisfacer los fines de la LCD, ya que, de interpretar el precepto de la primera manera indicada, nos encontraríamos con una previsión redundante respecto de la que se hace en el art. 38 LGT. Ahora bien, si los "registros generados" son los destinados a satisfacer los objetivos de la LCD, el precepto está entonces estableciendo una autorización a los operadores para emplear tales registros con fines de facturación y gestión del servicio, compatibilizando su doble uso con los de disponibilidad para la eventual cesión a los agentes facultados. En ello ve RODRÍGUEZ LAINZ una previsión destinada a ahorrar costes a los operadores, que no necesitarán duplicar los archivos para albergar datos idénticos, pero también que al

[803] Cf. art. 8.1 LCD.

[804] No así en el Proyecto, que no hacía referencia alguna al respecto.

[805] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit. p. 9.

tiempo debe contemplarse un riesgo añadido a la integridad de los datos[806], en cuanto se verán sometidos a manipulaciones que, voluntaria o involuntariamente, pueden poner en riesgo las garantías de seguridad que pretende la LCD.

Finalmente, para no abandonar el orden con que queremos abordar el estudio sistemático del articulado, no podemos dejar de glosar los apartados segundo y tercero del art. 4 LCD, los cuales se ocupan de transponer lo previsto en el art. 3.2 de la Directiva 2006/24/CE. En relación con las denominadas *llamadas infructuosas*, el art. 4.2 define las mismas como "aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada", aquellas llamadas en las que el receptor no ha respondido —en términos coloquiales, llamadas perdidas— o en las que saltó el contestador automático o el buzón de voz, bien tras varios tonos, bien porque el terminal estaba apagado o comunicando ——es este segundo supuesto por el que la Ley habla de la "intervención por parte del operador u operadores involucrados". Dispone al respecto el precepto que la obligación de conservación se extiende también "a los datos relativos a las *llamadas infructuosas*, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados". Así, la citada obligación de conservación no sólo tiene por objeto los datos de tráfico de una comunicación electrónica "exitosa", sino que se extiende a los datos relativos a este tipo de comunicaciones. En definitiva, los datos de tráfico relativos a este tipo de comunicaciones deberán ser conservados por parte de los operadores al igual que lo son las comunicaciones exitosas[807]. Acerca de la utilidad

---

[806] Es más, se trataría de una actuación contraria a las recomendaciones del Grupo del Artículo 29, de acuerdo con el cual ".os sistemas para el almacenamiento de datos a efectos de orden público deberían lógicamente separarse de los sistemas utilizados con fines comerciales" correcta satisfacción de la finalidad mediata de su conservación. Cf. Dictamen 3/2006 sobre la Directiva 2006/24/CE. En la misma línea, cf. Dictamen 4/2005.

[807] Indica al respecto GONZÁLEZ LÓPEZ que "las "llamadas infructuosas" se hallan incluidas dentro del ámbito de cobertura temporal del derecho al secreto de las comunicaciones, por representar una tentativa de comunicación, fallida no por motivos técnicos de imposibilidad de establecimiento de la llamada, sino de resultas de la ausencia de respuesta por parte del interlocutor o de la actuación del tercero representado por el operador". Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit. p. 7.

práctica de esta previsión, indica RODRÍGUEZ LAINZ que la misma "no es precisamente baladí", puesto que las llamadas infructuosas representan "un indicio evidente de relaciones entre personas investigadas, rompiendo cualquier atisbo de duda sobre el carácter casual o no deseado de una determinada conversación"[808].

La ley española ha optado por excluir las llamadas no conectadas, cuyos datos relativos "están excluidos —en palabras del art. 4.3 LCD— de las obligaciones de conservación contenidas en esta Ley". Añade a renglón seguido el precepto una definición de las mismas, de tal manera que "se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados". Debe entenderse al respecto que, al no producirse el éxito de la llamada, no concurre el presupuesto susceptible de hacer posible la comunicación, la cual no puede considerarse impedida tras ser iniciada, ya que ni siquiera se llega a establecer el contacto con el interlocutor que, de no mediar la intervención del operador o ser atendido por el receptor, permitiría la transmisión de información[809]. Para RODRÍGUEZ DELGADO, la razón es tan sencilla como asumir que el objeto de la Ley son las "comunicaciones electrónicas", es decir, que "para que haya comunicación se requiere una transmisión de señales mediante un código común al emisor y al receptor. En el caso de las llamadas "no conectadas" es claro que ese intercambio de código no se produce"[810].

32 Período de conservación de los datos

Otro punto capital en el escrutinio de la LCD se refiere a los plazos durante los cuales los proveedores deben conservar los datos de tráfico. Establece al respecto su art. 5 que la obligación de conservación de datos cesa a los doce meses desde la fecha en que se

[808] Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 15.

[809] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit. p. 7.

[810] Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 3.

haya producido la comunicación[811]. Nos encontramos así, obviamente, dentro de los parámetros que establece la Directiva 2006/24/CE, cuyo artículo 6 dispone, como ya vimos, que los datos conservados se deberán garantizar en un período comprendido entre los seis meses y dos años a partir de la fecha de la comunicación. No podemos dejar de notar aquí que el plazo establecido por el legislador español coincide con el que venía dispuesto —a la espera de su fallida concreción reglamentaria— por el art. 12 LSSI, que permitía a los operadores retener hasta un máximo de doce meses los datos necesarios para la localización del terminal empleado por el usuario para transmitir cualquier comunicación por vía electrónica a título oneroso.

Ahora bien, para no renunciar a la flexibilidad que ofrece la Directiva 2006/24/CE, el legislador español ha incluido en el mismo artículo una habilitación al Gobierno para, "reglamentariamente, ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses", decisión que además habrá de hacerse "previa consulta a los operadores" y "tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave"[812], modificación que hasta el momento no ha tenido

---

[811] El artículo 5 del Anteproyecto, también referido al período de conservación de los datos, presentaba un contenido similar con una redacción algo más defectuosa. El vigente tenor literal dispone:

"Artículo 5. Período de conservación de los datos.

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación".

[812] Cf. art. 5.1 LCD. Esta posibilidad se encontraba en la Disposición Final Tercera del Anteproyecto, y fue incluida en el articulado a propuesta del Consejo de Estado, que juzgó "conveniente que el artículo 5.1 del Anteproyecto, al tiempo que fija el plazo de doce meses, incluyera una remisión a lo dispuesto en la disposición final tercera ("sin perjuicio de..."), a fin de no inducir a error al destinatario de la norma, y de forma que éste sea consciente de que el plazo fijado de forma precisa en el citado artículo 5 puede no

lugar. En pro de una mayor claridad y seguridad jurídica, la Disposición Final Tercera de la LCD —rubricada como *Desarrollo reglamentario*— recoge a su vez una habilitación general al Gobierno para el desarrollo reglamentario de la Ley[813].

Respecto del concreto condicionamiento a que se refiere el art. 5.1 LCD de que la ampliación o reducción del plazo se realice "tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de los delitos", tal exigencia se antojó al Consejo de Estado como paradójica, al comprobar que el propio Anteproyecto —al fijar el plazo de un año— exigía al Gobierno que tomara en cuenta unos costes que ya debían haberse tenido en cuenta al elaborar la memoria económica de la ley —"siquiera fuera una previsión aproximativa"[814]—; un requisito procedimental y de prudencia que ni el propio legislador había respetado.

Por otra parte, el segundo apartado del art. 5 LCD dispone que lo establecido en el apartado primero se entiende sin perjuicio de lo previsto en el artículo 16.3 LOPD sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación. El referido precepto determina, en su vigente tenor, que la cancelación de datos da lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Transcurrido el citado plazo, el mismo artículo indica que debe procederse a su supresión. La integración de estas normas presenta ciertos aspectos dudosos que —a pesar de la advertencia del Consejo de Estado— la redacción final no ha sabido solventarse eficazmente[815]. La cuestión radica en si la excepción —"sin perjuicio de"— es aplicable a los operadores que conservaron los datos y los cedieron —de forma que deben conservar los datos cedidos, aunque no se dice hasta cuándo— o a los cesionarios de los datos, de modo que los operadores habrían de destruir los datos al

---

ser el realmente aplicable", como finalmente se hizo. Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.B.2.a).

[813] Disposición Final Tercera, LCD: "se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley".

[814] Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.B.2.a).

[815] Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.B.2.b).

final del período de conservación, incluyendo los cedidos, si bien entonces estos últimos no quedarían destruidos en cuanto obraran en poder del cesionario. Esta última posibilidad parece coherente con lo dispuesto en la Directiva transpuesta, que en su art. 7.d) establece que "los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación". Aunque el artículo 7.d) tanto de esta Directiva como de la Directiva 95/46/CE hablan de *destrucción* y no de *cancelación*, la LOPD habla de *cancelación* y no de *destrucción* —compárense los artículos 2.b)[816], 17.1[817] ó 28.3[818] de esta última Directiva, con los artículos 3.c)[819], 9[820]

[816] Cf. art. 2.b) Directiva 95/46/CE: "A efectos de la presente Directiva, se entenderá por: b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".

[817] Cf. art. 17.1 Directiva 95/46/CE: "Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales".

[818] Cf. art. 28.3 Directiva 95/46/CE: "La autoridad de control dispondrá, en particular, de: […] —poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales".

[819] Cf. art. 3.c) LOPD. "A los efectos de la presente Ley Orgánica se entenderá por: c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

[820] Cf. art. 9.1 LOPD —*Seguridad de los datos*—: "El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que esten expuestos, ya provengan de la acción humana o del medio físico o natural".

y 37.1[821] LOPD—. En última instancia, se percibe un problema relacionado con la traducción e incorporación de estas normas comunitarias. Como pauta para la interpretación, cabe notar que la secuencia terminológica en el artículo 16.3 LOPD es que la cancelación da lugar al bloqueo y, cumplido el plazo allí previsto, se procede a la supresión de los datos.

Se echa en falta en todo caso una referencia expresa a la supresión de los datos no cedidos[822] como garantía de seguridad jurídica, máxime dada la ausencia de una previsión de este tipo en el artículo 4.5 LOPD, que sólo alude a la cancelación, que no es equivalente a la supresión, sino al "bloqueo", de acuerdo con la definición del artículo 5.1.b) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Ello no obstante, debe entenderse que tal deberá ser el destino de los datos no cedidos[823].

Por lo demás, no podemos dejar de hacer notar que, si bien el plazo anual es plenamente predicable de todos los elementos *dinámicos* de las comunicaciones, obviamente no podrá suceder lo mismo respecto de ciertos elementos *estáticos* —en concreto, los datos de identificación de abonados o usuarios, a los que hemos denominado "datos de suscripción" o "datos de abonado"— durante todo el tiempo que se mantenga la relación contractual del abonado con su operador. La existencia de una relación duradera de servicio impone a la compañía proveedora el deber —y a la vez la necesidad— de conservar los datos identificadores de quiénes son sus clientes. Esto

[821] Cf. art. 37.1 LOPD —*Funciones*—: "Son funciones de la Agencia Española de Protección de Datos: […] Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones".

[822] Como sí hacía el Proyecto de Ley en su artículo 5.1, párrafo segundo.

[823] En cambio resulta más apropiada la referencia que se hace en la Ley a la conservación de los datos en los supuestos de conservación de datos bloqueados con arreglo al artículo 16.3 LOPD —artículo 5.2 LCD— frente a la referencia hecha en el Proyecto a dicho precepto, pero referida exclusivamente a la prescripción de las infracciones presentes en él (en definitiva, las establecidas en la LGT, como se desprende de su artículo 10), ya que las responsabilidades derivadas del tratamiento no se limitan exclusivamente a las previstas en la LGT.

hace que se solapen a la vez dos obligaciones de conservación: una para dar respuesta al mandato de la LCD y otra para poder prestar el servicio a aquéllos[824].

Para finalizar este apartado, no estará de más recordar que la norma europea transpuesta permite en su art. 12[825] que el plazo máximo de dos años pueda ser ampliado ante circunstancias especiales, para lo cual el Estado miembro que decida ampliar dicho período debe comunicarlo a la Comisión y a los demás Estados, indicando las razones que originaron la ampliación. Nada se ha previsto o reflejado en la LCD sobre esta posibilidad.

---

[824] En este punto resulta cuando menos anecdótico el tratamiento de la cuestión respecto de la cesión de información almacenada en los libros-registro de identidad de tarjetas telefónicas de prepago, puesto que la Disposición Adicional única, en su parágrafo segundo, habla de un período comprendido "desde la activación de la tarjeta prepago hasta que cese la obligación de conservación a la que se refiere el art. 5 de esta Ley". Evidentemente, no es que la conservación expire al año de la activación de la tarjeta, sino que lo será durante el tiempo en que la misma permanezca activa, toda vez que en cualquier caso el deber de conservación de datos de identidad de los comunicantes trascendería a estas modalidades de contratación sobre las que no se innova, sino que simplemente se garantiza un cierto principio de transparencia en la titularidad de los terminales de comunicación.

[825] Para mayor ilustración, volvemos a transcribir aquí el tenor del art. 12.1 de la Directiva 2006/24/CE —*Medidas futuras*—: "Todo Estado miembro que deba hacer frente a circunstancias especiales que justifiquen una ampliación limitada del período máximo de conservación recogido en el artículo 6 podrá adoptar las medidas que se impongan. El Estado miembro en cuestión informará inmediatamente a la Comisión y a los demás Estados miembros sobre las medidas adoptadas de conformidad con el presente artículo e indicará las razones que le llevan a adoptarlas.

2. En un plazo de seis meses tras la notificación mencionada en el apartado 1, la Comisión aprobará o rechazará las medidas nacionales en cuestión después de haber examinado si constituyen una discriminación arbitraria o una restricción encubierta al comercio entre los Estados miembros o constituyen un obstáculo para el funcionamiento del mercado interior. En caso de que la Comisión no adopte ninguna decisión en dicho plazo se considerará que las medidas nacionales han sido aprobadas.

3. Cuando, en virtud del apartado 2, las medidas nacionales adoptadas por un Estado miembro se aparten de las disposiciones de la presente Directiva, la Comisión examinará la oportunidad de proponer la modificación de la presente Directiva".

33 Protección y seguridad de los datos

La protección, seguridad y almacenamiento de los datos a conservar es un aspecto crucial de la regulación que analizamos. Su régimen ha sido objeto de desarrollo en el art. 8 LCD[826], que bajo la rúbrica "Protección y seguridad de los datos", transpone a lo largo de los cuatro apartados que lo forman el contenido de los arts. 7, 8 y 9 de la Directiva 2006/24/CE.

Indica el apartado primero que los sujetos obligados[827] deberán, en primer lugar, identificar al personal "especialmente autorizado" para acceder a los datos objeto de la Ley y, en segundo lugar, adoptar las medidas técnicas y organizativas que impidan su manipulación, el uso para fines distintos de los comprendidos en la misma, la destrucción accidental o ilícita, pérdida accidental, o su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la LOPD y en su normativa de desarrollo[828].

---

[826] Transcribimos aquí para su directo examen el tenor literal del art. 8, que dice así:

"Artículo 8. Protección y seguridad de los datos.

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley".

[827] Cf. art. 2 LCD.

[828] Esto es: la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Por su parte, los apartados segundo y tercero del art. 8 LCD establecen que las obligaciones relativas a las medidas para garantizar "la calidad de los datos almacenados y la confidencialidad y seguridad en el tratamiento", así como "el nivel de protección de los mismos", se determinarán también de conformidad con lo previsto en la LOPD y su normativa de desarrollo[829].

Al ser la Agencia Española de Protección de Datos la autoridad pública responsable de velar por el cumplimiento de las previsiones de la normativa española de protección de datos, el art. 8.4 LCD extiende su competencia a la aplicación de las mismas en los datos y medidas contemplados en la LCD, atribución ésta que resulta coherente con el planteamiento general del legislador español y con la naturaleza preventiva de delitos de la medida de conservación de datos, que la sitúa en el ámbito administrativo. Se incorpora así en el ordenamiento interno español el art. 9 de la Directiva 2006/24/CE, que establece que los Estados miembros designarán las autoridades de control que se han de encargar de vigilar con plena independencia la aplicación de estos principios, y que podrá tratarse de las mismas autoridades previstas en la Directiva de protección de datos[830] —como, de hecho, se ha dispuesto en una mayoría de Estados miembros—. Asimismo, dicha competencia se corresponde con lo previsto por el art. 37.e) LOPD, de acuerdo con el cual constituye una de las funciones de la Agencia requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la LOPD y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones. El papel de la Agencia reviste una especial relevancia ya que, por añadidura, de acuerdo con lo dispuesto en el artículo 18 LOPD, es la destinataria de las reclamaciones que los interesados le dirijan ante las eventuales negativas a informarles de los datos sujetos a tratamiento, a la rectificación de éstos u otras relacionadas con los derechos previstos en la Ley.

---

[829] Véase anterior nota a pie.

[830] Se refiere a la Directiva 95/46/CE, cuyo art. 28.1 dispone que "los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia".

De lo hasta aquí expuesto se echa de ver claramente cómo las normas de protección y seguridad de los datos en la LCD se configuran como auténticas normas de remisión a la compleja normativa sobre protección de datos que, hasta la fecha, han de entenderse referidas al Real Decreto 994/1999, de 11 de junio, por el que se aprueba el *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*, cuya vigencia provisional ha sido ratificada por la Disposición Transitoria Tercera de la LOPD, y se sobreentiende en el art. 8.3 LCD. Sin embargo, la remisión en bloque a tal normativa olvida un detalle trascendental: los datos de carácter personal de conservación obligatoria encuentran un difícil acomodo en la determinación de los niveles de seguridad exigibles a los responsables de los ficheros. Como ha puesto de manifiesto RODRÍGUEZ LAINZ, la existencia de datos que pueden considerarse encuadrados tanto en niveles de seguridad bajo, medio y alto —en los términos definidos en el art. 4 del mencionado Reglamento[831]— habrían hecho conveniente que el legislador hubiera determinado claramente el nivel de seguridad exigible, estableciendo acaso un catálogo de normas específicas sobre los criterios y exigencias de protección y seguridad de los ficheros donde se almacene tan ingente y valiosa información[832]. En opinión del mismo autor, el nivel de seguridad debería ser

---

[831] Dispone el artículo 4 —*Aplicación de los niveles de seguridad*— lo siguiente:

"1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el art. 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los arts. 17, 18, 19 y 20.

5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes".

[832] Cf. Rodríguez Lainz, J. L., Intervención judicial en los datos de tráfico…, op. cit., p. 333 y ss., donde se trata ampliamente la cuestión.

cuanto menos el medio[833], dado que los datos conservados pueden facilitar un perfil bastante cercano a la posible evaluación del individuo afectado, así como por la posterior trascendencia procesal que pueden llegar a adquirir. La tutela eficaz de los derechos fundamentales no merece menos.

Por otra parte, no puede dejar de notarse que esta técnica legislativa de la remisión contraviene los requisitos establecidos por el GT29, que exige que se definan unas normas mínimas en lo relativo a las medidas de seguridad técnica y organizativa. Más concretamente, sus Dictámenes 4/2005 y 3/2006 —sobre la Directiva 2006/24/CE— señalan que deberían especificarse los requisitos generales establecidos en la Directiva 2002/58/CE al respecto, todo lo cual parece alejarse de la técnica de remisión empleada en la LCD[834].

34 Normas generales, procedimiento de cesión y formato de entrega de los datos

34.1 Normas generales sobre cesión de datos y agentes facultados

La tercera de las obligaciones que se imponen a los operadores que presten servicios de comunicaciones electrónicas consiste en ceder los datos conservados. El art. 6 LCD[835],

---

[833] Cf. art. 4.4 del mencionado Reglamento.

[834] Así lo ha puesto de manifiesto GONZÁLEZ LÓPEZ, quien además señala que, aunque la falta de concreción se intentara solventar acudiendo a lo dispuesto en la Disposición Final Tercera de la LCD (que habilita al Gobierno a desarrollar lo previsto en la ley), "no dejaría de ser a todas luces inadecuado acudir a normas reglamentarias para establecer unas garantías cuya trascendencia hace necesario que se establezcan legalmente". Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 14.

[835] El texto del Anteproyecto estaba redactado en los siguientes términos:

"Artículo 6. Normas generales sobre cesión de datos.

1. Los datos conservados de conformidad con lo dispuesto en esta ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella o en otras normas con rango de ley, y para los fines que en ellas se determinan.

compuesto de dos apartados y bajo la rúbrica "normas generales sobre cesión de datos", establece un principio general al respecto, conforme al cual los datos conservados de conformidad con la LCD "sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial"[836]. Como puede apreciarse, el precepto se limita a enunciar la obligación de cesión, dejando los detalles sobre cómo debe ser ejecutado para los posteriores artículos 7, 9 y Disposición Final Cuarta[837].

La cesión de los datos constituye el instrumento adecuado para satisfacer la finalidad mediata de la conservación, esto es, permitir que aquellos datos que se revelen de interés para la detección, investigación o enjuiciamiento de delitos graves sean facilitados a las autoridades encargadas de dichas actividades. La LCD incardina adecuadamente en el término "cesión" el tipo de medida que supone la transmisión de los datos conservados a los agentes facultados. La LOPD define la "cesión" como "toda revelación de datos realizada a una persona distinta del interesado"[838].

Por su parte, el segundo apartado del art. 6 LCD pasa a abordar la delicada cuestión acerca de cuáles son las concretas autoridades públicas que tienen la consideración de "agentes facultados", y por tanto, son competentes para recabar los datos conservados. El legislador español, siguiendo de cerca una vez más lo dispuesto en la Directiva, hace suyo el concepto de agente facultado —ya adoptado por el RLGT en su art. 84.e)—

---

2. La cesión de la información se efectuará únicamente a los agentes facultados. A estos efectos, tendrán la consideración de agentes facultados los miembros de las fuerzas y cuerpos de seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial; el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia; así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal".

[836] Cf. art. 6.1 LCD.

[837] La decisión debe ser valorada positivamente, si tenemos presente la ausencia de regulación detallada al respecto en el precedente legislativo de la conservación de datos, el derogado art. 12 LSSI.

[838] Cf. art. 3.i) LOPD.

como destinatario de la información que ha de ser objeto de cesión. A estos efectos designa como tales los siguientes:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de Policía Judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial —en adelante, LOPJ—.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como Policía Judicial, de acuerdo con el art. 283.1 LECrim.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia[839].

---

[839] La redacción primitiva era más imprecisa. El art. 6 del Anteproyecto constaba de dos apartados. El primero de ellos contenía una regla general cuyo sentido era confuso y cuya redacción fue aclarada a sugerencia del Consejo de Estado —apart. B.III del Dictamen 32/2007— y de la AEPD. Se atribuía tal consideración, en primer lugar, a "los miembros de la Policía judicial, en los términos establecidos en el artículo 547 de la Ley Orgánica del Poder Judicial". Si el primer inciso parecía evocar una concepción orgánica de la Policía judicial, el segundo evidenciaba que se partía de una concepción funcional, que es la que inequívocamente refleja el art. 547 LOPJ a que se remitía. Convenía por tanto aclarar —como sugirió el CGPJ en su Informe— que la referencia a la Policía Judicial comprendía no sólo a los miembros de las unidades orgánicas de Policía Judicial, sino también a los agentes de las Fuerzas y Cuerpos de Seguridad del Estado que, sin participar de dicho encuadramiento orgánico, ejercen funciones de Policía Judicial, atendiendo al hecho de que en nuestro ordenamiento esta función, comprensiva del auxilio a los Juzgados y Tribunales y al Ministerio Fiscal en la averiguación de los delitos y en el descubrimiento y aseguramiento de los delincuentes compete —cuando fueren requeridos para prestarla— a todos los miembros de las Fuerzas y Cuerpos de Seguridad, tanto si dependen del Gobierno Central como de las Comunidades Autónomas, o de los Entes Locales, dentro del ámbito de sus respectivas competencias –vid. Título III del Libro VII, arts. 547 a 550 LOPJ, LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, y RD 769/1987, de 19 de junio—. De ahí que el Consejo de Estado sugiriera que se atribuyese la condición de agentes facultados a todos "los miembros de las fuerzas y cuerpos de seguridad, cuando desempeñen funciones de Policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica del Poder Judicial". Esta es la redacción que finalmente figura en el art. 6.2.a) LCD.

Este elenco de agentes de la LCD ha sido considerado excesivo por algunos autores —como, por ejemplo, RODRÍGUEZ DELGADO[840]— en cuanto incluye a los funcionarios de Vigilancia Aduanera, que el artículo 283 LECrim ni siquiera designa expresamente como Policía Judicial, como sí hace con otras figuras tales como los alcaldes, los serenos o los guardas de montes[841]. A pesar de la omisión, no hay obstáculo para que tales funcionarios se entiendan incluidos en la referencia del mismo artículo a "las autoridades administrativas encargadas de la seguridad pública y de la persecución de todos los delitos o de algunos especiales", y que constituyen —todos ellos— "la Policía Judicial y son auxiliares de los Jueces y Tribunales competentes en materia penal y del Ministerio fiscal, quedando obligados a seguir las instrucciones que de aquellas autoridades reciban a efectos de la investigación de los delitos y persecución de los delincuentes"[842]. No obstante, el hecho de que los agentes de aduanas —encargados principalmente del tráfico entre fronteras— conozcan de los delitos graves enmarcados en el ámbito de la LCD y de cuya investigación se ocupa tanto el CNI[843] como los Cuerpos y Fuerzas de Seguridad, sí que puede parecer excesivo en cuanto se trata de "darle potestad a un órgano, no designado expresamente por la ley como Policía Judicial, de unas atribuciones que deben ser tratadas con "delicadeza" por la ley, en especial cuando estamos hablando de datos sensiblemente personales, como es lo relativo a las comunicaciones electrónicas"[844].

En cualquier caso, entendemos que la norma no debe llevarnos a equívoco, pues cuando los agentes de aduanas actúan como "agentes facultados" por la LCD, están al mismo tiempo y en todo caso operando como Policía Judicial[845]. Si bien los

---

[840] Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 6.

[841] Cf. art. 283.3, 4 y 6 LECrim.

[842] Cf. art. 283.1 LECrim.

[843] Sobre la posición constitucional del CNI, cf. Ruiz Miguel, C., Servicios de inteligencia y seguridad del estado constitucional, Tecnos, 2002.

[844] Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 7.

[845] Acerca de las funciones de la Policía Judicial existen monografías buenas pero no actualizadas, cf. Martínez, R., Policía judicial y Constitución, Editorial Aranzadi, Pamplona, 2001; Sala i Donado, C., La policía judicial, McGraw-Hill Interamericana de España, Madrid, 1999; Magro Servet, V., Manual práctico de actuación policial-judicial en medidas de limitación de derechos fundamentales, La Ley, Madrid, 2006. No obstante, últimamente puede destacarse el artículo de López Rodríguez, J. A., "La

destinatarios de la información pudieran ser ellos mismos o la autoridad judicial que los comisiona para que recaben la información de los operadores obligados, resulta en todo caso evidente que en uno y otro supuesto la autoridad judicial que autoriza u ordena la cesión de datos es realmente el verdadero destinatario de la información y el garante de la proporcionalidad y necesidad de la medida de cesión. De hecho, el art. 547 LOPJ[846] concibe la Policía Judicial desde su dimensión de colaboración o auxilio a la autoridad judicial en su función investigadora[847].

En relación con esto, conviene añadir que el Juez competente para el acuerdo o autorización será quien resulte competente conforme a las normas de competencia objetiva y territorial definidas en los arts. 14 y 15 LECrim, mientras que en el supuesto de la actuación del CNI, el verdadero destinatario de la información será el Magistrado del Tribunal Supremo designado para tal menester.

De lo previsto en la LCD parece desprenderse una concepción del proceso penal en que las labores de investigación se atribuyen con carácter general a la Policía, limitándose el Juez a habilitar a ésta para proceder a la injerencia en los derechos fundamentales afectados. El legislador parece así ignorar —en observación de GONZÁLEZ LÓPEZ[848]— que, independientemente de lo acertado o no de este panorama a la luz de los niveles de especialización y profesionalización alcanzados por la Policía, lo cierto es que la investigación penal corresponde, con arreglo a nuestro actual modelo procesal penal, a los Jueces instructores y, en su caso, al Ministerio Fiscal, en tanto la Policía Judicial dispone de competencias investigadoras por propia autoridad sólo en supuestos de

---

Policía Judicial y la obsoleta Ley de Enjuiciamiento Criminal", en Diario La Ley, Nº 7637, 2011, donde se adelantan algunas de las tesis aquí expuestas.

[846] Dispone el citado precepto que "la función de la Policía Judicial comprende el auxilio a los juzgados y tribunales y al Ministerio Fiscal en la averiguación de los delitos y en el descubrimiento y aseguramiento de los delincuentes. Esta función competerá, cuando fueren requeridos para prestarla, a todos los miembros de las Fuerzas y Cuerpos de Seguridad, tanto si dependen del Gobierno central como de las comunidades autónomas o de los entes locales, dentro del ámbito de sus respectivas competencias".

[847] Así, a mayor abundamiento, hemos de recordar que en la interceptación legal de comunicaciones se utiliza el término "habilitado" para definir la actuación del agente, y los verbos "acordar" o "autorizar" para definir la actuación de la autoridad judicial.

[848] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit, p. 19.

actuación "a prevención". Sólo así se explica que en la LCD se identifique, sin ninguna matización, como exclusivos destinatarios de la cesión a los agentes facultados —la Policía o Vigilancia Aduanera[849]—, sin mención a los Jueces y Fiscales, que deberían ser los destinatarios de la información comunicada, previo control judicial en todo caso, disponiendo la Policía Judicial de la información únicamente en la medida en que actúen como auxiliares de estos órganos, que son los competentes para dirigir la investigación penal[850]. En cambio, parece obviarse la necesidad de control judicial de la medida cuando en el artículo 6.2 LCD se dispone que "la cesión de la información se efectuará únicamente a los agentes facultados". Como indica GONZÁLEZ LÓPEZ, "a la luz de esta previsión, cabe cuestionarse con qué garantías contará el sujeto afectado por la cesión de que ésta se ha llevado a cabo con arreglo a lo establecido en la resolución judicial habilitante"[851]. Además, como bien señala el mismo autor, la previsión supone una "clara incoherencia" con el planteamiento de la Ley en materia de secreto de las comunicaciones, ya que "si este derecho se ve afectado por la cesión, resulta aún más exigible que se realice el control judicial, reiteradamente identificado por la jurisprudencia como uno de los requisitos propios de la limitación de este derecho con fines de persecución penal"[852]. En todo caso, aunque se pretenda interpretar el precepto en el sentido de que, en última instancia, los datos serán puestos en conocimiento de la Policía Judicial, como comisionada del órgano director de la investigación —lo que desafortunadamente no parece desprenderse del tenor literal— no resulta admisible que se ignore el papel que el Juez o Fiscal desempeñan en nuestro actual modelo de proceso penal, que precisamente encuentra eco en el art. 11.2.d) LOPD[853]. Por otra parte, si vinculamos la previsión legal a las actuaciones "a prevención" de la Policía Judicial, no resulta lógico que la Policía aparezca como cesionaria directa, ya que desde el

[849] El CNI escapa a estas consideraciones, por ser su función la salvaguarda de la seguridad nacional.

[850] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit, p. 20.

[851] Ibíd.

[852] Ibíd.

[853] Dispone el art. 11.2.d) LOPD —*Comunicación de datos*—, que el consentimiento del interesado exigido para la cesión de datos no será preciso: "d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas".

momento en que el Juez ha debido autorizar la cesión, debe procederse a la incoación del correspondiente proceso penal y, por tanto, el Juez competente deberá hacerse cargo de la investigación. En definitiva, habiéndose establecido la exigencia de resolución judicial habilitante, lo coherente con dicho presupuesto es que los datos sean cedidos al órgano judicial a fin de que efectúe el control de la medida realizada y que, una vez efectuado éste, sea él el que facilite los datos recabados a los agentes facultados[854].

Así pues, la actuación previa de la Policía Judicial en su labor de investigación, cuando aún no hay causa judicial abierta, legitima la solicitud de acceso a la información contenida en las bases de datos de los distintos operadores: no es necesario que la habilitación jurisdiccional venga precedida de una investigación judicial en curso. Una vez instada la autorización judicial para tal acceso, la autoridad judicial tendrá conocimiento de los hechos y habrá de iniciar una actuación de investigación por su cuenta a la que se supeditará, desde entonces, la investigación policial. Como sucede en la intervención de las comunicaciones, la apertura de la instrucción puede derivar de la solicitud de cesión dirigida por las autoridades que actúan en funciones de policía judicial. Los únicos supuestos en que la Policía, por razón de sus competencias, debería ser en rigor considerada destinataria de la cesión son los de prevención de delitos, es decir, justamente cuando desempeña las labores que no corresponden a las de Policía Judicial y que, por tanto, a tenor de la Ley, no legitiman la cesión de datos de las comunicaciones.

Por otra parte, no puede pasar inadvertido el hecho de que el legislador parece haber rehuido la consideración del Ministerio Fiscal como destinatario de la información —como sí hacía el art. 12.3 LSSI—, consideración que siempre vendría condicionada por la necesaria autorización judicial previa, tal y como se establecía tanto en la anterior como en la actual redacción del art. 5 de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal. De este modo, nuestra norma

[854] A la luz de esta previsión, cabe cuestionarse con qué garantías contará el sujeto afectado por la cesión de que ésta se ha llevado a cabo con arreglo a lo establecido en la resolución judicial habilitante. Es más, supone una clara incoherencia con el planteamiento de la Ley en lo tocante al secreto de las comunicaciones, ya que, si éste derecho se ve afectado por la cesión, resulta aún más exigible que se realice el control judicial, reiteradamente identificado por la jurisprudencia como uno de los requisitos propios de la limitación de este derecho con fines de persecución penal.

veda definitivamente el acceso del Ministerio Fiscal a tal información en el desempeño de sus funciones investigadoras, en un contexto normativo un tanto ambiguo, pues lo que se les faculta en el art. 11.2 d) LOPD[855], ahora se les niega por la LCD. Frente a esta opinión, —mantenida por RODRÍGUEZ LAINZ[856]— opina GONZÁLEZ LÓPEZ[857] que la no conceptuación de la Fiscalía como destinatario de los datos en la LCD obedece a "la confusión reinante acerca del papel que corresponde a cada sujeto interviniente en el proceso penal en relación con la cesión de datos".

Mucho más problemática, en un plano diferente, es la distinción entre el agente facultado y el destinatario de la información almacenada en los libros-registro de servicios de telefonía por tarjeta de prepago, regulados en la Disposición Adicional Única de la LCD, sobre cuya complejidad legal y constitucional volveremos en detalle en la última parte de esta Tesis.

34.2 Procedimiento de cesión de datos

Continuando nuestro examen del articulado, y una vez que la LCD ha desarrollado las obligaciones principales de los prestadores de servicios de telecomunicaciones y designado *à sa façon* cuáles serán los agentes facultados para recabar los datos conservados, la cesión de los mismos es objeto de regulación por parte del art. 7 LCD[858], que se compone de tres apartados recogidos bajo la rúbrica "procedimiento de

---

[855] No obstante, hemos de reconocer que el art. 11.2 d) LOPD no parece que llegue a establecer a favor del Ministerio Público una facultad de injerencia sobre el derecho a la protección de los datos de carácter personal en el marco de la investigación y persecución de los delitos, una excepción a la regla general de la exclusión de tal facultad descrita en el art. 5.2 de su Estatuto Orgánico, respecto de la cual —y mientras no llegue a producirse una reforma radical del sistema de investigación criminal— debe entenderse que prevalece el principio de reserva de decisión judicial.

[856] Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (I), op. cit., p. 15.

[857] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit, p. 20.

[858] Transcribimos aquí el tenor literal del precepto para su directo examen:

"Artículo 7. Procedimiento de cesión de datos.

cesión de datos". El precepto se inicia declarando que los operadores están obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 —las categorías de datos ya examinadas— concernientes a comunicaciones que identifiquen a personas[859], previa la obtención de una resolución judicial que ha de determinar, conforme a lo previsto en la LECrim y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados[860]. La previsión de su determinación por el Juez es —además de un aspecto clave para la constitucionalidad de la norma— la forma de asegurar que no se produzca una extracción de datos a gran escala —como advertía el GT29 en su Dictamen 3/2006—, puesto que el Juez ha de proceder a dicha determinación con arreglo al principio de proporcionalidad en sentido estricto.

El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial "atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación"[861]. No obstante, el apartado 3 dispone en su segundo párrafo que si no se establece otro plazo distinto, la cesión debe efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 a.m.

---

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden".

[859] Cf. art. 7.1 LCD.

[860] Cf. art. 7.2 LCD.

[861] Cf. art. 7.3 LCD.

del día laborable siguiente a aquél en que el sujeto obligado reciba la orden. Conforme a la opinión de GONZÁLEZ LÓPEZ, tal previsión legal subsidiaria del acuerdo judicial a falta de fijación de plazo distinto debe valorarse como perfectamente aceptable[862].

Así pues, como vemos, la LCD deja primeramente a la discrecionalidad del Juez el plazo "razonable" para que el cumplimiento de la obligación de cesión se lleve a cabo, según la necesidad del caso concreto, así como a la proporcionalidad[863] del beneficio de la medida en relación a la injerencia infligida. Cabe hacer notar que la exigencia de que el plazo de ejecución de la orden de cesión se fije en la autorización judicial "atendiendo a la naturaleza y complejidad técnica de la operación" no resulta el más prudente criterio —como, por otra parte, ya puso de relieve el Consejo de Estado[864]—, pues no parece que el titular de un órgano judicial sea el más indicado para calibrar las susodichas "naturaleza y complejidad técnica", en tanto que las tales podrían ser distintas para cada operador en función de la configuración de sus equipos y de sus propios medios tecnológicos. Por contra, no cabe sino reconocer mayor peso a otros elementos no menos relevantes para la fijación del plazo, como pueden ser la mayor o menor urgencia de la cesión —a la que se refiere también el art. 7.3 LCD—, a efectos de la investigación o enjuiciamiento de que se trate en cada caso.

Cabe señalar que el Anteproyecto[865] preveía un plazo aún más breve —cuarenta y ocho horas— para aquellos datos con una antigüedad inferior a tres meses[866]. Dicha

---

[862] Cf. González López, J. L., Comentario a la Ley 25/2007…, op. cit., p. 24.

[863] Aunque resulte muy adecuada la previsión de que los datos que deban ser cedidos sean determinados en la resolución habilitante con atención al principio de proporcionalidad y necesidad, la referencia a este segundo principio es un subprincipio del de proporcionalidad. Acerca del principio de proporcionalidad, cf. Pedraz Penalva, E., "Principio de proporcionalidad y principio de oportunidad", en Constitución, jurisdicción y proceso, Akal, Madrid 1990, pp. 313-376.

[864] Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.B.4.

[865] La redacción original de la norma disponía lo siguiente:

"Artículo 7. Procedimiento de cesión de datos.

1. Los operadores estarán obligados a ceder al agente facultado, previa resolución judicial, los datos conservados a los que se refiere el artículo 3 de esta ley.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

previsión fue modulada tanto por sugerencia del Consejo de Estado[867] como a la vista de las alegaciones vertidas desde el sector de las telecomunicaciones, de las que ya dimos cuenta. No obstante, el legislador no perdió de vista el hecho de que, de acuerdo con el artículo 8 de la Directiva, los datos deben poder transmitirse "sin demora cuando las autoridades competentes así lo soliciten"[868]. En todo caso, compartimos la opinión de RODRÍGUEZ DELGADO para quien se trata un período de tiempo asequible para las empresas prestadoras de servicios de telecomunicaciones, que, a fin de cuentas, deben hacer dicha cesión de forma electrónica[869]. No obstante, quizás hubiese sido más

---

3. El plazo de ejecución de la orden de cesión será el fijado por los agentes facultados, atendiendo a la urgencia de la cesión a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación. Si no se establece otro plazo distinto, la cesión deberá efectuarse:

a) Cuando los datos tengan una antigüedad inferior a tres meses, dentro de cuarenta y ocho horas contadas a partir de las 8,00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden.

b) Cuando los datos tengan una antigüedad superior a tres meses, dentro de setenta y dos horas contadas a partir de las 8,00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden".

[866] Podría entenderse que la fijación de plazos de cuarenta y ocho y setenta y dos horas en función de que la antigüedad de los datos sea inferior a superior a tres meses respectivamente que hace el Anteproyecto —artículo 7.3— obedecía a la mayor dificultad técnica que se presume en este segundo caso para facilitar los datos. Esta razón, de ser la subyacente, es, sin embargo, discutible, ya que el tratamiento informatizado de la información almacenada no parece susceptible de ralentizarse por la antigüedad de los datos, sino por otras características como la concreción del dato que se busca, por lo que parece adecuado fijar un plazo común. En cualquier caso, no debe descartarse la existencia de complicaciones técnicas, pues precisamente el volumen de información que ha de manejarse sirvió de argumento a Vodafone España, S.A. para reclamar la fijación de los dos plazos de entrega que se plasmaron en el Proyecto (aunque con diferente duración de la antigüedad de referencia frente a lo que planteaba la empresa que señalaba un plazo de 48 horas para datos relativos a los tres últimos meses y setenta y dos para datos de antigüedad superior a 9) y que finalmente se refundieron en el más largo en la LCD. Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, antecedente quinto.

[867] Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.4.

[868] Al respecto, el Consejo de Estado echó en falta aquí algún estudio sobre las consecuencias económicas de las distintas soluciones posibles —puesto que ese había sido el principal argumento esgrimido para interesar una ampliación del plazo—, como podría ser, entre otras, la fijación de unos plazos residuales más holgados, permitiendo al órgano judicial reducirlos al máximo, incluso por debajo de los ahora previstos, por razones de urgencia o en función de las circunstancias concurrentes en cada caso. Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.B.4.

[869] Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 11.

conveniente establecer el plazo a contar, no desde las 8:00 a.m. del día siguiente, sino a última hora del día en que se solicita la cesión, ya que el horario de trabajo de los prestadores de servicios, como es natural, no comienza antes de dicha hora, por lo que en realidad el plazo se acorta a última hora de la tarde del día anterior, que es la hora real en que se cederán los datos solicitados. Aun así el plazo estándar de tres días para enviar de forma electrónica unos datos de tráfico almacenados por el prestador de servicios parece de todo punto razonable.

En lo tocante a la resolución judicial habilitante —que, en cuanto debe ser motivada, deberá adoptar la forma de auto—, no se acierta a entender la alusión que se hace en el art. 7.2 LCD a la LECrim como referencia normativa para establecer los datos que han de ser cedidos a los agentes facultados[870]. Esta mención podría interpretarse como una alusión a la incardinación de la medida en el marco de la investigación penal y, de este modo, a los fines del proceso penal, de manera que los datos recabados se restrinjan a aquellos precisos para averiguar el delito e identificar el delincuente. GONZÁLEZ LÓPEZ es partidario, en este sentido, de contemplar dicho apartado como:

> "la previsión legal de que la cesión de datos ha de partir de la existencia de indicios de comisión de un hecho delictivo que se dirijan contra un sujeto determinado, ya sea como sospechoso de autoría o como susceptible de aportar información acerca del delito y/o de su autor (principio de intervención indiciaria) y ajustarse a las exigencias de idoneidad, necesidad y proporcionalidad en sentido estricto, en referencia, por lo que se respecta a este último subprincipio, a la exigencia de que los datos recabados deberán ser exclusivamente los precisos para las finalidad a que se adscribe la medida" [871].

Las confusiones derivadas de la ambigua y desacertada expresión "sin perjuicio", del apartado 1 del art. 7 —"los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el art. 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente"—, han quedado solventadas tras el Acuerdo de la Sala Penal del TS de 23 de febrero de 2010, que ha venido a disponer que es necesaria la autorización judicial para que los operadores que prestan servicios de

[870] Acerca de los requisitos de la resolución, cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (y II), op. cit., p. 3.

[871] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 21.

comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo; "por lo cual" —indica la resolución— "el Ministerio fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007, de 18 de octubre"[872].

El régimen de cesión de los datos continúa su desarrollo en la Disposición Final Cuarta de la Ley 25/2007, de 18 de octubre, que bajo la rubrica "formato de entrega de los datos", esboza en sus dos apartados algunos detalles sobre el procedimiento mediante el cual los datos conservados deben propocionarse por los proveedores a las correspondientes autoridades.

Al respecto, indica su apartado primero que la cesión a los agentes facultados de los datos cuya conservación es obligatoria, se efectuará "en formato electrónico", en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses[873] desde la entrada en vigor de la Ley[874]. Dicha Orden no ha sido aún aprobada. Obviamente, el hecho de

---

[872] Siendo la cuestión abordada la siguiente: Segundo Asunto: Si el Ministerio Fiscal precisa de la autorización judicial para que le sea desvelada la identidad de la persona adjudicataria de la dirección IP con la que operan los ciudadanos en Internet".

[873] El primer borrado del Anteproyecto fijaba un plazo inicial de un mes para que se dictara la orden ministerial —Disposición Final Cuarta del Anteproyecto—. Tanto el Consejo de Estado como la Secretaría General Técnica del Ministerio del Interior, durante la tramitación de la norma, consideraron inadecuada la fijación del plazo, por lo que se propuso su supresión o bien la fijación de un plazo más realista. Esta es la opción finalmente seguida, extendiendo tal plazo a los tres meses, por haberse calificado como poco realista la primera. Sin embargo, algunos operadores defendieron que el plazo de adaptación previsto en el apartado 1 debía computarse a partir de la aprobación de la Orden, puesto que la adaptación estaría condicionada por los términos de éstas. El propio Consejo de Estado estimó conveniente que se estableciera un plazo máximo cuya brevedad no debía "verse como un obstáculo cuando todavía no ha comenzado la tramitación parlamentaria de la ley, de forma que la preparación de dicha orden mientras se tramita la ley permitiría una aprobación de la orden prácticamente inmediata tras la aprobación de aquella, facilitando así también la más rápida adaptación de los sujetos obligados y, en consecuencia, la más pronta disponibilidad de instrumentos útiles para la investigación, detección y enjuiciamientos de delitos". Nada de esto, sin embargo, ha tenido lugar. Al respecto, cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.B.4.

[874] La redacción proyectada del apartado 1 de la Disposición Adicional Cuarta establecía que la cesión a los agentes facultados de los datos se efectuaría en la forma que se determine por Orden del Ministro del

que la parte esencial del protocolo de cesión de los datos —el formato electrónico para la cesión— haya quedado pendiente de un posterior desarrollo reglamentario no debe llevarnos —así lo ha advertido RODRÍGUEZ LAINZ[875]— al sencillo argumento, quizás apetecido por las operadoras de telecomunicaciones, de que la obligación de cesión habría de quedar en suspenso hasta tanto no se dicte la Orden Ministerial de desarrollo, puesto que nos hallamos ante una simple norma de homologación de formatos electrónicos que no impide el cumplimiento de las obligaciones mediante su remisión en papel impreso o en formatos electrónicos compatibles con los sistemas operativos utilizados por los cesionarios, como realmente se está haciendo hasta la fecha. A falta de la debida homologación, que debería atender a la problemática del código abierto o cerrado que se utilice, indica GONZÁLEZ LÓPEZ que la fijación del formato se presenta como una cuestión de especial relevancia, ya que resulta susceptible de convertirse en fuente de objeciones procesales a la información aportada[876]. En defecto de homologación, es aconsejable que el formato quede señalado en la resolución judicial habilitante[877].

Igualmente desafortunado es lo que acontece con la previsión del apartado segundo de la Disposición Final Cuarta, conforme al cual los operadores obligados dispondrían de

---

Interior o del Ministro de Defensa, "según correspond[ier]a por la dependencia del Agente Facultado". Tal inciso fue criticado por cuanto obligaba a cada operador a una mayor disponibilidad de medios para realizar la cesión en dos formas diferentes, según cuál fuera la dependencia del agente facultado. A juicio del Consejo de Estado, era a la Administración a quien correspondía "coordinar sus medios y sus necesidades, y fijar de manera unitaria el modo en que haya de realizarse la cesión, en formato electrónico". Por añadidura, tal orientación hubiera planteado la existencia de otras dependencias de los agentes facultados: autonómica o local —si se trataba de dependencia orgánica— o de la Administración de Justicia —si de dependencia funcional—, pudiendo así multiplicarse las exigencias sobre la forma de practicar la cesión. El desacierto fue por fortuna enmendado en el texto finalmente aprobado, si bien la Administración, a la hora de aprobar la Orden, debería tener en cuenta tales observaciones. Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.B.4.

[875] Cf. Rodríguez Lainz, J. L., El principio de proporcionalidad… (y II), op. cit., p. 6.

[876] En relación con la problemática acerca del uso de códigos cerrados por las fuerzas policiales, cf. Pérez Gil, J., "Investigación penal y nuevas tecnologías: algunos de los retos pendientes", Revista Jurídica de Castilla y León, n. 7, octubre 2005, pp. 211-234.

[877] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit, p. 25. También del mismo autor, cf. Los datos de tráfico..., op. cit., p. 362.

un plazo de seis meses desde la entrada en vigor de la LCD para configurar, "a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos" [878]. Y es que, tal como se desarrollaron los acontecimientos, con la aprobación de esta disposición el legislador estaba *per se* incurriendo en un incumplimiento de los plazos de incorporación marcados por la Directiva. Como ya hemos dicho, aunque España disponía del plazo de dieciocho meses desde la adopción de la Directiva para implementarla en el ordenamiento nacional interno, nuestro país no cumplió dicho plazo dado que la LCD entró en vigor el 8 de noviembre de 2007, es decir, casi dos meses después del límite fijado por el art. 15.1 de la Directiva 2006/24/CE, conforme al cual los Estados miembros debían poner "en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar el 15 de septiembre de 2007". Si tenemos en cuenta que, como estamos viendo, la Disposición Final Cuarta, párrafo segundo, emplazaba a los proveedores a configurar sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos en los seis meses siguientes a la entrada en vigor de la LCD, esto nos lleva a concluir que la ley española sólo estuvo en condiciones de dar cumplida satisfacción a la Directiva a partir del 9 de mayo de 2008. El retraso total acumulado en la puesta en marcha de la normativa se revela así, en realidad, de ocho meses. Es evidente que tal dilación fue ya aparente para el Consejo de Estado, pues en su Dictamen, se adelantó a advertir explícitamente que si antes de los seis meses un determinado operador estaba en disposición de cumplir las obligaciones sobre conservación de datos, debería hacerlo, "de modo que la persona investigada no podrá ampararse en la falta de vigencia de la ley proyectada para impedir u oponerse a la cesión de los datos que se recaben de acuerdo con ella"[879].

[878] Cf. Disposición Final Cuarta, apart. segundo, LCD.

[879] Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.F.3.

35 Excepciones a los derechos de acceso y cancelación

El art. 9 LCD está dedicado a la regulación de la exceptuación de los derechos de acceso y cancelación que la LCD representa en el ámbito de la normativa sobre protección de datos. En primer lugar, el art. 9.1 LCD indica que el responsable del tratamiento de los datos no comunicará la cesión de los datos conservados efectuada de conformidad con la LCD. En segundo lugar, el art. 9.2 LCD dispone que el responsable del tratamiento de los datos debe denegar el ejercicio del derecho de cancelación en los términos y condiciones previstos en la LOPD[880]. Este art. 9 LCD —al que se remite igualmente el apart. 3 de la Disposición Adicional Única—, no deja de ser una consecuencia lógica del carácter impositivo de unos ficheros de datos de carácter personal de origen legal[881].

---

[880] Dispone el tenor literal del precepto lo siguiente:

"Artículo 9. Excepciones a los derechos de acceso y cancelación.

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre".

[881] No está de más reseñar que el contenido del art. 9 del Anteproyecto era bastante diferente al finalmente aprobado. Bajo la rúbrica "Excepciones a los derechos de acceso, rectificación y cancelación", disponía que el responsable del tratamiento de los datos "denegará el ejercicio de los derechos de acceso, rectificación y cancelación [...] cuando el afectado esté siendo objeto de investigación de un delito". Al respecto, señalaba el Consejo de Estado que la LOPD regula el derecho de acceso en su artículo 15 pero no prevé la denegación del acceso solicitado —sin perjuicio de la periodicidad o acreditación que exige su apartado 3—. La rectificación y cancelación, en cambio, están reguladas en el art. 16 LOPD, en el que se prevé expresamente que los datos "deberán ser conservados durante los plazos previstos en las disposiciones aplicables" lo que determina que no procede la cancelación de los datos que pudiera instar el afectado en tanto no se haya cumplido el plazo de conservación legalmente previsto. "Si el artículo 16.5 puede amparar una excepción al derecho de cancelación —razonaba el Consejo de Estado en su Dictamen—, es más dudoso que permita excluir el derecho de rectificación, puesto que parece que la rectificación habría de admitirse si los datos fueran efectivamente erróneos, en aplicación de lo previsto en la Ley Orgánica 15/1999 y, en particular, en relación con la calidad de los datos (artículo 4), y sin perjuicio de que el derecho de rectificación pueda modularse en el supuesto de que ahora se trata, a fin de garantizar al máximo su procedencia y justificación (la inexactitud de los datos preexistentes, etc.)".

Respecto de la exceptuación del deber de recabar el consentimiento del afectado que plantea el art. 9.1 LCD, hemos de señalar que, si bien el art. 6.1 LOPD establece que el tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado, el mismo precepto advierte *in fine* que este principio despliega su eficacia "salvo que la ley disponga otra cosa". De este modo, si la ley —la LCD, en nuestro caso— es la fuente misma de la regulación de unos ficheros que son completamente ajenos a la voluntad o consentimiento de los ciudadanos, se echa de ver claramente que la cesión de estos datos a los agentes facultados, bajo la salvaguardia de la autoridad judicial, se excepciona del principio del consentimiento con completa legitimidad[882].

Más allá de esto, hemos de matizar que, mientras que el secreto en lo referente a la actuación del CNI es connatural a la propia actuación de tal organismo público y a los fines a los que está destinado, la excepción consagrada por el art. 9.1 LCD, cuando se incardina en un proceso penal, hace que la comunicación de la existencia del acto de injerencia a los interesados dependa de las normas sobre el secreto sumarial recogidas en el art. 302 LECrim. Ello comporta que, en este último supuesto, si bien el responsable del fichero está eximido del deber de comunicación de la cesión del mismo a un tercero, el acto de injerencia deberá ser comunicado a la persona afectada en todos

---

También suscitaba importantes reservas la denegación del derecho de acceso que imponía el art. 9 del Anteproyecto, teniendo en cuenta que el art. 15 LOPD no prevé exclusión alguna de ese derecho —derecho de acceso que, al menos *a priori*, no parece que deba perjudicar, por sí, los fines a que se orienta la lcd—. De este modo, se sugirió que la finalidad perseguida con esa denegación del acceso se obtendría mejor excluyendo el conocimiento, por parte del interesado, de la cesión efectuada —esto es, de que los datos de la persona investigada han sido comunicados a los agentes facultados—, lo que podría buscar amparo en los artículos antes citados de la LOPD —y, en particular, en el artículo 11.2.a), en relación con el 27, sobre comunicación de la cesión de datos—. Así se explica la redacción del actual art. 9.1 LCD. Al respecto, cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.4.

[882] Discrepamos así del criterio de GONZÁLEZ LÓPEZ, para quien "una previsión de este tipo [en referencia al art. 9 LCD] es claramente inconstitucional, por vulnerar la reserva material a favor de ley orgánica del desarrollo de los derechos fundamentales [cf. art. 81 CE], que la LOPD claramente confirma, al tener sus artículos 16 y 18 —que prevé la posibilidad de acudir a la AEPD en caso de actuaciones contrarias a lo dispuesto en dicha Ley— carácter de ley orgánica —de acuerdo con lo previsto en su Disposición Final Segunda—, por hallarse en el Título III. El artículo 9.2 LCD implica, por tanto, una ilegítima restricción del derecho de cancelación del titular de los datos". Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit. p. 28.

aquellos supuestos en los que no se haya declarado previa o simultáneamente a la orden de cesión el secreto de las actuaciones, conforme a las normas generales de nuestro enjuiciamiento criminal. Nada cabe oponer, *a priori*, a la previsión de que el responsable del tratamiento de los datos no comunique la cesión efectuada con arreglo a lo dispuesto en la Ley, si entendemos por tal responsable al "sujeto obligado". La previsión indicada es adecuada siempre que se entienda que el responsable del tratamiento es el sujeto obligado, porque la atribución de tal condición no es algo que la Ley haga expresamente ni que resulte claro. De acuerdo con la definición de "responsable del fichero o tratamiento" que ofrece el art. 3.d) LOPD, dicho concepto se aplica a la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". Si atendemos al hecho de que tanto la finalidad y el contenido de la conservación de los datos, como el posible uso de éstos aparecen claramente delimitados en la Ley, resulta cuestionable calificar de "responsable" al sujeto obligado en lo tocante a la conservación efectuada con el fin de satisfacer los objetivos de la LCD, ya que su poder de decisión es prácticamente nulo. De hecho, su papel se asemeja más al de "encargado del tratamiento" —figura regulada en el art. 3.g) LOPD— por cuenta de las disposiciones legales al respecto. Por otra parte, la confusa redacción de la Ley plantea la duda de si con el término "responsable del tratamiento" la Ley se está refiriendo al responsable del tratamiento que comporta la conservación de los datos o al que supone la cesión y tratamiento posterior de los datos cedidos. Esta segunda posibilidad, que no es descartable a tenor de la Ley, debe, sin embargo, rechazarse, en opinión de GONZÁLEZ LÓPEZ, ya que una lectura del artículo 9 LCD en estos términos "sería claramente incompatible con el derecho de defensa y el derecho a la protección de los datos de carácter personal, los cuales, si bien admiten su puntual limitación, determinan que en un momento dado la cesión y posterior tratamiento de los datos deban ser puestos en conocimiento del imputado y del titular de los datos, respectivamente"[883].

En conexión con lo anterior, y dado que la cesión debe ser acordada por el órgano judicial, resulta lógico —aunque nada dice la LCD al respecto— que sea éste, y no el sujeto obligado, el que deba compatibilizar las necesidades de la investigación, que

[883] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 28.

pueden comportar la de asegurar la clandestinidad de la cesión, a fin de que el titular de los datos, prevenido por la adopción y práctica de la cesión, no oculte o destruya informaciones u otros elementos de interés para el esclarecimiento de los hechos investigados, o altere su conducta posterior, con el derecho de defensa del imputado y, en todo caso, el derecho a la protección de los datos de carácter personal del titular de los datos[884]. Puesto que el acuerdo por el Juez de la cesión debe comportar —con la única excepción posible del procedimiento de menores— la atribución a éste de la dirección de la investigación, y puesto que, en todo caso, abierta la instrucción, como resulta necesariamente de acudir al órgano judicial para practicar la cesión, el acuerdo del secreto instructorio corresponde en todo caso al Juez, será éste quien, en aras de la investigación, deba resolver motivadamente sobre la restricción de los derechos afectados, como han puesto de manifiesto tanto GONZÁLEZ LÓPEZ como RODRÍGUEZ LAINZ[885].

Por otra parte, acerca del derecho de cancelación al que se refiere el art. 9.2 LCD, y entendiendo que el responsable del tratamiento es el sujeto obligado, dicha disposición suscita importantes cuestiones. En primer lugar, debe destacarse que de la excepción al derecho de cancelación se desprende que el titular de los datos se halla informado de la existencia del tratamiento de sus datos, ya que sólo conociendo —o, al menos, intuyendo— la existencia del tratamiento resulta comprensible que acuda al responsable solicitando la cancelación de datos. Este conocimiento resultará de la información acerca de la conservación de datos que la propia publicidad de la LCD comporta, compatible con las previsiones del art. 5.5 LOPD —aplicadas a la cesión—. Dado que debe entenderse que, a pesar de la denominación del art. 9, la LCD no establece ninguna excepción a los derechos de acceso y rectificación, debe interpretarse que éste resulta plenamente operativo en relación con los datos conservados, lo cual ha de considerarse adecuado. La utilidad de dicho acceso, sin embargo, queda sumamente mermada, debido a la previsión del art. 9.2 LCD, que imposibilita la cancelación en todo caso, con lo que se excluye también la eventual cancelación de datos inexactos, incompletos o cuyo tratamiento no se ajuste a lo dispuesto en la LOPD, supuestos a los

---

[884] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit. p. 26.

[885] Cf. Rodríguez Lainz, J. L., "El principio de proporcionalidad... (I)", op. cit., p. 9; y González López, J. J., en Comentarios a la Ley 25/2007…, op. cit. p. 26.

que la Ley, en su artículo 16.2 vincula la posibilidad de rectificación o cancelación, previsión que resulta ilógica al abortar el efecto "sanador" del tratamiento de datos.

36 Incumplimiento de las obligaciones contempladas en la Ley

El legislador español, a la hora de regular los eventuales incumplimientos de los deberes contemplados en la LCD por parte de los operadores obligados, ha optado por integrar su regulación en el régimen sancionador general de la LGT. Así, el art. 10 LCD[886] —que constituye el único artículo del Capítulo III de la Ley—, establece que el incumplimiento de las obligaciones previstas en la LCD se sancionará "de acuerdo con lo dispuesto en la Ley 32/2003, de 3 de noviembre, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados".

Dejando ahora aparte la referencia a la responsabilidad penal, el régimen sancionador de la norma se remite principalmente al Título VIII de la LGT, que comprende los arts. 50 a 58 bajo la rúbrica de "Inspección y régimen sancionador"[887] y que articula un típico modelo de régimen administrativo sancionador, sobre los principios de la potestad sancionadora de la Administración Pública tal como se recogen en el Título IX de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones

---

[886] El tenor del precepto reza así: "Artículo 10. Régimen aplicable al Incumplimiento de obligaciones contempladas en esta Ley. El incumplimiento de las obligaciones previstas en esta Ley se sancionará de acuerdo con lo dispuesto en la Ley 32/2003, de 3 de noviembre, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados".

[887] La literalidad del artículo 10 del Anteproyecto limitaba la extensión del régimen sancionador al incumplimiento de las obligaciones específicas de "conservación, protección y seguridad". Por sugerencia del Consejo de Estado, la existencia de otras obligaciones que podrían exceder de lo que es estrictamente conservación, protección y seguridad —por ejemplo, sobre cancelación, bloqueo o supresión—, hizo que al final se optase por la utilización de una fórmula más amplia, sencillamente referida a las obligaciones "previstas en esta Ley". Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.C.1.

Públicas y del Procedimiento Administrativo Común[888]. Puesto que desbordaría el objeto de nuestro estudio exponer ahora con detalle el sistema de sanciones vigente en el Derecho de las telecomunicaciones, nos limitaremos a señalar que el Título VIII de la LGT establece las competencias orgánicas en materia de inspección y sanción[889], la responsabilidad de los distintos sujetos[890], la prescripción de las infracciones[891] y los tres tipos de infracciones existentes —muy graves, graves y leves[892]—. El catálogo de las mismas se desarrolla en los arts. 52, 53 y 54 LGT, respectivamente.

Como no podía ser de otra manera, la LCD ha procedido, mediante los apartados cuarto y quinto de su Disposición Final Primera, a actualizar la relación de faltas graves y muy graves de los arts. 54 y 53 LGT, incluyendo nuevas infracciones relativas a los deberes que aquella establece. En concreto, es considerada ahora falta muy grave el incumplimiento deliberado, por parte de los operadores, "de las obligaciones de conservación de los datos establecidas" en la LCD[893] así como "el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8" de la LCD[894]. Los apartados ñ) y r) del art. 54 LGT tipifican respectivamente como graves las mismas conductas, "salvo que deban considerarse como infracción muy grave" [895], lo que se producirá cuando el incumplimiento no sea deliberado.

Las sanciones previstas por el art. 56 LGT son todas de multa, sin perjuicio de que los órganos competentes estén facultados adicionalmente para la adopción de medidas cautelares o sanciones accesorias, tales como la retirada del mercado de los equipos o instalaciones que hubiera empleado el infractor, el precintado o la incautación de los equipos o aparatos, la clausura de las instalaciones, o la suspensión provisional de la eficacia del título habilitante para la ocupación del dominio público.

---

[888] Publicada en BOE, núm. 285, de 27 de noviembre de 1992, pp. 40300 a 40319.

[889] Cf. arts. 50 y 58 LGT.

[890] Cf. art. 51 LGT.

[891] Cf. art. 57 LGT.

[892] Cf. art. 52 LGT.

[893] Cf. art. 53.o) LGT.

[894] Cf. art. 53.z) LGT.

[895] Cf. art.54.ñ) y r) LGT, *in fine.*

Aplicado a nuestra materia, la comisión de una falta muy grave con relación a las obligaciones de la LCD —esto es, por incumplir bien las obligaciones de conservación de los datos, bien las de protección y seguridad de los mismos[896], son castigadas con multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción. En caso de que no resulte posible aplicar este criterio, el límite máximo de la sanción será de dos millones de euros. Las infracciones muy graves, en función de sus circunstancias, pueden dar lugar a la inhabilitación hasta de cinco años del operador para la explotación de redes o la prestación de servicios de comunicaciones electrónicas[897].

Cuando las mismas conductas infractoras merezcan la calificación de graves —por no ser "deliberadas"— se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio, el límite máximo de la sanción será de quinientos mil euros. Además, las infracciones graves, en función de sus circunstancias, pueden llevar aparejada amonestación pública, con publicación en el Boletín Oficial del Estado y en dos periódicos de difusión nacional, una vez que la resolución sancionadora tenga carácter firme[898].

La cuantía y gravedad de la sanción se gradúan teniendo en cuenta los criterios clásicos del derecho administrativo-sancionador español[899].

---

[896] Cf. art. 53.o) y z) LGT.

[897] Cf. art. 56.b) LGT.

[898] cf. art. 56.c) LGT.

[899] Así, dispone el art. 56.2 LGT que "la cuantía de la sanción que se imponga, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, lo siguiente:

a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

c) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

d) El daño causado.

Además de la sanción que corresponda imponer, como personas jurídicas, a las compañías de telecomunicaciones infractoras, se puede imponer además una multa de hasta sesenta mil euros a sus representantes legales o a las personas que integran los órganos directivos que hayan intervenido en el acuerdo o decisión, excepto aquellas personas que, formando parte de órganos colegiados de administración, no hubieran asistido a las reuniones o hubieran votado en contra o salvando su voto[900].

37 Modificaciones y derogaciones por la LCD

Para concluir nuestro análisis sistemático de la LCD, expondremos finalmente lo previsto en su extensa Disposición Final Primera, en virtud de la cual se introdujeron diversas modificaciones en los artículos 33, 38, 53 y 54 LGT y se derogaron varios preceptos.

Así, el antiguo art. 33 LGT ha visto añadírsele hasta nueve apartados más. Mientras el primero conserva su redacción original y establece el deber general de los operadores de garantizar el secreto de las comunicaciones de conformidad con los arts. 18.3 y 55.2 CE —para lo cual han de adoptar las medidas técnicas necesarias—, el resto de los apartados se ocupan de regular las obligaciones de las compañías en relación con la interceptación legal de las comunicaciones. Dicha disciplina estaba regulada inconvenientemente en una norma de rango reglamentario: el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el *Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, sobre el deber de colaboración de operadores concernidos en materia de interceptación legal de comunicaciones, la consolidación de la*

Además, para la fijación de la sanción se tendrá en cuenta la situación económica del infractor, derivada de su patrimonio, de sus ingresos, de sus cargas familiares y de las demás circunstancias personales que acredite que le afectan.

El infractor vendrá obligado, en su caso, al pago de las tasas que hubiera debido satisfacer en el supuesto de haber realizado la notificación a que se refiere el artículo 6 o de haber disfrutado de título para la utilización del dominio público radioeléctrico".

[900] Cf. art. 56.4 LGT.

normativa específica sobre registro de adquisición de tarjetas telefónicas de prepago[901]. Constatada la carencia legislativa, dos años después de su aprobación, el legislador, a través de la LCD, ha incorporado a la LGT los aspectos del Reglamento que ha estimado convenientes. Dicha operación es sin duda de máximo interés para la regulación de la interceptación de las comunicaciones en nuestro ordenamiento, pero al no afectar directamente al objeto de nuestro estudio, hemos de dejarla al margen de nuestro estudio[902].

Por su parte, el artículo 38.5 LGT encontró a través del apartado dos de la Disposición Final Primera una nueva redacción, conforme a la cual lo establecido en el art. 38.3, letras a) y d), se entiende "sin perjuicio de las obligaciones establecidas" en la LCD. Como ya vimos al principio, el art. 38.3.a) LGT reconoce el derecho de los abonados a los servicios de comunicaciones electrónicas a que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Asimismo, la letra d) reconoce el derecho de los abonados a que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación. Como la LCD supone una clara e incisiva excepción a lo dispuesto en estos dos preceptos, el legislador creyó conveniente consagrar tal excepción a través de una mención expresa a la misma, de tal modo que el art. 38 LGT presenta ahora la redacción expuesta. Debe notarse, además,

---

[901] Publicado en BOE núm. 102 de 29 de abril de 2005, pp. 14545 a 14588.

[902] No obstante, no podemos por menos que remitirnos a los excelentes trabajos sobre el particular elaborados por Mendoza Losana, A. I., "El nuevo Reglamento del servicio universal de telecomunicaciones: análisis de las novedades introducidas por RD 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios", en Estudios sobre telecomunicaciones y derecho de consumo (coord. por Angel Carrasco Perera), Aranzadi, 2005, págs. 265-306; y Zoco Zabala, C., "Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de SITEL con el artículo 18.3 CE", en Indret: Revista para el Análisis del Derecho, , Nº. 4, 2010, p. 17, disponible en http://www.indret.com/pdf/781_es.pdf.

que el nuevo párrafo vino a sustituir al que desempeñaba una labor similar respecto del fracasado art. 12 LSSI[903].

Por su parte, como ya hemos visto, los apartados tres y cuatro de la Disposición Final Primera de la LCD han procedido a actualizar el régimen sancionador establecido por la LGT para los operadores que incumplan los deberes contenidos en la normativa general de telecomunicaciones. Obviamente, la Disposición ha añadido al catálogo de infracciones las relativas a los deberes introducidos por la LCD. Así, el art. 53 LGT, que contempla los supuestos de infracciones muy graves, ha visto modificado sus apartados o) y z), que ahora consideran sancionable, en primer lugar, el incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del art. 33 LGT —que acabamos de tratar— y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la LCD[904]. En segundo lugar, se considera infracción muy grave la vulneración grave o reiterada de los derechos previstos en el art. 38.3 LGT —esto es, los derechos de los consumidores y usuarios finales—, salvo el previsto por el párrafo h)[905], cuya infracción se regirá por el régimen sancionador previsto en la LSSI, y "el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas" en el art. 8 LCD[906].

También se modificaron, esta vez por acción del apartado quinto de la Disposición Final Primera, los apartados ñ) y r) del art. 54 LGT, que describe la panoplia de infracciones graves previstas. El apartado ñ) pretende ser la infracción equivalente a la del apartado o) del art. 53 LGT, para los casos en que el incumplimiento no sea "deliberado". Por su parte, el apartado r) castiga la vulneración de los derechos

---

[903] El texto anterior afirmaba que "lo dispuesto en el párrafo a) del apartado 3 se entiende sin perjuicio de lo dispuesto 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". Nótese que no se hacía mención al derecho contenido en la letra d).

[904] Cf. art. 54.o) LGT.

[905] El art. 38.3.h) LGT establece el derecho de los abonados a "resolver anticipadamente y sin penalización el contrato, en los supuestos de propuestas de modificación de las condiciones contractuales por motivos válidos especificados en aquél y sin perjuicio de otras causas de resolución unilateral".

[906] Cf. art. 54.z) LGT.

previstos en el art. 38.3 LCD —derechos de los consumidores y usuarios finales— y el incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el art. 8 LCD, "salvo que deban considerarse como infracción muy grave".

Mencionaremos para finalizar la Disposición Transitoria Única —"vigencia del régimen de interceptación de telecomunicaciones"—, la cual establece que las normas dictadas en desarrollo del Capítulo III del Título III de la LGT, "continuarán en vigor en tanto no se opongan a lo dispuesto en esta Ley". El texto del Anteproyecto concluía con la coletilla "o sean modificadas", que fue eliminada porque la modificación no determina la pérdida de vigencia de la norma modificada, sino en los puntos concretos en que se produzca la modificación, efecto que no requiere su previsión expresa[907]. La citada disposición, como observó el Consejo de Estado, más parece una extraña disposición derogatoria —pues está redactada en sentido negativo— que una disposición transitoria, ya que no trata de perfilar el régimen aplicable a situaciones existentes en la entrada en vigor de la ley o de flexibilizar ésta, "sino de determinar la medida de la vigencia de determinadas normas preexistentes"[908]. A fin de cuentas, declarar su vigencia en tanto no se opongan a lo dispuesto en la Ley es tanto como derogarlas en cuanto se opongan a lo dispuesto en la misma, lo que no es, en definitiva, sino una especificación de lo que, con carácter general establece el apartado segudno de la Disposición Derogatoria Única. No estamos, desde luego, ante el más brillante alarde de depurada nomotecnia.

38 Costes

Entre las cosas que debemos mencionar antes de culminar el análisis objetivo de la LCD, se cuenta el que podríamos denominar *problema de los costes*. Una importante crítica formulada tanto respecto de la presente Ley como de su Directiva se refiere al gran coste que ésta supone para los operadores de comunicaciones electrónicas, que

[907] Cf. Dictamen 32/2007, de 22 de febrero, del Consejo de Estado, apart. III.D.2.

[908] Ibíd.

han de realizar las adaptaciones precisas para cumplir con sus obligaciones de conservación y cesión de datos y mantener tal sistema a sus expensas.

La obligación de captar y almacenar los datos de tráfico parece a primera vista bastante fácil de cumplir, ya que tan sólo requiere que el programa informático que elabora los datos de tráfico de la comunicación —origen, destino, fechas, etc.— almacene los datos mediante un registro. Sin embargo, este almacenamiento ha supuesto una modificación de los programas gestores de los datos, en la medida en que deben realizar una función que antes no desempeñaban, lo que ha originado, correlativamente, una necesidad de nuevos y amplios espacios de almacenamiento. Si bien los sistemas de almacenamiento han mejorado mucho en los últimos años, el ingente número de comunicaciones electrónicas y su largo período de conservación —que, no olvidemos, podría alcanzar los dos años[909]— supone un número tal de datos que han requerido una inmensa capacidad de almacenamiento electrónico.

Pese a la carga económica que supone la nueva normativa de conservación, lo cierto es que ni la Directiva 2006/24/CE ni la LCD han optado por prever ningún tipo de compensación económica a favor de los proveedores de servicios de comunicaciones electrónicas.

De hecho, en el caso español, el problema de los costes y la repercusión de esta reforma en el mercado de las telecomunicaciones apenas fue considerada por nuestro legislador. Como ya pusimos de manifiesto, el Consejo de Estado se quejó en el punto I de su Dictamen de la ausencia de información relativa a los efectos económicos que las medidas previstas tendrían sobre los sujetos obligados y que, previsiblemente, serían repercutidos sobre los usuarios. Así, en la memoria económica se incluyó un tercer epígrafe sobre "incidencia económica sobre el sector", pero su contenido se redujo prácticamente a distinguir entre los costes de adaptaciones técnicas y los de actividades administrativas —sin cuantificar unos ni otros— y a concluir que se "tendrá en consideración la necesaria proporción entre los objetivos a conseguir y los costes en que se incurra". En varios de los escritos de alegaciones u observaciones se plantearon alternativas en relación con la configuración legal de algunas de las medidas previstas

[909] Cf. art. 6 DCD.

—sobre plazos de conservación y de entrega, medidas sobre tarjetas prepago, sobre "llamadas infructuosas", etc.—, aludiendo a los elevados costes que suponían algunas exigencias previstas en la norma, y no impuestas por la norma comunitaria —o a las diferencias de coste, en función de la concreta configuración legal, de algunas de las medidas previstas, en las que cuantiosas inversiones tendrían una escasa utilidad marginal—. Desgraciadamente, el Gobierno español no prestó la suficiente atención a todas estas alegaciones y propuestas o, de hacerlo, no lo reflejó en el expediente que más tarde estudiaron las Cortes.

Son muchas las voces que, desde España como desde otros países de la Unión, se han manifestado a favor de que sean los poderes públicos los que asuman los costes que la normativa de conservación de datos comporta para los operadores. Así, por ejemplo, señala al respecto RODRÍGUEZ DELGADO que "este doble 'sobreesfuerzo' que los operadores deben realizar es fruto directo de la Ley y por lo tanto debería ser ésta la que estableciese mecanismos que aminorasen los costes económicos que el cumplimiento de las obligaciones generará en los sujetos obligados"[910].

En todo caso, a la vista de las actuales vicisitudes económicas por las que atraviesa tanto nuestro país como otros tantos Estados miembros de la Unión, parece claro que la posibilidad de establecer una compensación económica en favor de los operadores a cargo de los presupuestos nacionales ha quedado completamente postergada frente a la necesidad urgente y prioritaria de reducir el gasto público.

[910] Cf. Rodríguez Delgado, J. P., La ley 25/2007…, op. cit., p. 5.

CUARTA PARTE. CONSTITUCIONALIDAD DE LA LEY 25/2007, DE 18 DE OCTUBRE

39 Introducción: el impacto de la LCD en los derechos fundamentales de la Constitución Española

En la Cuarta Parte de esta Tesis examinaremos la LCD desde una perspectiva estrictamente constitucional, intentando en particular dar respuesta a la cuestión acerca de si las disposiciones de la norma son compatibles con el sistema de derechos fundamentales vigente en nuestro ordenamiento. Para ello, delimitaremos primero los concretos derechos fundamentales limitados por la Ley en presencia, para pasar luego a aplicar el test de constitucionalidad sobre las medidas de conservación de datos tal como han sido incorporadas a nuestro Derecho internto por el legislador español.

Fijado en tales términos el objetivo de las siguientes páginas, hemos de empezar nuestro análisis formulando una sencilla observación. A primera vista y sin prejuzgar su constitucionalidad, resulta patente que las medidas previstas en la LCD suponen una una notable afectación de derechos fundamentales, principalmente los reconocidos por el art. 18 CE[911]. Para el común de los ciudadanos, la mera perspectiva de que todos los datos externos de nuestras comunicaciones por teléfono e internet hayan de ser conservados durante un plazo de doce meses se antoja por sí misma notablemente invasiva de la esfera íntima que rodea a cada sujeto. En este sentido, tan preocupante

[911] Dispone el art. 18 CE que: "1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

constatación justifica sobradamente que las disposiciones centrales de la LCD sean sometidas a un riguroso control de constitucionalidad si su permanencia en nuestro Derecho es pretendida finalmente por el legislador.

Concretamente, para que la norma en presencia pueda adquirir carta de naturaleza en el ordenamiento español, debe quedar acreditado que sus medidas, aun comportando una injerencia en los derechos fundamentales afectados —*nominatim*, los del art. 18 CE, en los términos que veremos— respetan de todo punto los parámetros de legitimidad constitucional establecidos por nuestro texto fundamental y la jurisprudencia del TC. Conforme a estos, tanto la conservación generalizada de datos como las demás medidas de la LCD habrán de respetar las exigencias clásicas de cualquier restricción de derechos fundamentales, a saber: previsión legal, reserva de decisión judicial motivada y estricta observancia del principio de proporcionalidad. Este último principio se concreta en tres requisitos o condiciones: idoneidad de la medida para alcanzar el fin constitucionalmente legítimo perseguido —lo que se denomina *juicio de idoneidad*—; que la misma resulte imprescindible o necesaria para ello, esto es, que no existan otras medidas menos gravosas que, sin imponer sacrificio alguno de derechos fundamentales o con un sacrificio menor, sean igualmente aptas para dicho fin —*juicio de necesidad*—*;* y, por último, que se deriven de su aplicación más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o intereses en conflicto, o dicho de otro modo, que el sacrificio impuesto al derecho fundamental no resulte desmedido en relación con la gravedad de los hechos y las sospechas existentes —*juicio de proporcionalidad en sentido estricto*—[912].

Para llevar a cabo con éxito este examen, nos ocuparemos primeramente, a lo largo de las siguientes páginas, de clarificar la naturaleza de las obligaciones que derivan de la LCD desde una perspectiva jurídico-constitucional, para seguidamente examinar el modo en que sus medidas afectan a concretos derechos fundamentales y terminar sometiendo las mismas al test de constitucionalidad cuyas condiciones generales acabamos de apuntar.

---

[912] Cf. al respecto las SSTC 234/1997, de 18 de diciembre, 70/2002, de 3 de abril, 25/2005, de 14 de febrero y 206/2007, de 24 de septiembre, entre otras muchas.

40 Limitaciones de los derechos establecidas por la LCD

Desde un punto de la vista *procesal-penal*, la descripción de las limitaciones a los derechos establecidas por la LCD no presenta grandes dificultades. Nos hallamos ante una medida de investigación penal novedosa —con apenas una década de historia en nuestro entorno legal— que persigue una finalidad esencialmente probatoria, la de establecer la existencia del delito y el descubrimiento de las personas responsables del mismo. Teniendo como objeto la obtención de aquellos elementos que resulten necesarios para sustentar un procesamiento o imputación y la posterior condena, la finalidad principal de las acciones que se adopten al amparo de la LCD es hacerlas valer en el juicio oral. Todo ello sin olvidar que la conservación de datos también puede resultar un importante medio de investigación y un instrumento útil para obtener otros medios de prueba o decidir sobre los sucesivos actos de investigación. En este sentido, la literatura doctrinal española ha producido algunos estudios sobre nuestra norma, si bien se limita al examen de la LCD desde una perspectiva estrictamente procesal[913].

---

[913] Entre ellos, cabe destacar los siguientes: González López, J. J., Comentarios a la ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, en Revista General de Derecho Procesal, 16, 2008, Iustel, pp. 1-38; Consideraciones acerca de las dificultades conceptual e iusfundamental planteadas por los datos de las comunicaciones electrónicas en la investigación penal, en Inclusión digital: perspectivas y experiencias (coord. por Nicolás Cabezudo Rodríguez), 2011, pp. 151-80; Guerrero Picó, M. C., Protección de datos personales e Internet: la conservación indiscriminada de los datos de tráfico, en Revista de la Facultad de Derecho de la Universidad de Granada, n. 8, 2005, pp. 109-39; López-Barajas Perea, I., El deber de conservación de datos en la Unión Europea y sus límites, en Revista de Derecho de la Unión Europea, n. 16, 2009, pp. 195-220; Ormazábal Sánchez, G., Los deberes de conservación de datos por parte de los operadores de telecomunicaciones y su aportación al proceso mediante requerimiento judicial (Reflexiones a la luz de la legislación española y de la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea), en Diario La Ley, n. 7055, Sección Doctrina, 13 Nov. 2008, Año XXIX, Ref. D-322; Ortiz Pradillo, J. C., Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas, en La Ley Penal: revista de derecho penal, procesal y penitenciario, n. 75, Sección Jurisprudencia aplicada a la práctica, octubre 2010; Pérez Gil, J., y González López, J. J., Cesión de datos personales para la investigación penal: una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal, en Diario La Ley, n. 7401,

Desde la perspectiva netamente *constitucional*, sin embargo, el análisis de las limitaciones de los derechos impuestas por la LCD resulta mucho más complicado. Con toda probabilidad, la cuestión más difícil de dilucidar radica en la delimitación de los concretos derechos fundamentales afectados por dicha regulación. Esta dificultad procede tanto de la complejidad tecnológica como de la novedad de las medidas de conservación de datos, presentando ambas circunstancias importantes consecuencias. La primera de ellas es que la complejidad tecnológica de la conservación de datos no puede en absoluto obviarse, dado que no está ayuna de resultados jurídico-constitucionales relevantes, como ha quedado claro en otros puntos de la tesis. La segunda —estrechamente unida a la anterior— consiste en que la doctrina y la jurisprudencia ya asentadas en torno a otras medidas de investigación parecidas —como la interceptación del contenido o de los datos externos de las comunicaciones electrónicas— no pueden aplicarse analógica y acríticamente al objeto de nuestro estudio, so pena de llegar a conclusiones inexactas. En conclusión, al abordar la presente materia se impone a todas luces un examen pormenorizado y metódico de las medidas centrales de la LCD para poder dar cuenta exacta de cuál es la extensión de su injerencia en los derechos fundamentales. En este sentido, en las páginas que siguen avanzaremos siempre que sea posible por los caminos ya abiertos por otros institutos jurídicos, pero no dudaremos en desbrozar otros nuevos allí donde no existan y sea necesario para llegar a una conclusión.

Así pues, lo primero que hemos de afirmar es que la norma en presencia supone la creación de una nueva obligación para los operadores que prestan servicios de comunicaciones electrónicas de captar y conservar por el plazo de doce meses una amplia y detallada cantidad de datos generados por cada uno de sus usuarios en el marco de los servicios de comunicaciones electrónicas, de manera que estén

---

2010; Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones electrónicas a la luz de la directiva europea 2006/24/CE, en Revista de Contratación Electrónica, n. 92, abril 2008; Rodríguez Lainz, J. L., El principio de proporcionalidad en la nueva ley de conservación de datos relativos a las comunicaciones (I), Diario La Ley, n. 6859, viernes, 11 de enero, 2008; El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones (y II), en Diario La Ley, n. 6860, lunes, 14 de enero 2008.

disponibles para su cesión a las autoridades policiales —previa autorización judicial— para la averiguación y represión de delitos graves[914].

Formulada en estos términos la definición precedente, el primer riesgo de confusión radica en que la regulación en presencia no es una "interceptación de las comunicaciones" al uso, tal como podría parecer *prima facie*. Nos encontramos, en cambio, ante una medida que se diferencia de la clásica interceptación en aspectos importantes, que han de ser subrayados y ponderados con detenimiento. Aunque el resultado final sea el mismo —la obtención de los datos externos de las comunicaciones con fines procesales— y ambas medidas compartan la exigencia de autorización judicial, la LCD presenta una serie de rasgos que la hacen nítidamente diferente de la tradicional medida de interceptación de las comunicaciones[915]. El principal elemento que distingue a la LCD es que impone la obligación para los operadores de guardar todos y cada uno de los datos relevantes de las comunicaciones electrónicas de sus abonados durante un período de doce meses. De este modo, la gravedad de la injerencia en los derechos fundamentales que lleva a cabo la LCD no radica en la cesión de ciertos datos de las comunicaciones electrónicas a los agentes facultados para la investigación y enjuiciamiento de delitos —pues tal cesión se lleva siempre a cabo previa resolución judicial y de acuerdo con los principios de necesidad y proporcionalidad, tal como determina taxativamente el art. 7.2 LCD—, sino en esta obligación principal, cuyos rasgos separan la LCD de las demás medidas de interceptación hasta ahora conocidas. Sin perjuicio de que volvamos a examinar con detalle esta obligación de conservación generalizada de datos al analizar la proporcionalidad de la medida, su constatación nos permite formular ahora otras distinciones sumamente relevantes para nuestro análisis.

---

[914] Cf. art. 1 DCD.

[915] En torno a los rasgos y régimen de la interceptación de las comunicaciones en nuestro Derecho, cf. las siguientes monografías de referencia: Montero Aroca, J., La intervención de las comunicaciones telefónicas en el proceso penal (un estudio jurisprudencial), Tirant lo Blanch, Valencia, 1999; Rodríguez Lainz, J. L., La intervención de las comunicaciones telefónicas: su evolución en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo, Editorial Bosch, Barcelona, 2002; Manzano Sousa, M., La interceptación legal de las telecomunicaciones en la Unión Europea, Secretaría General Técnica, Ministerio del Interior, D.L., Madrid, 1996; López-Fragoso Alvarez, T. V., Las intervenciones telefónicas en el proceso penal, Constitución y Leyes, Madrid, 1991.

En primer lugar, ha de subrayarse que no estamos ante una medida *puramente procesal* sino, sobre todo, ante una norma *administrativa* que obliga a sujetos particulares —los operadores de servicios de comunicaciones electrónicas— a interceptar un ingente número de datos generados por los servicios que prestan a sus clientes[916]. El fuerte impacto de la LCD en la legislación administrativa sobre telecomunicaciones será ponderado en apartados posteriores.

En segundo lugar, no estamos ante un *acto de investigación en el marco de un procedimiento penal*. No se ha cometido ni se está investigando ningún delito en el momento en que tiene lugar la medida limitadora del derecho: la retención y archivo masivos de datos electrónicos. Los datos se interceptan pero, al contrario que en una intervención de las comunicaciones al uso, no se ponen en manos ni del Juez ni de la Policía Judicial; simplemente pasan a formar parte de un fichero de datos que el obligado debe mantener a su costa, y de acuerdo con unos mínimos de seguridad, durante el plazo de doce meses.

En tercer lugar, ninguna de estas acciones de interceptación y conservación se realiza *por orden o bajo control judicial*; es la LCD la que prescribe directa y genéricamente las acciones que debe llevar a cabo el obligado.

En cuarto lugar, la medida no afecta a un concreto individuo en un concreto proceso, sino a cualquier persona que tome parte de una comunicación telefónica o por internet, lo que en la práctica comprende a la *generalidad de la ciudadanía* en un aspecto esencial de la vida cotidiana. Este rasgo —como se aprecia fácilmente— resulta relevante a la hora de valorar la proporcionalidad de tal regulación.

---

[916] Sobre el carácter procesal o administrativo de la LCD, señala GONZÁLEZ LÓPEZ que "dado que la conservación generalizada, por tratarse de una medida predelictual y desvinculada de la existencia de sospechas o indicios no puede ser en ningún caso procesal, su encaje normativo en lugar de ubicarse en la ley procesal se ha desplazado en otro tipo de norma, en este caso administrativa. Una de las consecuencias de este fenómeno es que la regulación de la medida que constituye el objeto principal de la LCD (como dice su Exposición de Motivos) arrastra la de una medida propiamente procesal como es la cesión, que, de este modo, es regulada en una ley de corte administrativo, con una perspectiva necesariamente parcial" . Cf. González López, J. J., Comentarios a la Ley 25/2007…, op. cit. p. 28.

Todos los aspectos que acabamos de enumerar separan claramente la clásica intervención del contenido o de los datos externos de las comunicaciones —regulados principalmente en la LECrim— de la medida que constituye el núcleo de la LCD. La consideración de estas diferencias nos sitúa en una más clara perspectiva para valorar la normativa.

Otro rasgo fundamental de la LCD es el hecho de que no sea el poder público quien directamente se ocupe de interceptar todos los datos de tráfico y conservarlos en inmensas bases de datos. La injerencia en el derecho o derechos fundamentales se realiza *ex lege* por los particulares obligados. Todos los aspectos externos de cada una de las comunicaciones telefónicas o de internet que hayamos mantenido durante los últimos doce meses —quién, desde dónde, a quién, cuándo, etc.— quedan en manos de compañías de telecomunicaciones privadas, que deben almacenarlos a su costa y bajo su responsabilidad. Es cierto que los datos no estarán disponibles para el uso de los operadores, y que su custodia deberá rodearse de estrictas medidas de seguridad pero, en cualquier caso, la creación y mantenimiento por mandato legal de tan ingente masa de información personal supone, a todas luces, el surgimiento de una esfera de especial vulnerabilidad —artificialmente creada por expresa voluntad del legislador— y una potencial amenaza para la privacidad de cada ciudadano, así como una formidable injerencia en el espacio de libertades del que el Estado de derecho se supone protector, no agresor, por más que la conservación de los datos se haga y mantenga a través de particulares sometidos a un régimen de responsabilidad y a estrictas garantías de seguridad.

Así las cosas, aunque la autorización judicial y la consiguiente ponderación de acuerdo con criterios de necesidad y proporcionalidad resulten imprescindibles para la cesión y empleo en el concreto caso de los datos retenidos, las previsiones de la LCD siguen planteando la duda acerca de si tales criterios han sido correctamente ponderados por el propio legislador a la hora de determinar los contornos de la medida de conservación, y si las medidas adoptadas cumplen tales requisitos de constitucionalidad.

Para poder resolver satisfactoriamente esta cuestión, debemos previamente proceder a la exacta delimitación de los derechos fundamentales afectados por la Ley.

41 Derechos fundamentales afectados por la LCD

41.1 Consideraciones generales

La concreción de los derechos fundamentales que se ven afectados por la LCD resulta compleja y ciertamente polémica, particularmente en lo que se refiere a su medida central, el mandato legal por el cual se establece la conservación masiva por parte de los operadores de los datos externos de las comunicaciones electrónicas.

Mientras que una posición[917] mantiene que la obligación legal supone exclusivamente una injerencia en el derecho fundamental a la protección de datos de carácter personal, otra posición[918] considera que estamos ante una afectación tanto de éste como del derecho fundamental al secreto de las comunicaciones. Veamos esto con más detalle.

De acuerdo con la primera tesis, la acción por la que el operador debe captar la lista de datos del art. 5 LCD y conservarlos en una base de datos donde han de permanecer a disposición de las autoridades facultadas debe ser considerada como una interceptación de las comunicaciones sobre los datos externos. Esta interceptación presentaría sobre todo dos peculiaridades respecto de las tradicionales: se realiza por mandato legal, no judicial, y, en segundo término, los datos no se transmiten directamente a las autoridades públicas sino que pasan a formar parte de un fichero, a la espera de una eventual entrega a las mismas. Por tanto, la acción de captar todos estos datos afectaría al derecho al secreto de las comunicaciones y la de su prolongado archivo, al derecho a la protección de datos —abstracción hecha de los *datos de suscripción*, en los que es claro que únicamente éste último el que queda afectado—.

De acuerdo con la segunda tesis, no puede decirse que exista captación de los datos y, en consecuencia, no habría injerencia en el derecho al secreto de las comunicaciones. En la práctica, los operadores ya retienen esos datos para la prestación del servicio y su relación con los mismos es *per se* un tratamiento de los regulados en la LOPD. De este modo, sucedería con los datos de tráfico lo mismo que con los de suscripción;

---

[917] Parten de esta perspectiva los diversos estudios de RODRÍGUEZ LAINZ, listados en la bibliografía general de esta Tesis.

[918] Al respecto, véanse los artículos de GÓNZALEZ LÓPEZ, listados en la bibliografía general de esta Tesis.

simplemente, la LCD los haría indisponibles para el titular. En consecuencia, el único derecho que resulta afectado por las medidas de la LCD es el de la protección de datos personales, no el secreto.

En nuestro análisis adoptaremos la primera tesis, dado que tal perspectiva nos permitirá estudiar el problema con más intensidad, en la medida en que abordaremos el asunto desde la doble perspectiva tanto del secreto de las comunicaciones como de la protección de datos. Ciertamente, los datos electrónicos creados y gestionados en el marco de las telecomunicaciones están sujetos a la normativa de protección de datos. Así se desprende con claridad del art. 34 LGT[919]. Ahora bien, no puede perderse de vista que la normativa de protección de datos fue diseñada con anterioridad a la aparición de las comunicaciones electrónicas —sino para una variedad de realidades ajenas a éstas—, y en algunos puntos encaja mal en la misma, dado que los datos no se aportan por el usuario, ni se recogen del exterior —lo que es un presupuesto de hecho de la LOPD—, sino que se generan electrónicamente durante la prestación del servicio tecnológico cuya gestión queda en manos de los proveedores, dependiendo en buena parte de la configuración y desarrollo de la tecnología y no tanto de la voluntad de la compañía de recopilar éste o aquel dato. Como queda patente del tenor literal del art. 18.3 CE[920] y de la regulación de la LGT, los datos de las comunicaciones electrónicas *stricto sensu* están constitucionalmente protegidos por un régimen específico, distinto del de la LOPD aunque concurrente en muchos de sus aspectos. Así se desprende con

[919] Cf. art. 34. Protección de los datos de carácter personal (redacción según Real Decreto-ley 13/2012, de 30 de marzo): "1. Sin perjuicio de lo previsto en el apartado 6 del artículo 4 y en el segundo párrafo del artículo anterior, así como en la restante normativa específica aplicable, los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal conforme a la legislación vigente.

2. Los operadores a los que se refiere el apartado anterior deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos de carácter personal que sean exigidos por la Ley Orgánica 15/1999, de 13 de diciembre y su normativa de desarrollo y, en su caso, por la que se dicte en desarrollo de esta Ley en esta materia…".

[920] Dispone el precepto que "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

claridad del art. 33.1 LGT, que declara que los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deben garantizar el secreto de las comunicaciones de conformidad con los arts. 18.3 y 55.2 CE, debiendo adoptar las medidas técnicas necesarias. Ignorar esta dimensión sería ignorar la existencia del derecho al secreto de las comunicaciones y sus rasgos particulares, cayendo en el siempre tentador reduccionismo de examinar todo problema jurídico relacionado con la protección de la intimidad a través del derecho a la protección de datos. Por añadidura, sostener que estamos únicamente ante una injerencia en la protección de datos supondría ignorar el conjunto de garantías que, en virtud del art. 18.3 CE, rodean a las comunicaciones en nuestro régimen constitucional; garantías que se caracterizan por proteger con mayor vigor los datos relativos a las comunicaciones[921].

Finalmente, si la LCD incidiera en la protección de datos, deberíamos entonces plantearnos el porqué de la necesidad de autorización judicial para la cesión de los datos conservados ex art. 7 DCD, cuando tal garantía no es requerida con carácter general en la normativa de protección de datos personales para el acceso a los mismos[922]. Bastaría que la ley autorizara la cesión y la regulara con suficiente detalle para no dejar margen a la arbitrariedad, pues tal es el régimen general fijado por la LOPD[923].

---

[921] Cf. GÓMEZ SÁNCHEZ, Y., Derecho Constitucional Europeo: derechos y libertades, Sanz y Torres, Madrid, 2008, pp. 297-321.

[922] Cf. art. 11 LOPD.

[923] Dispone el art. 11 LOPD —Comunicación de datos— que "1. 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.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

En todo caso, el legislador español, al elaborar la norma, ha partido de la perspectiva de que la misma suponía una injerencia en el derecho al secreto de las comunicaciones. Así se desprende del hecho de que, en la Exposición de Motivos de la LCD, sostenga que "la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones ha venido emitiendo el Tribunal Constitucional"[924], al tiempo que, en el mismo lugar, manifiesta que el uso indebido de los datos conservados está "sometido a los mecanismos de control de la LOPD y su normativa de desarrollo"[925], bajo cuyo régimen sitúa las medidas de protección y seguridad de los datos en el art. 8 LCD[926] y otros aspectos de la normativa. Así pues, aunque no sea

---

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar".

[924] Cf. Exposición de Motivos de la LCD, apartado I, párrafo quinto.

[925] Cf. Exposición de Motivos de la LCD, apartado II, párrafo sexto.

[926] Dispone el art. 8 LCD que "1. los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

explicitado, del conjunto general de la regulación parece colegirse que, para el legislador español, la captación y cesión de los datos por parte de los operadores vendría a ser una restricción del derecho al secreto de las comunicaciones, en tanto que la conservación *per se* lo sería del derecho a la protección de datos de carácter personal.

Creemos que para abordar convenientemente tan compleja materia debemos ahora exponer el contenido de estos derechos en sus distintas dimensiones, tal como la doctrina del TC ha ido definiéndolos. No obstante, a fin de que esta explicación sirva mejor a los fines de esta Tesis y no sea una mera reposición de lo que es comúnmente sabido sobre estos derechos, desarrollaremos este análisis al hilo, en primer lugar, de la relación —desde la perspectiva de los derechos fundamentales— de los operadores con los datos que manejan para continuar —en segundo lugar y desde la misma perspectiva— con la relación de los operadores con los datos a conservar listados en el art. 3 LCD.

41.2 Relación de los operadores con los datos de las comunicaciones electrónicas de cuya transmisión se ocupan, desde la perspectiva de los derechos fundamentales

41.2.1 Introducción

Resulta evidente que, en la prestación de sus servicios, los operadores de telecomunicaciones producen y gestionan un sinfín de datos. De ellos, una buena parte son creados por la propia tecnología de la comunicación, tienen naturaleza electrónica —por ejemplo, los registros de llamadas, la duración de las mismas, las IPs, etc.— y su tratamiento por las compañías es necesario para la correcta prestación y mantenimiento del servicio. Otra porción de datos no procede directamente del medio tecnológico

---

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley".

empleado ni tiene naturaleza electrónica, sino que es recabada *ex professo* por los operadores para poder explotar su actividad económica convenientemente —el nombre del abonado, su domicilio, etc.—. Los primeros constituyen lo que podríamos denominar *datos externos de la comunicación electrónica* —incluyéndose en ellos los datos de localización—, mientras los segundos son *los datos de usuario o abonado*. Mientras el conjunto de aquellos es evidente que caen bajo la protección del derecho al secreto de las comunicaciones, estos lo hacen bajo el derecho a la protección de datos personales[927]. Para poder sostener debidamente esta afirmación, no cabe ahora sino exponer con la mayor concisión posible la doctrina sobre estos derechos fundamentales en nuestro sistema constitucional. Para mayor utilidad, abordaremos la exposición que sigue en el orden y con el enfoque que más interesa al objeto de aplicar sus conclusiones a nuestro estudio.

41.2.2 Los derechos al secreto de las comunicaciones y a la protección de datos de carácter personal en relación con los datos externos de las comunicaciones electrónicas

41.2.2.1 Secreto de las comunicaciones: objeto protegido

Casi resulta innecesario —aunque sin duda conveniente— empezar recordando que el secreto de las comunicaciones se reconoce como derecho fundamental en todas las constituciones contemporáneas, así como en las normas internacionales, como la Declaración Universal de Derechos Humanos[928] y el Pacto Internacional de Derechos

[927] En consecuencia —hecha abstracción de lo ahora dispuesto en la LCD— cuando una autoridad publica quiera recabar un dato de trafico, se debe acudir a la doctrina constitucional sobre la protección de estos datos para determinar las condiciones que hacen legitima su obtención; en tanto que la legislación de protección de datos será de aplicación cuando la información interesada se refiera a los datos relativos a los usuarios.

[928] Dispone el art. 12 de la Declaración que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias y ataques".

Civiles y Políticos[929]. En nuestro vigente texto constitucional se reconoce con rango de derecho fundamental en el art. 18.3 CE, según el cual "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial"[930]. El derecho —que, como recordaremos más adelante, posee un contenido más amplio y distinto del derecho a la intimidad— garantiza a los interlocutores o comunicantes una protección que se proyecta sobre el proceso de comunicación mismo con independencia de que el contenido del mensaje transmitido pertenezca o no al ámbito de lo personal, lo íntimo o lo reservado[931]. Así lo ha venido considerando nuestro TC desde la importantísima STC 114/1984, de 29 de noviembre, que explicitó por vez primera la extensión para los interlocutores o comunicantes de la protección constitucional de este derecho en los siguientes términos:

> "Rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último 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)" [932].

---

[929] Conforme a su art. 17: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y su reputación. 2. Toda persona tiene derecho a la protección de la Ley contra tales injerencias y ataques".

[930] Queda sujeto por tanto a la protección reforzada que establece el art. 53.3 CE, de manera que cualquier ciudadano puede recabar su tutela ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional.

[931] Cf. STC 114/1984, de 29 de noviembre.

[932] Otra cita importante, dentro de la misma resolución: "La protección constitucional del derecho, para los interlocutores o comunicantes 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". Esta cita vuelve a aparecer, entre otras, en las SSTC 34/1996, de 11 de marzo, 70/2002, de 3 de abril y 123/2002, de 20 de mayo.

Así pues, el objeto de este derecho no es otro que la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo comunicado, de tal forma que toda comunicación es para la norma fundamental secreta aunque sólo algunas sean íntimas[933]; dicho de otro modo: no se dispensa el secreto en función del contenido de la comunicación pues —como expresivamente ha afirmado JIMÉNEZ CAMPO[934]— el secreto es un atributo jurídico de la comunicación y no de su contenido[935].

De esta manera, a pesar de nuestra sistemática constitucional —que conecta el derecho al secreto de las comunicaciones con el derecho a la intimidad— es cuestión pacífica la autonomía y sustantividad propia del derecho al secreto de las comunicaciones, que tiene entre sus consecuencias directas el que sea posible violar el secreto de las comunicaciones sin incidir por ello en la esfera íntima de una persona[936].

Concretando aún más, hemos de aclarar que el objeto del derecho goza de un máximo nivel de protección en tanto que se extiende no sólo al contenido de la conversación o información transmitida, sino, igualmente, a los datos técnicos reservados, mediante cuyo conocimiento podría llegarse a conocer la existencia misma de la comunicación[937]. Estos datos son los que hemos denominado "datos de tráfico", o con mayor exactitud, "datos relativos (o externos) a las comunicaciones electrónicas", y permiten conocer algunos extremos relativos a la comunicación como el momento y la

---

[933] Cf. STC 123/2002, de 20 de mayo. De hecho, como es bien sabido, el desarrollo ideológico y jurídico de la inviolabilidad del domicilio y del secreto de las comunicaciones como derechos individuales es históricamente anterior a la aparición en el plano jurídico de la idea de la necesidad de proteger la vida privada o la intimidad personal como tales. Cf. Aroz Santisteban, Derecho al respeto de la vida privada y familiar, op. cit., p. 256.

[934] Cf. Jiménez Campo, J., La garantía constitucional del secreto de las comunicaciones, *Revista Española de Derecho Constitucional*, año 7, núm. 20, 1987.

[935] Como ha repetido el TC, el constituyente español no ha querido proteger exclusivamente el secreto de las comunicaciones que tengan un carácter "íntimo", sino cualquier clase de comunicación, con independencia de su contenido.

[936] Aplicando esto al objeto de nuestro estudio, se echa de ver que cualquier comunicación cerrada que se realice a través de los medios regulados por la LGT goza de la protección de este derecho.

[937] Cf. Rodríguez Lainz, J. L., Intervención judicial en 105 datos de tráfico de las comunicaciones, Bosch, Barcelona, 2003, p. 21; Hernández Guerrero, F., La intervención de las comunicaciones electrónicas, *Estudios jurídicos del Ministerio Fiscal*, n. 111, 2001, p. 349.

duración, así como otros de gran relevancia como la identidad de las personas que establecen el contacto. Todos ellos han de ser conservados por mandato expreso de la LCD.

Desde una perspectiva estrictamente constitucional, la doctrina ha definido estos datos de tráfico como "las informaciones que se generan o tratan en el curso de una comunicación y difieren de su contenido material entendiendo por tal aquella información cuya transmisión voluntaria por el emisor al receptor motiva la comunicación"[938].

Aunque el art. 64.a) RLGT —recogiendo el art. 2.b) DPCE— define los datos de tráfico como "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación", la LCD formula a su manera una definición cuando se refiere a aquellos datos que se hayan generado o tratado en el marco de una comunicación de telefonía fija, móvil o internet[939]. De esta manera incluye dentro de su ámbito de aplicación los datos necesarios para identificar el origen y destino de la comunicación, la identidad de los usuarios o abonados de ambos —nombre y dirección—, o los que permiten determinar el momento y duración, el tipo de servicio y el equipo de comunicación utilizado por los usuarios que, cuando se trate de un equipo móvil, también abarcará los datos necesarios para su localización[940]. No cabe duda de que de este modo la LCD no hace sino abrazar un concepto amplio del término, ya que no sólo incluye los elementos esenciales del dato de tráfico —terminales conectados, identificación de los usuarios y datación de la comunicación—, sino también a otros que podrían ser calificados como servicios de valor añadido —vg. la localización del usuario con GPS[941]—. De hecho, la

---

[938] Cf. Retención de datos de tráfico de las telecomunicaciones y proceso penal, en VV.AA., Estudios jurídicos sobre la Sociedad de la Información y nuevas tecnologías. Libro con motivo del XX Aniversario de la Facultad de Derecho, Servicio de Publicaciones de la Universidad de Burgos, Burgos, 2005, pp. 375-394.

[939] Cf. Exposición de Motivos de la LCD, apartado II.

[940] Cf. art. 3.1 LCD.

[941] El art. 2.g) de la Directiva 2002/58/CE define los servicios de valor añadido como todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vaya más allá de lo necesario para la transmisión de una comunicación o su facturación. Cf. art. 2.g).1 de la

tendencia legislativa hacia una interpretación amplia del concepto "dato de tráfico" resulta aún más clara en el Convenio número 185, del Consejo de Europa, sobre Ciberdelincuencia, de 23 de noviembre de 2001 —ratificado por el Estado español el 20 de mayo de 2010— que también define los datos de tráfico *lato sensu* en su art. 1.d), entendiendo por tales todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando origen, destino, itinerario, tiempo, fecha, tamaño y duración de la comunicación o tipo de servicio subyacente[942].

En definitiva, del análisis de todas estas definiciones se desprende la meridiana conclusión de que la amplia cantidad de información personal que los datos de tráfico pueden aportar ha hecho que los mismos se consideren o bien parte del objeto de protección del derecho al secreto de las comunicaciones, o bien parte incluso del contenido de la comunicación en algunos casos [943]. La constante evolución de las tecnologías de la comunicación hace que, en ocasiones, estas definiciones amplias de los datos de tráfico incluyan informaciones que por su naturaleza podrían tener distintos tratamientos según las circunstancias. Sirva de ejemplo al respecto lo señalado por GONZÁLEZ LÓPEZ acerca de cómo unos mismos datos pueden tener diverso tratamiento en el caso de los datos de localización de los servicios de valor añadido[944], que pueden tratarse accesoriamente a la comunicación —en cuyo caso constituyen datos de tráfico—, pero también son susceptibles de tratarse al margen de la comunicación e,

---

Directiva 2002/58/CE. También, cf. Loza Corera, M., y Rodríguez Casal, C., Nueva legislación europea en materia de protección de datos, Diario La Ley, núm. 5549, mayo 2002.

[942] Nótese cómo esta definición se apoya en una dependencia temporal y funcional de los datos de tráfico con respecto a la comunicación.

[943] Por ello, cuando, en un caso concreto, lo que la Policía hace no es identificar los números telefónicos en comunicación, sino, tan sólo, averiguar el correspondiente a uno de los comunicantes, no puede afirmarse con propiedad que se esté interviniendo en esa comunicación, dado que la comunicación, por definición, requiere, al menos, dos comunicantes y, por tanto, la actuación sobre un solo individuo y varios objetos de su pertenencia nunca puede constituir injerencia en sus comunicaciones ni, menos aún, en las de un tercero. Cf. STS 130/2007, de 19 de febrero (voto particular).

[944] Cf. González López, J. J., Utilización en el proceso penal de datos vinculados…, op., cit, p. 368. El art. 2.e) de la Directiva 2002/58/CE define los datos de localización como cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.

incluso, como parte del contenido material cuando ésta sea la información que el emisor desea transmitir al receptor (vg. una posición geográfica). Así, el régimen será distinto según se trate de datos de cobertura en el curso de una comunicación y durante el lapso temporal en el que ésta se está produciendo —pues al formar parte integrante de ella estarán amparados por el art. 18.3 CE—, o de datos de localización distintos a los de tráfico[945], supuesto éste en que su protección debe ampararse por otros derechos, como el del art. 18.4 CE[946].

Para analizar el enfoque de nuestra jurisprudencia constitucional a la doctrina conforme a la cual los datos externos de la comunicación quedan protegidos por el secreto del art. 18.3 CE, es obligado tomar como punto de partida la línea emprendida en la ya citada STC 114/1984, de 29 de noviembre[947], que recogía a su vez la jurisprudencia del TEDH en el célebre caso Malone contra Reino Unido, de 2 de agosto de 1984. En ella, el Tribunal de Estrasburgo reconoció expresamente la posibilidad de que el art. 8 CEDH resulte violado, no sólo por acceder al mensaje transmitido, sino por el empleo de un artificio técnico que permitía registrar cuáles habían sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma[948]. Sobre esta base, nuestro Tribunal Constitucional sostuvo desde entonces que el concepto de "secreto" que recoge el art. 18.3 CE no cubre sólo el contenido de la comunicación, sino también otros aspectos de la misma, como por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales, la propia existencia de la comunicación, así como la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino; y ello con independencia del carácter público o privado de la red de transmisión de la comunicación y del medio de transmisión —eléctrico, electromagnético u óptico, etc. [949]—.

---

[945] Según Loza Corera, M. y Rodrfguez Casal, E., los datos más precisos de lo necesario para la transmisión de la comunicación no son meros datos de tráfico. Cf. Loza Corera, M. y Rodríguez Casal, E., Nueva legislación europea en materia de protección de datos…, op. cit., p. 23.

[946] Cf. Pérez Gil, J., Los datos sobre localización geográfica en…, op. cit., pp. 346 y 347.

[947] Así lo recordaba a su vez el Tribunal Constitucional en su Sentencia 56/2003, de 24 de marzo.

[948] Ibíd.

[949] Cf. STC 114/1984, de 29 de noviembre. Dentro de su séptimo fundamento jurídico se definen los márgenes que conforman el derecho al secreto de las comunicaciones, que lo conforman como un

No obstante, la afirmación de que los números de teléfono marcados, la hora y la duración de la llamada forman parte de los datos externos al proceso de comunicación, y, por ello, requieren el mismo nivel de protección que el contenido de aquélla, siendo decisiva, sólo resuelve una pequeña parte de nuestra cuestión, ya que hoy en día las comunicaciones electrónicas —telefonía móvil, internet, etc.— generan toda una serie de datos de tráfico que van mucho más allá de aquéllos respecto de los que el TEDH tuvo ocasión de pronunciarse hace más de veinticinco años. Como hemos tenido ocasión de comprobar, el concepto de datos externos manejado por el TEDH en la sentencia del caso Malone se ha visto desbordado por la más amplia noción de "datos de tráfico", en cuyo ámbito se incluyen elementos de una naturaleza y funcionalidad muy heterogénea que no coinciden con la referida técnica del "recuento" considerada en aquella resolución. Baste considerar al respecto la actual telefonía móvil, cuya tecnología permite situar geográficamente un teléfono operativo aun cuando no se esté llevando a cabo una comunicación en ese momento. Además, los avances que se vienen produciendo en el ámbito de las comunicaciones electrónicas determinan que estemos ante un concepto que se halla en constante ampliación de la información integrable en la categoría de datos de tráfico[950].

Sea cuales fueren los concretos datos de tráfico que deben quedar excluidos de la protección del secreto de las comunicaciones, lo cierto es que una amplia mayoría de los que la LCD obliga captar y conservar caen sin duda dentro de su ámbito de protección, suponiendo su retención generalizada una clara afectación del derecho —

---

derecho autónomo que "consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas". El concepto de secreto del artículo 18.3 "no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales".

La Fiscalía General del Estado en su Consulta 1/1999, de 22 de enero, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones, recogió esta doctrina afirmando que no es posible disociar, sin merma relevante de garantías, realidades tan sustancialmente integradas como son el mensaje y su proceso de transmisión.

[950] Cf. González López, J. J., Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva, en *Protección de datos y proceso penal* (Coord. Pedraz Peñalva), La Ley, 2010, p. 365.

baste pernsar en números de teléfono marcados, la hora y la duración de la llamada—. No obstante, para comprender mejor el modo en que esta injerencia tiene lugar en términos jurídico-constitucionales, resulta imprescindible contemplar el derecho desde la perspectiva de los terceros, esto es, de aquellos que, sin ser emisor o receptor, ven mermadas sus facultades de actuación en virtud de la protección dispensada por el secreto de las comunicaciones.

41.2.2.2 Secreto de las comunicaciones: protección frente a las intromisiones de terceros.

El siguiente aspecto del derecho fundamental que consideramos extraordinariamente relevante para nuestros fines radica en el hecho de que lo que éste protege es el proceso de comunicación *frente a las intromisiones de terceros*[951]. A los efectos de la lesión del derecho al secreto de las comunicaciones, lo decisivo no es tanto el contenido de la información como el que un tercero, sin autorización de los sujetos de la comunicación, intervenga o revele su contenido[952]. Como ha afirmado el TC, el fundamento del carácter autónomo y separado de este derecho fundamental y de su específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación[953].

El desarrollo de esta doctrina en lo que a las telecomunicaciones se refiere encuentra su reflejo en el desarrollo legal de la materia, principalmente en el art. 33 LGT, que establece que los operadores que exploten redes públicas de comunicaciones o que presten servicios de comunicaciones electrónicas disponibles al público deben garantizar el secreto de las comunicaciones de conformidad con los arts. 18.3 y 55.2

---

[951] A través de la imposición a todos del secreto, el bien constitucionalmente protegido es la libertad de las comunicaciones. Cf. STC 123/2002, de 20 de mayo. Se persigue asegurar el derecho a transmitir libremente el propio pensamiento y hacerlo llegar sin interferencias a quien, también libremente, se elija como destinatario. Cf. STS de 19 de febrero de 2007.

[952] Cf. STC 114/1984, de 29 de noviembre.

[953] Cf. STC 123/2002, de 20 de mayo.

CE, debiendo adoptar las medidas técnicas necesarias con tal finalidad[954]. Volveremos sobre este punto con más detalle al tratar la relación de los operadores con los datos de las comunicaciones electrónicas listados en el art. 3 LCD.

La protección frente a terceros, que forma parte esencial del secreto de las comunicaciones, nos lleva de la mano a comentar otros aspectos del mismo que sirven tanto para dar cuenta exacta de su actual fisonomía como para reforzar y avanzar otros puntos importantes de la argumentación. En concreto, debemos detenernos a examinar las condiciones *ex Constitutione* de la injerencia en tal derecho fundamental y los criterios para graduar o modularla.

Dado los rasgos anteriormente apuntados, tanto la doctrina como la jurisprudencia han sostenido tradicionalmente que el secreto de las comunicaciones presenta un nítido carácter *formal*, que se contrapone al *material* del derecho a la intimidad[955]. Se ha venido así entendiendo durante años que dicho carácter impedía *modulaciones o grados de actuación en su injerencia*, por lo que la sola injerencia no consentida por un tercero en el ámbito de lo que se entiende por objeto del derecho suponía una infracción del mismo de alcance constitucional[956].

Este carácter rígido ha conducido a que las intromisiones, según consolidada doctrina, estén sometidas siempre a un *plus* de protección, que se concreta en una reserva jurisdiccional casi absoluta[957]. Dicho de otra manera: en nuestro ordenamiento la

---

[954] El art. 5.2 del Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la *Carta de derechos del usuario de los servicios de comunicaciones electrónicas*, dispone que los operadores no podrán acceder a la línea de un usuario final sin su consentimiento expreso e inequívoco.

[955] Cf. Moreno Catena, V., Garantía de los derechos fundamentales en la investigación penal, en *Poder Judicial*, 1987, p. 155; Asencio Mellado, J. M., Prueba prohibida y prueba preconstituda, Trivium, Madrid, 1989, p. 154; López-Fragoso Álvarez, T., Las intervenciones telefónicas en el proceso penal, Colex, Madrid, 1991, p. 22.

[956] Cf. STC 123/2002, de 20 de mayo.

[957] De forma expresa, la Constitución Italiana establece que la limitación del derecho al secreto de las comunicaciones sólo podrá producirse por auto motivado de la autoridad judicial con las garantías previstas en la ley.

restricción de este derecho ha quedado prohibida para cualquier autoridad que no sea la judicial, en virtud del art. 18.3 CE y su desarrollo en la LECrim[958].

Sin embargo, no puede perderse de vista que esta doctrina se originó principalmente en torno a la interceptación del *contenido* de las comunicaciones, sin perjuicio de que, en los últimos años, la jurisprudencia del TC en la materia[959] haya evolucionado de la mano de los avances tecnológicos y la aparición de las nuevas técnicas de investigación basadas en el análisis de los datos de tráfico de las comunicaciones. Como afirma la doctrina [960] , en el estado actual de las telecomunicaciones, tan útil resulta la interceptación de los contenidos de las comunicaciones de la persona investigada como el conocimiento de los medios con que cuenta para ejecutar, favorecer u ocultar los delitos que son objeto de una concreta investigación criminal. Así, han proliferado en nuestros días las técnicas de investigación basadas en el análisis de estos datos electrónicos, cuya utilidad es sobradamente reconocida. A través de los datos de tráfico puede obtenerse información decisiva para el enjuiciamiento de delitos, como la identidad de otros miembros de la organización criminal con los que mantiene conversaciones el imputado. Los datos de tráfico aportan también valiosa información sobre el origen de la comunicación, lo que permite, en algunos casos, ubicar el equipo informático desde el que se ha llevado a cabo, así como identificar a un abonado titular de la línea de conexión a través de la cual se accede a internet[961].

En relación con estos novedosos medios de investigación, nuestro TC ha declarado que ciertos aspectos formales de la comunicación, como la entrega de los listados por las compañías telefónicas a la Policía sin consentimiento del titular del teléfono, requiere también la correspondiente resolución judicial, pues supone una injerencia en el proceso de comunicación que está comprendida en el ámbito de protección del derecho

---

[958] Cf. art. 579 LECrim. La única excepción a este principio se concreta en los supuestos en que se investiguen bandas armadas o terroristas —arts. 55.3 y 25.2 CE—.

[959] Cf. Rodríguez Lainz, J. L., La intervención de las comunicaciones telefónicas: su evolución en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo, Editorial Bosch, Barcelona, 2002.

[960] Cf. Rodríguez Lainz, J. L., Identificación del terminal y sujeto pasivo en la intervención judicial de las comunicaciones, en Diario La Ley, núm. 6585, 2006.

[961] Cf. Salom Clonet, J., Incidencia de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos, op. cit., p. 136 y ss.

al secreto de las comunicaciones telefónicas del art. 18.3 CE. En su Sentencia 70/2002, de 3 de abril, el TC precisa que el artículo 18.3 del texto normativo contiene una especial protección de las comunicaciones, cualquiera que sea el sistema empleado para realizarlas, que se declara indemne frente a cualquier interferencia no autorizada judicialmente, concluyendo que la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos, de modo que la protección de este derecho alcanza a las interferencias habidas o producidas en un proceso de comunicación[962].Tal doctrina es plenamente aplicable al acceso a los datos conservados por mandato de la LCD, que como ya sabemos, requiere asimismo la autorización judicial de los listados y cualquiera otra de las informaciones retenidas.

Ahora bien, aunque el acceso y registro de estos datos constituye una forma de injerencia en el derecho al secreto de las comunicaciones, el propio TC ha reconocido que su intensidad es menor que la que se produce con la materialización de las escuchas telefónicas, siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad[963]. Con estos razonamientos, el TC —refiriéndose a un "ámbito externo" del secreto de las comunicaciones— ha venido a romper o matizar el carácter totalmente rígido de este derecho que había defendido, reconociendo en consecuencia la posibilidad de que existan distintos grados de intervención en el secreto de las comunicaciones, entre los que se cita como ejemplos, de un lado, la grabación de la conversación y, de otro, el simple recuento del número de llamadas y de los destinatarios de las mismas[964]. En consecuencia, aun admitiendo que todas estas conductas suponen una intromisión en el derecho al secreto de las comunicaciones, la distinta potencialidad lesiva que presentan supone reconocer también, correlativamente, que las garantías que rodean su injerencia pueden y deben ser menores[965].

---

[962] Cf. F. J. 9.

[963] Cf. STC 123/2002, de 20 de mayo.

[964] Ibíd.

[965] En la misma línea se sitúa el *Convenio sobre Ciberdelincuencia* de 23 de noviembre de 2001, ratificado por el Estado español el 20 de mayo de 2010, según el cual la recogida de los datos de tráfico

De este modo, al otorgar carta de naturaleza en nuestro sistema constitucional al *principio de menor intensidad* en la injerencia, el TC se ve obligado a reconocer —consecuentemente— la posibilidad de supuestos en los que se dé una menor exigencia constitucional en el respeto al derecho al secreto de las comunicaciones aún dentro del ámbito del derecho garantizado por el 18.3 CE, estableciéndose un doble régimen de protección constitucional de un mismo derecho, con un gradual nivel de protección. La opción por esta nueva línea interpretativa vio la luz en la trascendental STC 123/2002, de 20 de mayo, que trató la difícil cuestión de una orden de interceptación de datos de tráfico de comunicaciones telefónicas —concretamente, un listado de llamadas—, acordada por un Juzgado de Instrucción por una resolución de mero trámite: una providencia. La resolución muestra como principal campo de aplicación de ese principio de la menor intensidad el del denominado juicio de proporcionalidad de la medida, cuando literalmente llega a advertir que "no puede desconocerse [...] la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las "escuchas telefónicas", siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad". Por su parte, la STC 26/2006, de 30 de enero, volvió a hacer uso de la doctrina de la menor intensidad en la injerencia en el derecho al secreto de las comunicaciones de la persona concernida en un supuesto en el que los indicios aducidos por la unidad policial solicitante eran, según opinión del Juez instructor, demasiado vagos e imprecisos para conceder una autorización de injerencia sobre contenidos, pese a lo cual se admitió la constitucionalidad de la investigación preambular referida tan solo al listado de llamadas emitidas y recibidas. La STC 26/2006 confirmó la validez de la investigación basada en el listado de llamadas, pero no una injerencia sobre los contenidos dado el carácter impreciso de los indicios alegados por la Policía Judicial. Sin negar la existencia de indicios, el órgano jurisdiccional no los consideró suficientes para realizar una intervención total de las comunicaciones, pero sí para conocer la identidad de los interlocutores[966]. De esta

---

se estima, en principio, menos intrusiva toda vez que no revela el contenido de la comunicación, que se considera más sensible.

[966] No obstante, para una más completa ilustración, debe aclararse que esta doctrina constitucional tuvo un difícil acomodo en la jurisprudencia del Tribunal Supremo, a quien le costaba realmente definir de forma clara la frontera entre los ámbitos de protección del derecho al secreto de las comunicaciones en

manera se ve claramente que la intervención de los datos de tráfico puede acordarse como una diligencia previa a la intervención del contenido material que, con base en la menor lesividad para el derecho afectado, puede superar más fácilmente el juicio de necesidad[967], como también ha señalado la doctrina[968]. En todo caso, como vemos, la

---

cuanto a afectante a los datos de tráfico asociados a las mismas, y la protección constitucional de los datos de carácter personal. Las SSTS 459/1999, de 2 de marzo, y 2384/2001, de 7 de diciembre, anticiparon una clara afinidad por el principio del menor rigor en ambos componentes de la resolución habilitante; mientras que la más reciente STS 306/2002, de 25 de febrero aplicaba, sin quiebra ni relajación alguna, las doctrinas sentadas por los precedentes de las SSTS 816/2001, de 22 de mayo, 1233/2001, de 25 de junio y 1521/2001, de 23 de julio, exigentes del mismo rigor protector tanto respecto de los contenidos como de los datos adyacentes. O bien se vanalizaba la trascendencia constitucional de la afectación de lo que era considerado una auténtica mixtura entre los derechos al secreto de las comunicaciones y el derecho a la protección de datos de carácter personal, o bien se brindaba a los datos de tráfico exactamente la misma protección propia de los contenidos de comunicaciones.

La línea jurisprudencial, sin embargo, sobre todo desde la publicación de la STC 123/2002, de 20 de mayo, evolucionó claramente hacia el camino abierto por la implicación del principio de la menor intensidad de la injerencia, aunque de nuevo sin una capacidad clara de diferenciar los intereses y derechos constitucionales en conflicto, cual sucediera en la STS 1219/2004, de 10 de diciembre. Las SSTS 1086/2003, de 25 de julio, y 558/2005, de 27 de abril, incidieron de nuevo en la licitud del empleo de la fórmula de la providencia en el contexto de una intervención de contenidos ya acordada y en fase de ejecución. Evidentemente la situación es distinta, pues en un principio la ejecución de una medida afectante al contenido serviría de cobertura para la aceptación del recabo de listado de llamadas objeto de injerencia, tanto en el pasado como en el futuro, por considerar que los derechos afectados —en este caso sí se habla de la protección de datos de carácter personal— son acreedores de un nivel de exigencia y control mucho más bajo que el de una intervención sobre contenidos de comunicaciones. Las resoluciones más recientes, sí llegan a diferenciar claramente unos y otros ámbitos de protección constitucional, como sucede en la STS 130/2007, de 19 de febrero, en la que se considera interceptación de datos accesorios a comunicaciones el rastreo de frecuencias con las que se emiten comunicaciones a través de teléfonos móviles, sin contar para ello con una previa autorización judicial; y sobre todo la STS 780/2007, de 3 de octubre, que tras distinguir con claridad la naturaleza de contenido de comunicación y dato de carácter personal de los datos de tráfico en función del momento y la fuente de su obtención, sienta, ya aparentemente con carácter consolidado, la doctrina de que el recabo del listado de llamadas requiere de "un nivel de exigencia y control mucho más bajo que el de una intervención de las conversaciones porque la injerencia es mucho menor sin que exista vulneración al derecho fundamental al secreto de las comunicaciones".

[967] Cf. STS 1476/2005, de 25 de noviembre

aplicación del principio de la menor intensidad en la injerencia se proyecta sobre el juicio de proporcionalidad, toda vez que éste determina si está justificado el sacrificio del derecho fundamental afectado en función de las circunstancias del caso concreto[969]. De este modo, la autonomía de la intervención de los datos de tráfico con respecto a la intervención del contenido material nos permite sostener que el primer tipo de intervención podría adoptarse —además de para localizar o establecer vínculos entre sospechosos— con vistas a determinar si procede la intervención del contenido material, y por ello, podría fundarse en la investigación de delitos de menor entidad[970].

---

[968] Cf. González López, J. J., Los datos de tráfico de las comunicaciones electrónicas en el proceso penal, op. cit., p. 167.

[969] En una posición discrepante, VELASCO NÚÑEZ considera anticuada y obsoleta esta jurisprudencia, pues entiende que los datos de tráfico no deben incluirse como parte de la comunicación, sino que su protección constitucional resulta más adecuada por la vía del art. 18.1 o, al estar automatizados, por la del art. 18.4 CE. Entiende que el contenido del mensaje es el único núcleo duro y contenido efectivo u objeto posible de protección exclusiva del derecho al secreto de las comunicaciones del art. 18.3 CE. En la misma línea, el voto particular de la STS de 19 de febrero de 2007 señala que lo trascendente del contenido digno de protección por parte del derecho al secreto de las comunicaciones ha de ser aquello que, en realidad pueda llevar a calificar la injerencia como verdaderamente gravosa en el ámbito personal del investigado, es decir, los contenidos ideológicos de esa comunicación, los mensajes y el intercambio de ideas, opiniones, pensamientos, sentimientos, etc., que constituyen la esencia de la misma; en una palabra, la "conversación" que es susceptible de ser objeto de escucha y grabación y cuyo conocimiento permite obtener información de trascendencia probatoria. Los números identificativos con los que operan terminales no pueden constituir, por sí mismos, materia amparada por el secreto de las comunicaciones, pues afirmar lo contrario supondría confundir los medios que posibilitan la comunicación con la comunicación misma. Algunos autores entienden así que resulta más congruente y adecuado a la nueva realidad tecnológica que la cesión del listado de conversaciones mantenidas desde el teléfono móvil de un investigado no afecte el contenido del derecho al secreto de las comunicaciones garantizado por el 18.3 CE, toda vez que se trata en definitiva de datos de carácter personal custodiados en ficheros automatizados —SSTS 30 de noviembre de 2005 y 23 de enero de 2007—. Consideran que no puede haber equiparación posible entre una conversación intervenida y la mera indicación del teléfono y titular al que se efectuó la llamada —STS de 2 de octubre de 2004—. Cf. Velasco Núñez, E., Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios informáticos), Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia, CGPJ, Madrid, 2008, p. 112.

[970] Un precedente puede encontrarse en la vieja discusión sobre si los términos "observar" e "intervenir", utilizados en los párrafos 2 y 3 del art. 579 de la Ley de Enjuiciamiento Criminal, tienen o no

No puede dejar de notarse, en relación con esto último, que los criterios hasta ahora manejados por el TC para interpretar la noción de delito grave, lo son por razón de justificar una grave injerencia sobre derechos fundamentales de las personas concernidas, cual es la interceptación de los contenidos de las comunicaciones. Ello traía consigo la lógica consecuencia de que, a menor afectación del derecho constitucional, menor exigencia en la relevancia del fin público perseguido, lo cual, aplicado a la investigación y esclarecimiento de delitos, legitimaría supuestos no tan graves como los que podrían justificar una injerencia sobre contenidos. Tales reflexiones serán de suma utilidad para nuestro escrutinio al abordar más adelante la noción de delito grave en la LCD y su validez constitucional.

41.2.2.3 Secreto de las comunicaciones: distinción con la intimidad

No quisiéramos terminar esta exposición sobre las relaciones entre las medidas de la LCD y el derecho al secreto de las comunicaciones sin ofrecer una delimitación más completa de este derecho que nos permita salir al paso de posibles contraargumentos o malas interpretaciones. Concretamente, expondremos ahora las razones por las que el derecho a la intimidad no ha de ser ponderado a la hora de juzgar la constitucionalidad de las medidas contempladas por la LCD.

---

significados jurídicos distintos. Así, la intervención implicaría tomar conocimiento de la conversación telefónica, mientras que la observación supondría una menor injerencia, dado que no se llega a conocer el contenido de la conversación pero sí de su existencia, de sus interlocutores y de la duración. Pero, en este caso, la mayor parte de la doctrina ha entendido que el legislador no ha atribuido una eficacia jurídica distinta a ambos términos en función de la gravedad del delito, pues ello hubiera llevado a la paradójica consecuencia de que en los supuestos de delitos más graves sólo podría acordarse la injerencia más leve —la observación—. Así, el término "observación" debe ser entendido en sentido amplio, comprensivo tanto de la escucha o grabación de una conversación como del simple control de las llamadas realizadas desde un terminal. A pesar de ello, algunos autores han entendido que la regulación vigente de esta materia no constituye un obstáculo para entender que pueden existir grados distintos de limitación o de injerencia en el derecho fundamental al secreto de las comunicaciones, tal y como ha sido expuesto más arriba. Cf. Montero Aroca, J., La intervención de las comunicaciones telefónicas en el proceso penal, Tirant lo Blanch, Valencia, 1999, p. 21; y Nadal Gómez, L., La intervención de las comunicaciones telefónicas, Tribunales de Justicia, Revista española de derecho procesal, núm. 11, 2002.

Ciertamente, es innegable que el derecho al secreto de las comunicaciones se relaciona estrechamente con el derecho a la intimidad, dada la enorme virtualidad expansiva del derecho a la vida privada y el secreto de las comunicaciones en un contexto en el que existe una gran capacidad tecnológica de control social en manos del Estado. La propia sistemática constitucional —como señalamos— conecta intimidad y secreto de las comunicaciones al incluirlos en un mismo artículo: el 18 CE. También la jurisprudencia los ha puesto en conexión, afirmando que el secreto es una categoría jurídica funcional y estrechamente asociada a la de intimidad, en relación con la que opera como derecho fundamental-medio preordenado a la protección de las comunicaciones, debido —precisamente— a que éstas son el vehículo de contenidos inherentes al derecho fundamental-fin representado por la segunda[971]. En este sentido, también es indudable que ambos sirven al objeto de garantizar una cierta esfera de actuación y de desarrollo personal.

De hecho, una parte de la doctrina ha interpretado —creemos que erradamente— la conexión del derecho al secreto de las comunicaciones y el derecho a la intimidad como una relación de subordinación o derivación del primero respecto del segundo, de tal forma que la intimidad sería el género y el secreto de las comunicaciones una especie de la misma. Los defensores de esta posición entienden que el art. 18.1 CE se referiría de forma amplia al contenido del derecho a la intimidad mientras que los tres epígrafes siguientes vendrían a proteger los aspectos más vulnerables del mismo, cuales son la inviolabilidad del domicilio, el secreto de las comunicaciones y la protección del honor y la propia imagen frente al uso de la informática[972].

Desde esta perspectiva, el derecho al secreto de las comunicaciones debería ser tratado como un aspecto del derecho a la intimidad[973]. Todo el contenido normativo del precepto constitucional sería así reductible a la intimidad como bien jurídico

---

[971] Cf. STS de 19 de febrero de 2007.

[972] Cf. Ortí Vallejo, A., Derecho a la intimidad e informática, Comares, Granada, 1995; López Ortega, J. J., La protección de la intimidad en la investigación penal: necesidad y proporcionalidad de la injerencia como presupuesto de validez, Perfiles del Derecho Constitucional a la vida privada y familiar. Cuadernos de Derecho Judicial, CGPJ, Madrid, 1997, pp. 277-281.

[973] Cf. Rodríguez Ruiz, B., El secreto de las comunicaciones: tecnología e intimidad, McGraw-Hill, Madrid, 1998, p. 23.

autónomo[974] sin perjuicio de la heterogeneidad de las diferentes formas de intrusión[975]. Los apartados segundo, tercero y cuarto del art. 18 CE constituirían meras manifestaciones de un derecho único, lo cual no implicaría que, en todos estos supuestos, la afectación de la intimidad sea la misma, ni que, por tanto, las garantías procesales hayan de coincidir a la hora de limitar cada uno de estos derechos fundamentales[976].

Ciertamente, la cuestión no resulta sencilla, pues los bienes jurídicos protegidos por ambos derechos están evidentemente relacionados entre sí, como es el caso de las medidas de la LCD. De hecho, estos regímenes —como ha señalado algún autor[977]— pueden llegar a confluir e, incluso, en determinadas circunstancias, a fundirse hasta el punto de poder llegar a precisar la protección conjunta de ambas normas constitucionales.

Por una parte, el derecho a la intimidad personal y familiar del art. 18.1 CE es pacíficamente definido como un ámbito propio y reservado frente a la acción y al conocimiento de los demás y necesario para mantener una calidad mínima de la vida humana[978]. La intimidad, como concepto de carácter material, designa el área que cada cual se reserva para sí o para su familia, apartándola del conocimiento de terceros. Además, dada su naturaleza, el derecho a la intimidad personal y familiar sólo es

---

[974] Cf. Parejo Alfonso, L., El derecho fundamental a la intimidad y sus restricciones, Perfiles del Derecho Constitucional a la vida privada y familiar, Cuadernos de Derecho Judicial, CGPJ, Madrid, 1997, pp. 19-26.

[975] Destaca LÓPEZ ORTEGA que las posibilidades de lesión de este bien jurídico no se agotan en los tres supuestos mencionados, sino que también alcanza a las intervenciones corporales, a las vigilancias físicas, a la captación clandestina de imágenes y a la actuación de los agentes encubiertos. Cf. López Ortega, La protección de la intimidad en la investigación penal…, op. cit, p. 280.

[976] Cf. Gimeno Sendra, V., Las intervenciones electrónicas y la Policía Judicial, Diario La Ley, núm. 7298, 2009, pp. 2 y 3.

[977] Cf. Rodríguez Lainz, J. L., Intervención judicial en los datos de tráfico…, op. cit., p. 447.

[978] Cf. SSTC 73/1982, de 2 de diciembre; 197/1991, de 17 de octubre; y 143/1994, de 9 de mayo, entre otras.

predicable, con carácter general, de las personas físicas[979]. De forma diferente, la titularidad del derecho al secreto de las comunicaciones puede corresponder tanto a las personas físicas como a las jurídicas teniendo el cuenta el carácter de la información que posibilita su ejercicio por éstas últimas[980].

Además, sin negar que el derecho al secreto de las comunicaciones se relaciona con el derecho a la intimidad, no puede desconocerse —como bien defiende LÓPEZ-BARAJAS[981]— que posee un contenido más amplio, toda vez que garantiza a los interlocutores o comunicantes una protección que se proyecta sobre el proceso de comunicación mismo con independencia de que el contenido del mensaje transmitido pertenezca o no al ámbito de lo personal, lo íntimo o lo reservado[982]. Como ya hemos dicho, el objeto de este derecho es la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo comunicado, de tal forma que toda comunicación es para la norma fundamental secreta aunque sólo algunas sean íntimas[983]: no se dispensa el secreto en función del contenido de la comunicación, sino a cualquier clase de comunicación. Así, el objeto de este derecho es la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo que se está comunicando[984].

De esta manera, a pesar de nuestra sistemática constitucional, que parece conectar el derecho al secreto de las comunicaciones con el derecho a la intimidad, queda definitivamente clara la autonomía y sustantividad del derecho al secreto de las

---

[979] Cf. ATC 17 de abril de 1984. Ahora bien, en ocasiones, también se ha reconocido el derecho a la inviolabilidad del domicilio a las personas jurídicas como, por ejemplo, en la STC 137/1985, de 17 de octubre.

[980] Cf. Gimeno Sendra, V., Las intervenciones electrónicas y la Policía Judicial…, op. cit., p. 4.

[981] Cf. López-Barajas Perea, I., La intervención de las comunicaciones electrónicas, La Ley, Madrid, 2011, p. 121.

[982] Cf. STC 114/1984, de 29 de noviembre.

[983] Cf. STC 123/2002, de 20 de mayo.

[984] Cf. STC 123/2002, de 20 de mayo. Por otra parte, algún autor ha destacado el hecho de que el desarrollo ideológico y jurídico de la inviolabilidad del domicilio y del secreto de las comunicaciones como derechos individuales es históricamente anterior a la aparición en el plano jurídico de la idea de la necesidad de proteger la vida privada o la intimidad personal como tales. Cf. Aroz Santisteban, Derecho al respeto de la vida privada y familiar, op. cit., p. 256.

comunicaciones con independencia de que el contenido de lo comunicado incida en la esfera de lo íntimo. Es perfectamente posible violar el secreto de las comunicaciones sin atentar a la esfera íntima de una persona. Aplicado a nuestro caso, esto supone concluir que la afectación del primero —llevada a cabo por parte de la LCD— no comporta por sí misma del segundo, ni al revés.

Finalmente, conviene recordar que la separación del ámbito de protección de los derechos fundamentales a la intimidad personal —art. 18.1 CE— y al secreto de las comunicaciones —art. 18.3 CE—, se proyecta sobre su régimen jurídico. Así**,** mientras ex art. 18.3 CE la intervención de las comunicaciones requiere siempre resolución judicial, no existe en la Constitución reserva jurisdiccional absoluta respecto del derecho a la intimidad personal, donde se ha admitido, de forma excepcional, que en determinados casos y con la suficiente y precisa habilitación legal, sea posible que la Policía Judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas[985]. De forma diferente, en el caso del derecho al secreto de las comunicaciones nuestra ley fundamental ha sometido su limitación a un *plus* de protección, estableciendo una reserva jurisdiccional casi absoluta, en los términos ya vistos[986]. La única excepción a este principio se concreta en los supuestos en que se investiguen bandas armadas o terroristas —arts. 55.3 y 25.2 CE—. No es de extrañar que esta interdicción encuentre su necesario reflejo en el art. 6 LCD, que establece que los datos conservados de conformidad con la LCD "sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial"[987]. Un mecanismo de cesión de los datos conservados que no previera dicha autorización habría de considerarse inconstitucional a todas luces.

---

[985] Cf. SSTC 114/1984, de 29 de noviembre; 37/1999, de 22 de marzo; 70/2002, de 3 de abril, y STS de 30 de noviembre de 2005. También, cf. Gimeno Sendra, V., Derecho Procesal Penal, Colex, Madrid, 2004.

[986] De forma expresa, la Constitución Italiana establece que la limitación del derecho al secreto de las comunicaciones sólo podrá producirse por auto motivado de la autoridad judicial con las garantías previstas en la ley (art. 14).

[987] Cf. art. 6.1 LCD.

41.2.2.4 Protección de datos de carácter personal: concepto de la protección de datos y distinción con el secreto de las comunicaciones

La estrecha relación de los derechos fundamentales implicados nos obliga a ser particularmente cuidadosos a la hora de delimitar los distintos bienes jurídicos y los ámbitos de protección implicados. En el estudio de la constitucionalidad de la LCD, no podemos dejar de abordar sus relaciones con el derecho fundamental a la protección de datos de carácter personal —también llamado derecho a la autodeterminación informativa [988] —, que suele presentar especial relieve en el ámbito de las comunicaciones electrónicas y se concibe además como una garantía necesaria frente a las nuevas formas concretas de amenazas a la dignidad y derechos de las personas en general[989]. Pese a que la CE omite toda referencia a la protección de datos, el TC lo ha considerado un derecho fundamental autónomo respecto a la intimidad, dotado de un estatus jurídico propio, que encuentra su fundamento en el art. 18.4 CE, el cual establece que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" [990]. Su desarrollo se ha llevado a cabo por la LOPD[991]

Centrándonos en el objeto de nuestro estudio, el criterio para delimitar el ámbito del derecho a la protección de datos respecto al derecho al secreto de las comunicaciones viene dado por la STC 123/2002, en la que el TC estableció que "la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u

---

[988] Cf. Martín-Retortillo Baquer, L., Consideraciones comunes a los artículos 49, 50 y 51 de la Ley General de Telecomunicaciones, en AA.VV., *Comentarios a la Ley General de Telecomunicaciones*, Civitas, Madrid, 1998, p. 428.

[989] Cf. STC 292/2000, de 30 de noviembre.

[990] Ibíd.

[991] Mientras que el ordenamiento comunitario hace lo propio a través de la Directiva 95/46/CE de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y 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.

otros derechos puesto que no suponen una interferencia en un proceso de comunicación"[992]. De este modo, la protección de este derecho alcanza sólo a las interferencias habidas o producidas durante el proceso de comunicación propiamente —precisión que también se recoge en la STC 56/2003—[993], y así, los datos relativos al emisor y receptor de una comunicación, una vez finalizada ésta, ya no deben protegerse por el derecho fundamental al secreto de las comunicaciones, a pesar de su estrecha conexión con la comunicación realizada[994]. Siendo más concretos, lo antedicho comporta que mientras dura el proceso de comunicación, resulta afectado el derecho al secreto de las comunicaciones ya incida el acto de injerencia sobre el contenido de la comunicación o se limite a sus elementos externos o adyacentes. En cambio, cuando la comunicación se ha consumado y los datos de tráfico relativos a las comunicaciones se almacenan en una base de datos como las establecidas por la LCD, pasan a configurarse como datos de carácter personal relativos a una comunicación que tuvo lugar en el pasado. Por las razones que ya adelantamos, la conservación de datos implica a nuestro entender una restricción del derecho al secreto de las comunicaciones en lo que se refiere a la acción de captar los datos. A partir de ese momento, el acto del almacenaje y tratamiento está sometido a la LOPD e implica en consecuencia una injerencia en el derecho a la protección de datos.

Volviendo a nuestra exposición, si la posición del TC ha sido en todo momento firme y decidida en la doctrina sobre la extensión de este derecho[995] —con algunos

---

[992] Cf. STC 123/2002, de 20 de mayo.

[993] Citado también en Dictamen 32/2007 del Consejo de Estado…, doc. cit., apartado II.B.

[994] Cf. STC 70/2002, de 3 de abril.

[995] La doctrina del TEDH, centrada esencialmente en la famosa sentencia del caso Malone, no parece que ofrezca una diferencia sustancial con la posición mantenida por nuestra jurisprudencia, fiel seguidora en este punto de una doctrina que no en vano tiene su origen en dicho Tribunal. Sin embargo, la diferenciación podría encontrarse en una visión diversa de las comunicaciones ya consumadas como amparadas aún por el derecho al secreto de la correspondencia privada regulado en el art. 8.1 CEDH. Si para la tradición constitucional española las comunicaciones ya consumadas almacenadas en determinados soportes documentales, bien archivos físicos o informáticos, tendrían la consideración de documentos, y protegidos tan sólo por tanto por el derecho a la intimidad, la visión del TEDH, al menos en su reciente STEDH de 16 de octubre de 2007 —caso Wieser y Bicos Beiligungen Gmbh v. Austria—, en un supuesto de registro en sede de servicio jurídico de una empresa se accedió al contenido de

pronunciamientos ligeramente más ambiguos, como los de las SSTC 70 y 120/2002, y sobre todo con la más reciente STC 230/2007, de 5 de noviembre[996]— en la doctrina emanada por el TS puede apreciarse un cierto grado de desorientación a la hora de aplicar los postulados defendidos por el Tribunal Constitucional, manteniéndose la cierta confusión que le ha caracterizado a la hora de discriminar, conforme a las directrices anticipadas por el TEDH y el TC, cuándo se afecta al derecho al secreto de las comunicaciones y cuándo al derecho a la protección de datos de carácter personal o simplemente a la intimidad. En esta borrosa línea se mueven sentencias tales como las SSTS 1683/2003, de 11 de diciembre y 75/2003, de 23 de enero, que tratan la cuestión prácticamente a título de anécdota, o como la STS 1086/2003, de 25 de julio[997], que llega a afirmar que la técnica de recabar el listado de llamadas no afecta al derecho a la intimidad de la persona concernida; otras sentencias, como la STS 1683/2003, de 11 de diciembre, son incapaces de separar del régimen de la garantía del derecho al secreto de las comunicaciones los datos de tráfico de comunicaciones ya consumadas,

---

mensajes recibidos por otra empresa, encajó el conflicto en la protección del derecho al secreto de la correspondencia privada. Entre otras interesantes consideraciones acerca de la actuación judicial de registro de archivos informáticos, el Tribunal llega a afirmar de forma tajante que "la búsqueda e incautación de datos electrónicos constituye una interferencia del derecho de los interesados al respeto de su correspondencia dentro del ámbito del art. 8". Realmente, si bien acto seguido se hace una clara distinción con la protección de la privacidad, sobre la que no se entra al entenderse ya vulnerado el derecho a la correspondencia privada, se está realizando una interpretación más abierta del derecho al secreto de las comunicaciones que no tendría parangón en nuestro ordenamiento jurídico, en el que sí se diferencian con claridad ambos ámbitos de protección, y en los que en uno y otro caso se da una respuesta efectiva a la salvaguardia de los distintos derechos afectados.

[996] "La entrega de listados por las compañías telefónicas a la policía sin consentimiento requiere resolución judicial, pues la forma de obtención de datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones telefónicas del art. 18.3. CE". La cita de tales sentencias nos podría llevar al equívoco de pensar que tales peticiones de listados afectarían siempre y en todo caso al derecho al secreto de las comunicaciones, pero no debe olvidarse que tal doctrina parte del precedente de la STEDH de 2 de agosto de 1984 —caso Malone vs. Reino Unido—; y ésta hacía referencia a la obtención, mediante la técnica del recuento, de los números marcados por determinado terminal telefónico, cuando la comunicación tenía lugar, y que las mismas sentencias se contextualizan en el marco de la doctrina general antes descrita.

[997] Cf. STS 1683/2003, de 11 de diciembre.

sometiéndolos al régimen de aquéllas. El acierto en la diferenciación podrá encontrarse, sin embargo, claramente, a través de las SSTS 459/1999, de 22 de marzo, 1086/2003, de 25 de julio y 1231/2003, de 25 de septiembre, que en tal contexto, y ante la imputación por parte del recurrente de transgresión del art. 18.3 CE, nos dirá que "no se trata de una intervención en el proceso de comunicación, ya entendido como transmisión de conversaciones, ni localización, al tiempo de su realización, de las llamadas efectuadas, de la identificación de usuarios, limitándose a la comprobación de unos números". La STS 780/2007, de 3 de octubre, centra ya de una forma incontestable el conflicto en la línea de considerar a los datos de tráfico de conversaciones ya mantenidas en el ámbito de la protección de los datos de carácter personal. Si analizamos la jurisprudencia, comprobamos que la entrega por la operadora del listado de las llamadas ya ejecutadas con anterioridad desde un determinado número de teléfono no afecta al contenido propio del derecho al secreto de las comunicaciones, toda vez que se trata, en definitiva, de datos de carácter personal, custodiados en ficheros automatizados —a los que se refiere la LOPD— en desarrollo de lo previsto en el art. 18.4 CE, estableciéndose en la misma que el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, el cual, sin embargo, no será preciso cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas. De hecho, 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. El registro de las llamadas efectuadas desde un determinado número de teléfono forma parte del conjunto de datos que las correspondientes compañías telefónicas obtienen y conservan para poder determinar el precio que periódicamente debe abonarles el titular de aquél, de forma semejante a como hacen las entidades bancarias con los titulares de las cuentas corrientes, al remitirles periódicamente información sobre el movimiento de las mismas[998].

[998] Cf. STS 459/1999, de 7 de diciembre.

La doctrina expuesta se complementa con un criterio doctrinal muy extendido[999], conforme al cual un mismo dato de tráfico puede conceptuarse como un elemento *dinámico* —esto es, como un elemento externo de una comunicación *que está teniendo lugar*— o como un elemento *estático* —como un dato que es almacenado cuando la comunicación se da por concluida, incluidas las comunicaciones infructuosas[1000]—.

El hecho de que un mismo dato de tráfico pueda presentar un carácter dinámico o estático, implica como vemos una gran diferencia a efectos de la legitimidad de una injerencia sobre el mismo. Concretamente, en nuestro marco constitucional se constatan claras diferencias entre las exigencias propias de una injerencia sobre las comunicaciones y las de una injerencia sobre datos de carácter personal. La intervención de las comunicaciones ex art. 18.3 CE requiere siempre resolución judicial, pero no existe en la Constitución reserva jurisdiccional absoluta respecto del derecho a la intimidad personal, donde se ha admitido, de forma excepcional, que en determinados casos y, con la suficiente y precisa habilitación legal, es posible que la Policía Judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas[1001].

Vuelta la mirada sobre la LCD y los datos de telecomunicaciones, los denominados datos de abonado no ofrecen duda alguna sobre su protección conforme al derecho fundamental que comentamos. Mucho mas compleja es la protección de los datos de localización y los datos de trafico *stricto sensu*, que también quedan retenidos por mandato de la LCD[1002]. Lo cierto es que, si bien los datos de tráfico siguen siendo

---

[999] Cf., vg., Rodríguez Lainz, J.L., Los límites a la dimensión formal del derecho al secreto de las comunicaciones, Diario La Ley, Nº 7669, Sección Doctrina, 8 Jul. 2011, Año XXXII, p. 5.

[1000] Sincrónico o diacrónico serían denominaciones más exactas.

[1001] Cf. Gimeno Sendra, V., Las intervenciones telefónicas en la jurisprudencia del TC y TS, Estudios jurídicos en homenaje al profesor Aurelio Menéndez, Civitas, Madrid, 1996.

[1002] Imagínese un caso en el que los comunicantes convienen en transmitirse el número de abonado de un teléfono móvil recién activado mediante una llamada infructuosa a teléfono que no estaba judicialmente intervenido para tratar de eludir posibles intervenciones; en puridad, estaríamos hablando en este caso de una comunicación en la que coinciden dato de tráfico y contenido, pues éste mismo es el objeto de lo que se transmite. Si el dato se obtuviera ex post, acudiendo a la información almacenada en los archivos de la operadora telefónica, se crearían claras tensiones en el análisis del derecho constitucional afectado y la

conceptualmente datos de tráfico "con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso, bien de la lícita facturación del servicio prestado, bien de su ilícita difusión", los tales experimentan un importante cambio cuando pasan a estar protegidos por el derecho a la protección de datos[1003]. Desde el momento en que se trata de datos relacionados con comunicaciones perfeccionadas, su protección bajo un ámbito distinto al del secreto de las comunicaciones se convierte en un factor a tener en cuenta a la hora de establecer el juicio de proporcionalidad de la medida invasiva del derecho de las personas concernidas. En todo caso, cuando hayamos expuesto la regulación de su tratamiento según la LGT volveremos sobre este asunto para ofrecer una plausible respuesta.

41.2.2.5 Proteccion de datos: distinción con la intimidad

Al igual que hemos hecho al tratar el derecho al secreto de las comunicaciones, parece conveniente que —a fin de garantizar que nuestro análisis del marco constitucional de la LCD sea completo, sin dejar margen a la duda o la inexactitud— añadamos ahora algunas observaciones sobre los rasgos que distinguen la protección de datos del derecho a la intimidad, al hilo de lo cual expondremos otros rasgos del primero.

Lo cierto es que, aunque los dos derechos comparten el objetivo de ofrecer una eficaz protección constitucional de la vida privada, personal y familiar, se diferencian entre sí tanto por el objeto de su protección como por su contenido.

En primer lugar, el objeto de protección del derecho fundamental a la protección de datos es más amplio que el de la intimidad, en tanto que el mismo "no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales"[1004]. El constituyente —ha explicado el TC[1005]— quiso garantizar

---

posible superación del límite perfilado en el art. 1.3 LCD: la no conservación de contenidos de comunicaciones.

[1003] Cf. STC 123/2002, de 20 de mayo.

[1004] STC 292/2000, de 30 de noviembre.

mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto: "su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal" [1006]. Esto también alcanza, por consiguiente, a aquellos datos personales públicos que, por el hecho de serlo, esto es, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado. El que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos datos personales objeto de tutela son todos aquellos que identifican o permitan identificar a cualquier persona, pudiendo servir para la confección del perfil ideológico de la persona, racial, sexual, económico o de cualquier otra índole que, en determinadas circunstancias, puede constituir una amenaza para el individuo[1007]. Así, el derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no relativos al honor, la ideología, la intimidad personal y familiar o a cualquier otro bien constitucionalmente amparado [1008]. Esa amplia definición permite acoger todos los formatos en los que aparece la información y no es imprescindible que identifiquen clara e inequívocamente a su titular, sino que se trata de proteger, por lo tanto, "cualquier información", incluso aquella que en un inicio podría considerarse como irrelevante, pero que poniéndola en relación con otro tipo de datos puede dar un perfil completo de la persona o sirvan como medio para identificarlo. Se habla de *identificabilidad* cuando la identidad de un sujeto no se puede deducir directamente de un conjunto de datos pero sí pueda resultar de interrelacionarlos con otros. A su vez, este criterio de la *identificabilidad* hay que entenderlo como lo "razonablemente identificable", de tal manera que los supuestos en que la vinculación entre el titular de los datos y la información que se dispone para identificarlo requiera esfuerzos

---

[1005] Ibíd.

[1006] Ibíd.

[1007] Cf. STEDH 27798/1995, de 16 de febrero de 2000, Amann contra Suiza, ap. 65, y STC 292/2000, de 30 de noviembre. Al respecto, cf. también SAN de 24 de enero de 2003, Rec. 400/2001, fundamento jurídico quinto, que se fundamenta en la sentencia constitucional aludida.

[1008] Cf. SSTC 110/1984, de 26 de noviembre, y 144/1999, de 22 de julio.

desproporcionados, no se puede decir que se está ante datos personales estrictamente[1009]. Se trata, por tanto, de un derecho dotado de una doble dimensión: como un instituto de garantía, capaz de albergar en su seno una eficaz barrera de protección frente a intrusiones no deseadas no sólo respecto de los tradicionales derechos al honor y a la vida privada y familiar, sino de los restantes derechos —"el pleno ejercicio de sus derechos"—; y como derecho constitucional de nuevo cuño, la libertad informática, que define como "derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática"[1010].

El segundo aspecto del derecho fundamental a la protección de datos de carácter personal que lo diferencia del derecho a la intimidad radica en su contenido. A diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de los así conocidos, el derecho a la protección de datos atribuye a su titular un concreto haz de facultades consistente en diversos poderes jurídicos, cuyo ejercicio impone a terceros deberes que no se contienen en el derecho fundamental a la intimidad y que comparten con éste el cometido de garantizar una eficaz protección de los mismos[1011]. El derecho a la autodeterminación informativa, por tanto, se erige en la facultad de controlar todos los datos que se refieren a cada uno y acoge tanto la potestad de imponer a terceros el deber de abstenerse de intromisión alguna en esta esfera, como la facultad positiva de controlar lo que ocurre con dichos datos, mediante el ejercicio del derecho de acceso, de rectificación, de cancelación, de información, de consentimiento y de oposición[1012]. El mencionado haz de facultades que, como nos advierte el TC, "consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya

---

[1009] Cf. Conclusiones y recomendaciones de la APD, en la inspección sectorial de oficio de "Concursos, juegos y sorteos de Televisión", disponible en http://www.agpd.es.

[1010] Cf. STC 254/1993, de 20 de julio.

[1011] Cf. SSTC 73/1982, de 2 de diciembre; 89/1987, de 3 de junio; 234/1988, de 2 diciembre; 197/1991, de 17 de octubre; 134/1999, de 15 de julio; o 115/2000, de 10 de mayo.

[1012] Cf. STC 292/2000, de 30 de noviembre.

concreta regulación debe establecer la Ley"[1013], garantiza a la persona un poder de control y disposición sobre sus datos personales imponiendo a los terceros determinados deberes de hacer[1014]. Sirvan de ejemplo el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos[1015]. El afectado, como titular de los datos objeto de tratamiento, es la persona que se halla en condiciones de ceder los datos y acceder a la información acerca de su almacenamiento, tratamiento o transferencia[1016]. Todo ciudadano puede autorizar el tratamiento de sus datos personales mediante una manifestación de voluntad inequívoca, libre, específica e informada aquel de derecho[1017]. Ésta es la principal manifestación del principio de autodeterminación informativa o *habeas data*. Estas garantías incluyen el derecho a controlar su uso, aunque se inserten en un programa informático, o afecten a la salud de los trabajadores[1018]. En cualquier caso, se exige que el ciudadano pueda conocer la existencia y los rasgos de esos ficheros y, sobre todo, el tratamiento que les dan las entidades públicas o privadas que los posean[1019]. El derecho a la protección de los datos personales puede definirse como el poder de disposición sobre los mismos, y una de las facultades principales que compone dicho derecho, que consiste en conocer quién o quiénes los poseen, consiste en conocer cuál es la finalidad de su tratamiento y, en función de todo ello, la facultad de facilitarlos, modificarlos y eliminarlos[1020]. De aquí se desprende que, en un inicio,

---

[1013] Ibíd.

[1014] Tal "concreta regulación" en nuestro Derecho positivo se contiene en la LOPD y, en el ordenamiento comunitario, por la Directiva 95/46/CE, 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 por la Directiva 2002/58/CE relativa la tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

[1015] Cf. STC 254/1993, de 20 de Julio.

[1016] Cf. Art. 3.c) LOPD.

[1017] Cf. Art. 3 LOPD.

[1018] Cf. STC 202/1999, de 8 de noviembre, fundamento jurídico 5. Por todas, SSTC 30/1999, de 8 de marzo, fundamento jurídico único; 223/1998, de 24 de noviembre, fundamento jurídico único, y 198/1998, de 13 octubre, fundamento jurídico único.

[1019] Cf. STC 254/1993, de 20 de julio.

[1020] Cf. STEDH 23224/1994, de 25 de marzo de 1998, Kopp contra Suiza, ap. 53.

sólo mediante el consentimiento informado del ciudadano sus datos personales pueden ser tratados, conservados, modificados y eliminados[1021].

De todo lo expuesto se deduce que el derecho fundamental a la intimidad referido en el art. 18.1 CE no aporta por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico, dadas las amplísimas posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales. Afirma en este sentido nuestro Tribunal Constitucional que la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede del ámbito propio del derecho fundamental a la intimidad —art. 18.1 CE—, y que se traduce en un derecho de control sobre los datos relativos a la propia persona[1022]. La llamada "libertad informática" es así el derecho a controlar el uso de los mismos datos insertos en un programa informático —*habeas data*— y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención. Aspecto que —junto con los anteriores— afecta directamente a las disposiciones de la LCD.

Lo expuesto no ha impedido, no obstante, que el propio TC conecte ambos derechos, afirmando que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos y de contenido aparentemente neutro, no incluyese garantías adecuadas

---

[1021] El TEDH ha exceptuado la necesidad de ese consentimiento en ciertos supuestos que han de preverse por ley, siempre que esa medida sea estrictamente necesaria en una sociedad democrática. Además, el contenido de esa norma ha de ser previsible y fijar unas garantías adecuadas y suficientes contra los abusos. Cf. STEDH 28341/1995, de 4 de mayo de 2000, Rotaru contra Rumania, ap. 59.

Como una de las excepciones, la Ley presupone que la firma de un contrato comporta la cesión, conservación y tratamiento de ciertos datos personales —art. 11 LOPD—. La entidad pública o privada que los posee —tenedor— ha de tratarlos conforme al principio de proporcionalidad. Eso significa que no pueden ser empleados para finalidades distintas de aquéllas para las que hubieran sido recogidos. Cf. art. 4.2 LOPD y SSTC 254/1993, de 20 de julio, fundamento jurídico 7., y 94/1998, de 4 de mayo, fundamento jurídico 4.

Con carácter general, se prohibe el tratamiento de los datos personales, cuando no exista una justificación que permita mantener los datos en el fichero, o cuando se están utilizando en contra del consentimiento manifestado por el afectado. Cf. SAN (S. 3.ª) de 11 de mayo de 2001, Rec. 12/2000, y SAN de 6 de julio de 2001, Rec. 314/2000.

[1022] Cf. SSTC 202/1999, de 20 de julio, y 202/2000, de 24 de julio.

frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera que lo harían las intromisiones directas en el contenido nuclear de ésta[1023]. Sin embargo, no puede desconocerse que la enorme variedad de datos de carácter personal y la pluralidad de bases de información en poder de sujetos muy diversos, dificulta mucho la posibilidad de conseguir una legislación uniforme sobre la materia en el marco de la investigación penal[1024]. Existen multitud de normas reglamentarias sectoriales que contemplan excepciones a la norma general[1025].

41.2.3 Proteccion de los datos externos de la comunicación electrónica y de los datos de abonado en la LGT

Una vez explicadas las implicaciones jurídico-constitucionales de la LCD en lo que respecta a los derechos fundamentales en liza, nos ocuparemos ahora de exponer cómo nuestro legislador ha desarrollado y concretado toda esta doctrina en el marco del Derecho de las telecomunicaciones, es decir, cómo la LGT regula la relación de los proveedores de servicios de redes con ambos tipos de datos[1026].

[1023] Cf. STC 143/1994, de 9 de mayo.

[1024] Cf. Pedraz Penalva, E., La utilización en el proceso penal…, op. cit. p. 34.

[1025] Por su parte, el TEDH afirma que el mero hecho de memorizar datos relativos a la vida privada de una persona constituye una injerencia en el sentido del art. 8 CEDH, con independencia de que la información memorizada se utilice o no posteriormente. Sin embargo, para determinar si la información de carácter personal conservada por las autoridades hace que entre en juego uno de los aspectos de la noción de vida privada, el Tribunal tendrá debidamente en cuenta el contexto particular en el que ha sido recogida y conservada la información, el carácter de los datos consignados, la manera en la que son utilizados y tratados y los resultados que pueden extraerse de ellos. Cf. STEDH de 4 de diciembre de 2008, caso. S. y Harper contra Reino Unido.

[1026] Sobre esta cuestión, cf. las clásicas monografías: De la Quadra Salcedo, T., Derecho de la Regulacion Economica, Tomo IV: Telecomunicaciones, Iustel, Portal Derecho, 2009; Cremades, J., y Rodriguez-Arana Muñoz, J., Comentarios a la Ley General de Telecomunicaciones, La Ley, 2004; y, Garcia de Enterria, E., Comentarios a la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, Civitas Ediciones, 2004.

Con este fin, hemos de empezar nuestro análisis estudiando la relación entre las compañías de comunicaciones electrónicas —telefónicas y de internet— y los datos externos que gestionan. Como ya hemos dicho, el derecho al secreto de las comunicaciones viene a proteger el proceso de comunicación entre los sujetos emisores y receptores frente a intromisiones de terceros[1027]. Esta protección se extiende en la actualidad tanto al contenido de la comunicación —incluido en el núcleo del derecho desde sus orígenes— como a los aspectos formales del proceso de transmisión —los datos de tráfico externos de la comunicacion—, y defiende frente a la injerencia tanto de terceros completamente ajenos a la comunicación como —lo que es trascendental para nuestro estudio— de los terceros que actúan en calidad de facilitadores técnicos de la comunicación, entre ellos, señaladamente, los operadores. En principio, el derecho fundamental impone que los únicos datos de tráfico que estos últimos pueden conocer, utilizar o retener sean sólo los necesarios para poder llevar a cabo eficazmente su labor transmisora, y por el tiempo exclusivamente necesario para tal fin. Este rasgo del secreto de las comunicaciones ha sido tradicionalmente descuidado por la doctrina y por la jurisprudencia, más preocupados por las implicaciones procesales y penales del derecho fundamental. Sin embargo, tal faceta no ha sido desatendida por el legislador, que al ocuparse de regular las telecomunicaciones en la LGT, determina, en primer lugar, que los operadores que exploten redes públicas de comunicaciones o que presten servicios de comunicaciones electrónicas disponibles al público deben garantizar el secreto de las comunicaciones, adoptando las medidas técnicas necesarias con tal finalidad —cf. art. 33 LGT—, y en segundo lugar, que los abonados a los servicios de comunicaciones electrónicas tienen derecho a que sus datos de tráfico "se hagan

[1027] Además, en una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo una garantía de la libertad individual, sino que se erige, asimismo, en la garantía para el ejercicio de otros múltiples derechos y libertales tales como la libertad de opinión, ideológica y de pensamiento, la libertad de expresión e información, etc. Como ha indicado el TC, constituye asimismo un instrumento de desarrollo cultural, científico y tecnológico colectivo, y en todo caso, una garantía del pluralismo y de la democracia. Cf. SSTC 281/2006, de 9 de octubre; 56/2003, de 24 de marzo, y 123/2002, de 20 de mayo.

anónimos o se cancelen" cuando "ya no sean necesarios a los efectos de la transmisión de una comunicación"[1028].

Veamos todos estos aspectos con mayor detenimiento.

En primer lugar, conviene destacar que ya entre los principales objetivos de la LGT[1029] se cuenta expresamente la defensa de los intereses de los usuarios[1030], que se lleva a

---

[1028] Cf. art. 38.3.a) LGT. Sostenemos que el derecho recogido en la LGT no es de mera configuración legal, sino que forma parte del contenido del derecho fundamental, por más que doctrina y jurisprudencia no hayan dedicado mucha atención a este rasgo del derecho al secreto de las comunicaciones. La LCD viene a ratificar la existencia de esta faceta del derecho, al verse obligada a explicitar que las compañías no están autorizadas a aprovechar o utilizar los registros generados —cf. art. 4.1 LCD—. De este modo, el mero hecho de la captación de una amplia lista de datos de tráfico y su archivo automatizado por parte de los operadores debe estimarse como una injerencia imperio legis en el derecho al secreto de las comunicaciones. El hecho de que los datos queden retenidos e inutilizados no modifica esta valoración, puesto que la medida legislativa viene a obligar a que se realicen unas conductas contrarias al contenido del derecho, que de operar plenamente, obligarían a que todas esas categorías de datos ni fueran captados ni mucho menos conservados ni tratados.

Asimismo, el art. 5.2 del Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la *Carta de derechos del usuario de los servicios de comunicaciones electrónicas*, dispone en la misma línea que los operadores no podrán acceder a la línea de un usuario final sin su consentimiento expreso e inequívoco.

[1029] El tenor literal del artículo reza así:

Artículo 3. *Objetivos y principios de la Ley.*

Los objetivos y principios de esta Ley son los siguientes:

a) Fomentar la competencia efectiva en los mercados de telecomunicaciones y, en particular, en la explotación de las redes y en la prestación de los servicios de comunicaciones electrónicas y en el suministro de los recursos asociados a ellos. Todo ello promoviendo una inversión eficiente en materia de infraestructuras y fomentando la innovación.
b) Garantizar el cumplimiento de las referidas condiciones y de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas, en especial las de servicio universal.
c) Promover el desarrollo del sector de las telecomunicaciones, así como la utilización de los nuevos servicios y el despliegue de redes, y el acceso a éstos, en condiciones de igualdad, e impulsar la cohesión territorial, económica y social.
d) Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones, como la numeración y el espectro radioeléctrico, y la adecuada protección de este último, y el acceso a los derechos de ocupación de la propiedad pública y privada.

cabo "asegurando su derecho al acceso a los servicios de comunicaciones electrónicas", así como la salvaguarda, en la prestación de éstos, "de los imperativos constitucionales, en particular, el de no discriminación, el del respeto a los derechos al honor, a la intimidad, a la protección de los datos personales y al secreto en las comunicaciones, el de la protección a la juventud y a la infancia y la satisfacción de las necesidades de los grupos con necesidades especiales, tales como las personas con discapacidad"[1031].

A los efectos anteriores, establece el art. 3.e) LGT que podrán imponerse obligaciones a los prestadores de los servicios para la garantía de dichos derechos, aspecto que la LGT desarrolla en sus arts. 33 a 38, que comprenden el Capítulo III del Título III bajo la ya expresiva rúbrica de *Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas*[1032]. Así, el art. 33 LGT establece un deber general de protección del secreto de las comunicaciones por parte de los operadores que explotan redes públicas de comunicaciones electrónicas o que prestan servicios de comunicaciones electrónicas disponibles al público[1033]. En este sentido, las compañías

---

e) Defender los intereses de los usuarios, asegurando su derecho al acceso a los servicios de comunicaciones electrónicas en adecuadas condiciones de elección, precio y calidad, y salvaguardar, en la prestación de éstos, la vigencia de los imperativos constitucionales, en particular, el de no discriminación, el del respeto a los derechos al honor, a la intimidad, a la protección de los datos personales y al secreto en las comunicaciones, el de la protección a la juventud y a la infancia y la satisfacción de las necesidades de los grupos con necesidades especiales, tales como las personas con discapacidad. A estos efectos, podrán imponerse obligaciones a los prestadores de los servicios para la garantía de dichos derechos.

f) Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.

g) Promover el desarrollo de la industria de productos y servicios de telecomunicaciones.

h) Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea".

[1030] Cf. art. 3.e) LGT.

[1031] El art. 3.e) LGT se hace eco así de lo dispuesto en el art. 20 CE.

[1032] Es precisamente en el área regulada por estos seis artículos en donde las disposiciones de la LCD vienen a encuadrarse como una excepción a sus principios generales.

[1033] Transcribimos aquí el texto original del artículo, tal como fue publicado el 4 de noviembre de 2003 y estuvo en vigor hasta la LCD: "Artículo 33. Secreto de las comunicaciones. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas

dedicadas a la explotación de estas redes tienen la obligación expresa de garantizar el secreto de las comunicaciones "de conformidad con los artículos 18.3 y 55.2 de la Constitución" y "debiendo adoptar las medidas técnicas necesarias" para preservar tal finalidad[1034].

En relación con esto, cabe señalar que —en su redacción previa a la entrada en vigor de la LCD— el art. 33 LGT añadía el deber adicional para los operadores de adoptar a su costa "las medidas que se establezcan reglamentariamente para la ejecución de las interceptaciones dispuestas conforme a lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia". En estas dos últimas normas citadas se recogía y recoge una buena porción del régimen conforme al cual puede efectuarse en nuestro Estado de derecho la interceptación de las comunicaciones con fines de descubrimiento y comprobación de hechos delictivos[1035] o para el cumplimiento de las funciones asignadas al CNI[1036].

---

disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

Asimismo, los operadores deberán adoptar a su costa las medidas que se establezcan reglamentariamente para la ejecución de las interceptaciones dispuestas conforme a lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia".

[1034] Como es bien sabido, el art. 18.3 CE es el que garantiza en nuestra carta magna el secreto de las comunicaciones y "en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial", en tanto que el art. 55.2 CE previene la posible suspensión de este derecho de acuerdo con una ley orgánica, con la necesaria intervención judicial y el adecuado control parlamentario, para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas" No estará de más recordar que el art. 55.2 CE dispone que "una Ley Orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas".

[1035] Cf. art. 579.1 LECrim.

[1036] Cf. art. único, apartado 1, de la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. Con la entrada en vigor de la LCD, el art. 33 LGT recibió una nueva y mucho más amplia redacción a través de su Disposición Final Primera, que le añadió nueve

Regulado en estos términos el principal medio de injerencia en el derecho al secreto de las comunicaciones, los demás artículos se centran de reforzar las garantías de este derecho y el modo en que debe ser respetado por las compañías de telecomunicaciones en el desarrollo de sus actividades.

Así, la LGT extiende su preocupación por la privacidad a la regulación de las redes de comunicaciones electrónicas en el interior de los edificios[1037] y a las condiciones para el cifrado en las redes y servicios de comunicaciones electrónicas[1038]. Es decir, aspectos de la protección del secreto frente a la injerencia de terceros completamente ajenos al proceso comunicativo. Por su parte, el art. 35 LGT explicita las precauciones y garantías que han de observarse cuando en la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general. Entre las mismas y a efectos de nuestra materia, hemos de destacar el hecho de que la norma establezca expresamente que cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan no pueden ser "ni almacenados ni divulgados" y deberán ser "inmediatamente destruidos"[1039]. De esta manera, la LGT protege el secreto de las comunicaciones frente a la intromisión de terceros que —por su posición— no son completamente ajenos al proceso comunicativo sino facilitadores del mismo, respecto de cuya actividad vemos que se establece un principio y deber de

---

nuevos apartados que contienen numerosos detalles sobre el régimen de interceptación de las comunicaciones desde la perspectiva de las obligaciones que atañen a los proveedores. De acuerdo con la Exposición de Motivos , las modificaciones incluidas buscan adaptar la LGT al contenido de la LCD; sin embargo, resulta más cierto señalar que lo que lo que realmente llevan a cabo los nuevos apartado es incorporar a la LGT las previsiones sobre intervención de las comunicaciones que con anterioridad se incluían en los artículos 84.i), 86.2, 87.2 y 3, 88, 89.2 , 95 y 96 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios —en adelante, RLGT —, así como una ligera pero relevante modificación de las previsiones contenidas en el contenido original del artículo 33 LGT. Tal regulación complementa técnicamente la del art. 579 LECrim, que se ocupa de la vertiente procesal.

[1037] Cf. art. 37 LGT.

[1038] Cf. art. 36 LGT.

[1039] Cf. art. 35.1.b) LGT.

no retención de los datos, prohibición de su divulgación, y obligación de destruirlos, conforme a los que los operadores deben actuar en caso de tener que acceder al contenido de las comunicaciones por motivos de mantenimiento técnico.

El cuidado con el que el legislador español ha venido proveyendo al secreto de las comunicaciones en favor de los usuarios de las telecomunicaciones se manifiesta con mayor elocuencia en el art. 38 LGT que, sin perjuicio de todo lo dispuesto en la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, reconoce una serie de derechos de los consumidores y usuarios finales de estos servicios[1040].

De la extensa regulación contenida en este art. 38 LGT, se deduce el derecho del abonado a decidir y disponer como desee acerca del uso y destino de los datos de tráfico que generen sus comunicaciones, lo que, por una parte, no es más que una consecuencia de los derechos al secreto de las comunicaciones y a la protección de datos, y por otro, se traduce en un principio general consistente en el derecho de los abonados de los servicios de comunicaciones electrónicas a que los datos externos de sus comunicaciones no puedan ser accedidos, captados, conservados, mostrados ni tratados por parte de los operadores sin que medie su consentimiento previo e informado. Este principio encuentra su concreción, por ejemplo, en el explícito derecho de los usuarios a que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación, tal como establece el art. 38.3.a) LGT. "Los datos de tráfico —se indica a renglón seguido— necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnacion de la factura del servicio o para que el operador pueda exigir su pago". Además, el principio se concreta en el derecho a que los datos de tráfico de los abonados sean utilizados con fines comerciales o para la prestación de servicios de valor añadido "únicamente cuando hubieran prestado su consentimiento informado para ello"[1041], así como a recibir facturas no desglosadas cuando así se solicite[1042]. También

[1040] Cf. art. 38.8 LGT.

[1041] Cf. art. 38.3.b) LGT.

[1042] Cf. art. 38.3.c) LGT.

cabe subrayar el que las compañías no puedan legalmente proceder al tratamiento de los datos de localización distintos a los datos de tráfico salvo cuando se hayan hecho anónimos o previo consentimiento informado y —lo que es también relevante— "únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado"[1043].

El art. 38.3 LGT también reconoce otros derechos que, básicamente, no hacen sino reafirmar el derecho del abonado a disponer como desee —y en la medida que sea técnicamente posible— de los datos de tráfico que generan sus comunicaciones, como por ejemplo, el derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada, o de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada[1044]. Tal derecho se traduce a nuestros efectos en la potestad para el abonado de ocultar a terceros ciertos datos de tráfico.

Así pues, parece demostrado que el derecho al secreto de las comunicaciones —tal como se desarrolla en nuestro Derecho— protege los datos *internos* y *externos* de las comunicaciones y excluye por principio no sólo a terceros sino también a los propios operadores, que pueden hacer uso únicamente de aquellos datos que sean necesarios para la prestación adecuada del servicio, debiendo, en los demás casos, recabar el previo consentimiento informado del abonado.

Respecto de los datos estrictamente "de suscripción" —aquellos directamente recabados por la compañía de sus clientes, no generados por la tecnología de la comunicación— la LGT los ubica bajo la protección del derecho a la protección de datos cuando, en su art. 34, prevé la obligación para los operadores de garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal conforme a la legislación vigente —es decir, la LOPD y su desarrollo reglamentario—, adoptando las

[1043] Cf. art. 38.3.d) LGT.

[1044] Cf. art. 38.3.f) y g) LGT.

medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, "con el fin de garantizar los niveles de protección de los datos de carácter personal que sean exigidos por la normativa de desarrollo de esta ley en esta materia".

41.3 Relación de los operadores con los datos de las comunicaciones electrónicas listados en el art. 3 LCD, desde la perspectiva de los derechos fundamentales

De todo lo que acabamos de exponer en el apartado anterior se echa de ver cómo la entrada en este marco regulatorio de la LCD supuso la irrupción de una amplísima excepción a todas las previsiones que concretaban el principio general de libre disposición de los datos por parte de los abonados. Quizás no haya mejor prueba de ello que el hecho de que el legislador se viera obligado a añadir a través de la Disposición Final Primera, apartado segundo, LCD, un nuevo párrafo al art. 38.5 LGT, que ahora advierte que lo establecido en las dichas letras —a) y d) del apartado 3— se entiende "sin perjuicio de las obligaciones establecidas en la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones"[1045]. Este nuevo inciso vino además a sustituir a otro —dado por la redacción original— en virtud del cual lo dispuesto en el párrafo a) del apartado 3 se entendía sin perjuicio de lo dispuesto en el art. 12 LSSI.

Así pues, la LCD, al disponer la conservación generalizada de datos de las comunicaciones electrónicas, comporta la afectación de dos derechos fundamentales.

[1045] Para hacer más exhaustiva nuestra exposición, debemos señalar que estos poderes de disposición del abonado respecto de sus datos de tráfico conocen otras excepciones por parte del art. 38.5. Así, el apartado indica que los usuarios finales no podrán ejercer los derechos reconocidos en los párrafos d) y f) del apartado 3 cuando se trate de llamadas efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen reglamentariamente, en especial a través del número 112. Del mismo modo, y por un período de tiempo limitado, los usuarios finales no podrán ejercer el derecho reconocido en el párrafo f) del apartado 3 cuando el abonado a la línea de destino haya solicitado la identificación de las llamadas maliciosas o molestas realizadas a su línea.

Respecto de los *datos de suscripción*, los proveedores tienen el deber de conservarlos por doce meses, estableciéndose así por imperativo legal una incisiva excepción a la regulación general del derecho a la protección de datos. Estos datos, que fueron proporcionados voluntariamente por el usuario, ahora se conservarán tanto al margen de su voluntad como de lo dispuesto en la LGT.

Respecto de todos *los demás datos externos* —los generados por la tecnología comunicativa—, la acción del operador por mandato legal sobre estos datos ha dado lugar a los dos tipos de interpretaciones acerca de cuál es el derecho fundamental afectado, en los términos que expusimos anteriormente.

42 Test de constitucionalidad de la LCD

Una vez que hemos delimitado los derechos fundamentales que se ven afectados por las medidas de la LCD, estamos en condiciones idóneas para aplicar sobre éstas el test de constitucionalidad que, de acuerdo con la jurisprudencia del TC y del TEDH, nos permitirán concluir si la injerencia en los derechos operada por la LCD resulta o no legítima y admisible en nuestro sistema constitucional. Tal como anunciamos al principio de esta Parte Cuarta, el primer requisito que ha de superar el examen de constitucionalidad es el de previsión legal.

42.1 Previsión legal

El principio de legalidad constituye —como es sabido— un presupuesto común para todo acto del poder público limitativo de cualquier derecho fundamental. Por mandato expreso de la CE, toda injerencia estatal en el ámbito de los derechos fundamentales y

de las libertades públicas que incida directamente sobre su desarrollo o limite o condicione su ejercicio precisa de una habilitación legal[1046].

Concretamente, nuestro sistema constitucional exige una triple condición sobre la previsión legal de las medidas limitativas de los derechos fundamentales. En primer lugar, debe concurrir la existencia de una disposición jurídica que habilite a la autoridad judicial para la imposición de la medida en el caso concreto. En segundo lugar, dicha disposición debe gozar de un determinado rango legal. Finalmente, es preciso que, como garantía de seguridad, la ley en cuestión presente un cierto grado de lo que viene a conocerse como "calidad"[1047].

Examinaremos a continuación la manera en que la LCD cumple con estas tres condiciones.

42.1.1 Existencia de disposición jurídica

Del mismo modo que el art. 8.2 CEDH dispone que toda injerencia de la autoridad pública en la esfera privada ha de estar "prevista por la Ley", el mandato expreso de nuestra CE hace que toda injerencia en el ámbito de los derechos fundamentales y de las libertades públicas que limite o condicione su ejercicio precise una habilitación legal[1048]. No podría ser de otra manera. Los derechos fundamentales garantizan un estatus jurídico de libertad y, por tanto, sólo el legislador tiene la facultad de habilitar al poder público para que disponga de medios de investigación que restrinjan este espacio protegido[1049] —particularmente, como es el caso de la LCD, en el ámbito del proceso penal, donde se ventilan asuntos que implican una profunda injerencia en la libertad del imputado y de sus derechos fundamentales[1050]—.

[1046] Cf. art. 53 CE.

[1047] Cf. STC 169/2001, de 16 de julio.

[1048] Cf. STC 49/1999, de 5 de abril.

[1049] Cf. SSTC 25/1981, de 14 de julio, y 81/1991, de 22 de abril

[1050] Cf. STC 18/1999, de 22 de febrero. Así, por ejemplo, cabe notar que el precedente histórico más cercano a las medidas de la LCD —que para muchos autores son las intervenciones telefónicas— se

En el supuesto concreto de nuestra norma, el requisito de la previsión legal de la norma habilitante según las exigencias de la doctrina del TEDH, entendida como la previsión normativa que permita a cualquier persona conocer cuándo y bajo qué circunstancias puede verse afectado su derecho fundamental, queda claramente perfilado en dos niveles de regulación: uno primero de captación, almacenamiento y conservación sin posibilidad alguna de tratamiento, desarrollado en los arts. 1.2, 2 a 5, 8, 9, y Disposición Adicional Única —en sus aparts. 1, 3, 7 y 8— LCD; y un segundo nivel, de mayor intensidad y trascendencia en la afectación de concretos derechos de las personas afectadas, de cesión y utilización de la información así facilitada, desarrollado en los arts. 1.1 y 3, 6, 7 y Disposición Adicional Única —aparts. 2 y 4— LCD.

Es evidente que la conclusión no puede ser otra que el que la LCD cumple con este primer requisito de la mera existencia de disposición jurídica.

42.1.2 Rango legal: la reserva de ley orgánica

Mucho más cuestionable es la observancia por la LCD del segundo requisito que ha de concurrir en relación con la necesidad de previsión legal de la medida, esto es, que norma goce de un determinado rango legal.

En el caso español, el art. 81.1 CE[1051] exige que las normas relativas al desarrollo de los derechos fundamentales y de las libertades públicas tengan carácter de ley orgánica. Aplicado al objeto de nuestro estudio, el hecho de que el rango normativo de la LCD sea el de una ley ordinaria, ha dado lugar a que una mayoría de voces, tanto desde la doctrina como desde la jurisprudencia del TS, hayan sostenido la insuficiencia de este rango y, en consecuencia, la propia inconstitucionalidad de la norma.

---

regulan en nuestro ordenamiento procesal penal sólo desde 1988, cuando se aprobó el vigente art. 579 LECrim.

[1051] Dispone el precepto que: "1. Son Leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución.

2. La aprobación, modificación o derogación de las Leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto".

La necesidad de ley orgánica para regular las medidas de la LCD ya fue planteada en sus alegaciones al Anteproyecto —con apoyo en una eventual incidencia en el derecho a la intimidad— por la Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España[1052].

Más tarde, algunos autores han seguido sosteniendo que la norma debería haber adoptado la forma de ley orgánica dado que su regulación afecta al contenido de los derechos fundamentales[1053]. Así lo entienden, por ejemplo, ORTIZ NAVARRO y LUCAS MARTÍN, para quienes la LCD desarrolla de forma directa el contenido y régimen jurídico del derecho fundamental al secreto de las comunicaciones[1054]. También RODRÍGUEZ DELGADO se ha mostrado favorable a la aprobación de la norma mediante ley orgánica, pues "hubiese dado una mayor eficacia a la misma, así como una mayor protección a los usuarios, porque al fin y al cabo, los datos de tráfico, aun siendo irrelevantes en el contenido de la comunicación, son parte esencial de la misma"[1055]. O GONZÁLEZ LÓPEZ, que sostuvo tal opinión tanto antes como después de la aprobación de la LCD, y para el cual, "ya se mantenga, como hace la Ley, que los derechos fundamentales afectados incluyen el derecho al secreto de las comunicaciones o que tal vinculación no se produce, residenciándose la principal afección en el derecho a la protección de los datos de carácter personal, lo cierto es que la existencia, en todo caso, de restricción de derechos fundamentales conlleva la necesidad de que la ley reguladora revista el carácter de orgánica, como se desprende del artículo 81 CE"[1056].

Por su parte, ORTIZ PRADILLO advierte que, si bien es cierto que la LCD se remite expresamente a la LOPD en lo referido al nivel de protección de los datos conservados,

---

[1052] Cf. Dictamen 32/2007 del Consejo de Estado…, doc. cit., antecedente quinto, apart. e).

[1053] Cf. *inter alia*, González López, J. J., Los datos de tráfico de las comunicaciones…, op. cit., pp. 183 y 331; y Ortiz Pradillo, J. C., Tecnología versus proporcionalidad en la investigación penal: la nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas, La Ley Penal, n. 75, Sección Jurisprudencia aplicada a la práctica, octubre 2010, Editorial La Ley, p. 4.

[1054] Ortiz Navarro, J. F., y Lucas Martín, J., Ámbito de protección del derecho al secreto de las comunicaciones", en Práctica Penal, SepinNET Revista, 2008.

[1055] Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 7.

[1056] Dicha deficiencia fue advertida respecto del Proyecto de Ley en González López, J.J., Los datos de tráfico..., op.cit., p. 425; y en Comentarios a la Ley 25/2007…, doc. cit, p. 10.

su calidad, confidencialidad y seguridad en el tratamiento de los mismos, su art. 9 regula "excepciones" a los derechos de acceso y cancelación previstos en los arts. 15 y 16 LOPD[1057]. Esto supone que una ley ordinaria estaría estableciendo excepciones a un derecho fundamental regulado en una ley orgánica, parte del contenido esencial del art. 18.4 CE. De aquí se deduciría un claro motivo de inconstitucionalidad de la LCD.

Lo cierto es que el propio TS se ha hecho eco también de esta problemática al declarar que "no deja de llamar la atención la clamorosa insuficiencia [*sic*], desde el punto de vista de su jerarquía normativa, de una Ley [en referencia a la LCD] que, regulando aspectos intrínsecamente ligados al derecho al secreto de las comunicaciones, y a la protección de datos personales, no acata lo previsto en el art. 81.1 de la Constitución"[1058]. En su posterior Sentencia de 18 de noviembre de 2008, el TS hizo hincapié en el hecho de que la LCD carezca de carácter orgánico, considerando tal falta como "jurídicamente relevante" a la hora de interpretar tanto la LCD como la afectación de derechos fundamentales en la obtención de alguno de los datos contenidos en el art. 3 LCD por parte de la Policía Judicial[1059].

Por las razones expuestas, no cabe sino concluir que la aprobación mediante ley orgánica de la LCD habría sido más conveniente, en tanto que al menos despejaría las dudas de constitucionalidad que pesan sobre ella.

[1057] Cf. Ortiz Pradillo, Juan Carlos, Tecnología versus Proporcionalidad…, op. cit., p. 7.

[1058] Cf. STS 249/2008, de 20 de mayo.

[1059] "Se refiere únicamente a la «cesión» de los datos conservados en los correspondientes ficheros automatizados y que, en todo caso, no alude expresamente a su recogida por la Policía Judicial al margen de los mismos, ni tampoco cabe desconocer que dicha averiguación, cuando se lleva a cabo en el marco de una investigación criminal relativa a un delito de especial gravedad —como es el caso—, difícilmente puede considerarse que suponga una indebida y desproporcionada restricción de un derecho fundamental y que, por ello, suponga una vulneración constitucional con sus lógicas consecuencias (v. art. 11.1 LOPJ)".

42.1.3 La calidad de la Ley

Por otra parte, la jurisprudencia constitucional exige no sólo que la injerencia estatal en el ámbito del derecho esté presidida por el principio de legalidad; el respeto a dicho principio requiere también para tales casos que se trate de "una ley de singular precisión" [1060] . La idea subyacente es que el Derecho ha de usar términos suficientemente claros para indicar en qué circunstancias y bajo qué condiciones se habilita a los poderes públicos para autorizar una medida consistente en la interceptación de las comunicaciones. En este ámbito, cualquier ciudadano tiene derecho a poder prever las posibles consecuencias que una determinada acción puede acarrear sobre su persona. El peligro de arbitrariedad aparece con una claridad singular allí donde el poder de apreciación es ejercido en secreto. Por ello, cuando se trata por ejemplo de medidas secretas de vigilancia o de interceptación de las comunicaciones por las autoridades públicas, resulta imprescindible que las normas que las regulen sean claras y detalladas, sobre todo si consideramos el hecho de que los procedimientos técnicos no cesan de perfeccionarse.

En el marco de nuestra jurisprudencia constitucional —que recoge y desarrolla las ideas anteriores—, el TC ha manifestado que la calidad de la ley implica que se trate de una "ley de singular precisión"[1061], en el sentido que use términos suficientemente claros para indicar en qué circunstancias y bajo qué condiciones se habilita a los poderes públicos para autorizar una medida consistente —por poner el caso de la LCD— en conservar y ceder los datos de tráfico con fines penales[1062]. En aplicación de esta doctrina, el TC enumeró en la STC 49/1999 cada una de las exigencias derivadas de nuestra Constitución que deben cumplirse por la norma limitadora para considerarla acomodada a las exigencias del art. 8 CEDH en materia de previsibilidad de la ley[1063].

[1060] Cf. SSTC 49/1999, de 22 de febrero; 123/1997, de 1 de julio; 54/1996, de 26 de marzo; 49/1996, de 26 de marzo, y 85/1994, de 14 de marzo.

[1061] Ibíd.

[1062] Recuérdese que España ha sido condenada en numerosas ocasiones por el TEDH por la insuficiencia del art. 579 LECrim.

[1063] Entre ellas, se encuentra la naturaleza de las infracciones susceptibles de poder dar lugar a ella. En el caso de las interceptaciones telefónicas, la falta de previsión legal en este punto ha obligado al TC a suplir las insuficiencias legales precisando los requisitos necesarios para garantizar la legitimidad de las

En referencia a las escuchas telefónicas —materia cercana a la de la LCD—, los requisitos son los siguientes[1064]: la definición de las categorías de personas susceptibles de ser sometidas a escucha judicial; la naturaleza de las infracciones susceptibles de poder dar lugar a ella; la fijación de un límite a la duración de la ejecución de la medida; el procedimiento de trascripción de las conversaciones interceptadas; las precauciones a observar, para comunicar, intactas y completas, las grabaciones realizadas a los fines de control eventual por el Juez y por la defensa; las circunstancias en las cuales puede o debe procederse a borrar o destruir las cintas, especialmente en caso de sobreseimiento o puesta en libertad[1065].

---

injerencias lo que ha generado un gran casuismo jurisprudencial que, sin embargo, ha pasado finalmente el examen del TEDH —en la Sentencia Abdulkadir Coban— si bien considera deseable una modificación legislativa.

Así, si echamos la mirada sobre la evolución legislativa en España sobre la materia, comprobamos que la redacción originaria de la LECrim, que data de 1882, sólo contemplaba las intervenciones postales y telegráficas. Sólo a partir de la Ley Orgánica 4/1988, de 25 de mayo, la que modificó el art. 579 de nuestra LECrim, quedaron debidamente autorizados los Jueces de Instrucción para la práctica de todo tipo de intervención de las comunicaciones, incluidas las telefónicas.

Dicha Sentencia no es sino el reflejo de otra inmediatamente anterior, de 30 de julio de 1998, emitida por el TEDH en el caso Valenzuela Contreras contra España, y en la que el Tribunal elaboró una minuciosa enumeración de los requisitos que resultan imprescindibles para practicar la intervención, y que a su vez reafirmaba lo sostenido por sus sentencias Kruslin y Huvig, de 24 y 26 de abril de 1990. Así, entre las garantías mínimas que deben figurar en la Ley, la jurisprudencia del TEDH incluye las siguientes: la definición de las categorías de personas susceptibles de interceptación judicial; la naturaleza de las infracciones a que puedan dar lugar; la fijación de un límite al período de la ejecución de la medida; las condiciones del establecimiento de las transcripciones de síntesis consignando las conversaciones interceptadas; las precauciones a tomar para comunicar, intactas y completas, las grabaciones realizadas, a fin de su eventual control por el Juez y la defensa; y, finalmente, las circunstancias en las que puede o debe realizarse el borrado o la destrucción de las citadas cintas, especialmente tras un sobreseimiento o una absolución .

[1064] Cf. SSTCS 26/2006, de 30 de enero, y 184/2000, de 10 de julio, que han declarado que el art. 579 LECrim —que habilita legalmente la interceptación— adolece de vaguedad e indeterminación en aspectos esenciales.

[1065] Por su parte, la Circular de la Fiscalía General del Estado 1/1999, de 29 de diciembre, aconsejó modificar la actual regulación procesal para acomodarla a las exigencias del arto 8 CEDH y a la interpretación que del mismo viene realizando el TEDH.

Si aplicamos estos criterios a la LCD, se comprueba que la norma no cumple con algunos de ellos. Como critica ORTIZ PRADILLO[1066], nuestra Ley, para regular la cesión de los datos a los agentes facultados, se remite a una resolución judicial conforme a lo previsto en la LECrim y de acuerdo con los principios de necesidad y proporcionalidad[1067] —art. 7.2 LCD— de un modo tan vago y genérico que resulta claramente insuficiente, por su falta de detalle, con la jurisprudencia del TEDH respecto a la calidad y la claridad de aquella ley que se ocupe de regular una restricción a un derecho fundamental.

No puede dejar de señalarse que la falta de una regulación completa de la intervención de las comunicaciones electrónicas incide en la eficacia de la actuación de las Fuerzas y Cuerpos de Seguridad del Estado. Como ha sucedido a lo largo de décadas con las escuchas telefónicas —y podría fácilmente suceder en el caso de la LCD—, el hecho de que los Tribunales hayan tenido que ir colmando las lagunas legales ha generado un gran casuismo jurisprudencial que se refleja en una disparidad de criterios en aspectos trascendentales. Esta situación origina un gran desconcierto en la actuación de la Policía Judicial que, en ocasiones, ve anuladas sus investigaciones o incluso se ve incursa en responsabilidad por vulneración del derecho al secreto de las comunicaciones y por la obtención ilícita de pruebas[1068]. La legalidad del medio empleado dependerá de la interpretación del usuario, sin más orientación que el control judicial sobre la investigación. No parece razonable que la actividad investigadora de los servicios policiales fracasen por la pasividad del legislador. Por todo ello, resulta sumamente aconsejable que las imprecisiones de la LCD sean subsanadas lo más pronto posible por el legislador.

No obstante, no podemos obviar que, en la práctica, la probabilidad de que esto suceda es escasa, dado el reducido interés que la materia presenta, no sólo a nivel político, sino

---

[1066] Cf. Ortiz Pradillo, J. C., Tecnología versus Proporcionalidad…, op. cit., p. 7.

[1067] Las confusiones derivadas de la ambigua expresión del art. 7.1 —"Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el art. 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente"—, han quedado solventadas tras el Acuerdo de la Sala Penal del TS de 23 de febrero de 2010, que exige autorización judicial para que los operadores cedan los datos especificados en el art. 3 LCD.

[1068] Cf. Rodríguez Lainz, J.L., "El principio de proporcionalidad... (I)", op.cit., p. 13.

para la opinión pública de nuestro país. A la espera de que la Comisión Europea tome la iniciativa y —como ha anunciado— proceda a la revisión de la DCD en una línea más garantista[1069], lo cierto es que todo apunta que nuestra ley de transposición quedará intacta. Ante esta perspectiva, parece aconsejable formular ahora algunas consideraciones sobre las consecuencias de esta insuficiencia legislativa de la LCD.

A la luz de nuestro Derecho vigente, el mecanismo de control de constitucionalidad de las leyes que establece la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional —en adelante, LOTC— está previsto para actuar sobre las disposiciones legales que en su contenido contradigan la Constitución, pero no respecto de lo que en su enunciado no se contempla[1070]. En este caso, el planteamiento de la cuestión de inconstitucionalidad no resultaría útil en la medida en que la declaración de inconstitucionalidad acarrearía la nulidad de un precepto que, en el caso que nos ocupa, no es contrario a la Constitución por lo que dice, sino por lo que deja de decir[1071].

Por ello, cuando nos encontremos ante un precepto con un contenido constitucionalmente válido, pero insuficiente —como ocurre con el del art. 579 LECrim o con los de la LCD—, el remedio consistente en la declaración de inconstitucionalidad por defecto de la disposición legal sería contraproducente en tanto que agravaría el defecto mismo, pues dejaríamos el ordenamiento desprovisto de cualquier habilitación legal de la injerencia en las comunicaciones telefónicas o electrónicas, incrementando así la falta de certeza y de seguridad jurídicas[1072].

El TC —ni siquiera hipotéticamente a través de una sentencia interpretativa— puede colmar todos los vacíos de la ley con la necesaria precisión. Por vía interpretativa no puede resolver, en abstracto, más de lo que de manera concreta haya ido estableciendo. Precisamente por ello, resulta imprescindible la intervención del legislador para producir una regulación ajustada a las exigencias constitucionales como único remedio para la reparación de la eventual inconstitucionalidad, supliendo las insuficiencias de las que trae causa.

[1069] Cf. Informe de evaluación…, op. cit. p. 8.6 (*próximos pasos*).

[1070] Cf. STC 184/2003, de 23 de octubre.

[1071] Así ocurrió en el asunto resuelto por la STC 67/1998, de 18 de marzo.

[1072] Cf. STC 184/2003, de 23 de octubre, y las allí se refieren.

Así pues, tal como ha declarado el TC en numerosas ocasiones, no es tarea de esta institución definir positivamente cuáles sean los posibles modos de ajuste constitucional[1073]. Es al legislador a quien corresponde, en uso de la libertad de configuración normativa propia de su potestad legislativa, solucionar la situación de vacío completando debidamente un precepto legal[1074].

Buena prueba de todo ello es que, aunque exista unanimidad en la doctrina sobre la insuficiencia del art. 579 LECrim como norma habilitante de la restricción del derecho al secreto de las comunicaciones telefónicas desde perspectiva de la determinación y precisión necesarias para satisfacer la exigencia de previsibilidad del alcance de la injerencia para los eventualmente afectados por ella, no existe acuerdo, sin embargo, a la hora de concretar cuál sea el alcance que debe darse a dichas deficiencias. Resulta necesario distinguir entre los requisitos de las intervenciones que vienen impuestos directamente por la Constitución y los que derivan de la legalidad ordinaria, dado el distinto alcance que produce la infracción de cada tipo.

El Proyecto de Ley de la Ley Orgánica 6/2007, de 24 de mayo, por la que se modificaba la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional, contemplaba expresamente la inconstitucionalidad por insuficiencia legislativa, ya que uno de sus objetivos originarios consistía, precisamente, en delimitar con mayor precisión cuáles eran los efectos de las sentencias en los procesos de inconstitucionalidad[1075]. La redacción prevista para el art. 39.3 LOTC disponía que:

> "Cuando la sentencia declare la inconstitucionalidad por insuficiencia normativa podrá conceder un plazo al legislador para que actúe en consecuencia. Si éste incumpliera dicho mandato, el Tribunal Constitucional resolverá lo que proceda para subsanar la insuficiencia".

Se acogía de esta manera la doctrina del período transitorio, según la cual las medidas restrictivas de derechos fundamentales carentes de regulación legal sólo pueden adoptarse con carácter excepcional durante un período transitorio, hasta que se les dote

---

[1073] Ibíd.

[1074] Ibíd.

[1075] Publicado en el Boletín Oficial de las Cortes Generales de 25 de noviembre de 2005.

de la suficiente cobertura legal. Sin embargo, finalmente, la reforma de la LOTC no hizo referencia alguna a esta inconstitucionalidad por insuficiencia legislativa.

Por ello, hemos de remitirnos de nuevo a la doctrina del TC que, en su STC 49/1999, estableció que, si bien es cierto que la insuficiencia de la ley constituye, por sí sola, una vulneración del derecho fundamental, no lo es menos que para que dicha vulneración pueda tener efectos sobre las resoluciones judiciales impugnadas en amparo resulta preciso que la actuación de los órganos judiciales que autorizaron las intervenciones haya sido constitucionalmente ilegítima, esto es: que a dichas resoluciones sea imputable de forma directa e inmediata la vulneración del derecho fundamental[1076]. En todo caso, no puede entenderse que el Juez haya vulnerado el derecho o derechos fundamentales implicados por la sola insuficiencia de la ley[1077].

De hecho, el propio TEDH, en el caso Abdulkadir Coban contra España, de 26 de septiembre de 2006, reconoció en relación con las interceptaciones telefónicas que en el Derecho español existe ya una jurisprudencia consolidada y bien establecida al respecto. De este modo, aunque consideró deseable una modificación legislativa que incorporase los principios que se desprenden de la jurisprudencia del Tribunal —ya señalados—, entiende que el art. 579 LECrim, modificado por la Ley Orgánica 4/1988, de 25 de mayo, y completado por la jurisprudencia tanto del Tribunal Constitucional como del Tribunal Supremo, formula normas detalladas y precisa *a priori*, con suficiente claridad, el alcance y las modalidades del ejercicio del poder de apreciación de las autoridades en este concreto ámbito[1078].

[1076] Cf. art. 44.1.b) LOTC.

[1077] Cf. STC 49/1999, de 5 de abril, y, *mutatis mutandi*, STC 47/2000, de 17 de febrero. En el mismo sentido se manifiesta el TS en su sentencia de 11 de abril de 2005, según la cual la falta de contenido material del art. 579 LECrim. no es suficiente para inhabilitar la medida, siempre y cuando el órgano judicial haya respetado escrupulosamente la doctrina y los principios que la jurisprudencia ha sentado sobre esta cuestión.

[1078] En todo caso, hay que reconocer que tal postura no es admitida de forma unánime. No han faltado autores que entienden que la falta de apoyo legal —entendido como ausencia de una norma con la suficiente certeza— sigue constituyendo una vulneración del derecho afectado que debe conducir a declarar la nulidad de este tipo de diligencias.

En consecuencia, no podemos sino concluir que una reforma futura de la LCD debería subsanar todos estos aspectos constitucionalmente deficientes que acabamos de apuntar.

42.2 Reserva de decisión judicial motivada

El siguiente requisito para que la restricción de derechos fundamentales de la LCD sea compatible con nuestro orden constitucional es la reserva de decisión judicial motivada**.**

El art. 18.3 CE dispone una reserva jurisdiccional casi absoluta para limitar el derecho al secreto de las comunicaciones[1079], de tal forma que la única excepción que se contempla se circunscribe a los supuestos en que se investiguen bandas armadas o terroristas[1080]. Por tanto, en nuestro Derecho queda prohibida la restricción de este derecho por cualquier autoridad que no sea la judicial. Aunque el art. 8.2 CEDH no exige que el acto de injerencia en el derecho al secreto de las comunicaciones venga autorizado por un órgano de naturaleza judicial[1081], prevalece la reserva jurisdiccional de nuestro Derecho interno de acuerdo con la cláusula de mayor protección para los derechos fundamentales[1082]. A juicio de la doctrina, el plus de protección al que la CE sometió el derecho al secreto de las comunicaciones responde, posiblemente, a los abusos en materia de escuchas cometidos en nuestro país en los años precedentes[1083].

Vuelta la atención sobre la LCD, se comprueba cómo, ante la intensidad de la injerencia y —probablemente— ante la ya examinada dificultad de delimitar los concretos derechos fundamentales implicados, el legislador español ha cortado el nudo

---

[1079] Cf. art. 18.3 CE: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

[1080] Cf. arts. 55.3 y 25.2 CE.

[1081] El art. 8.2 CEDH se refiere a la injerencia de la autoridad pública en el ejercicio de este derecho.

[1082] De forma diferente, en el Derecho comparado se contempla la posible autorización de la injerencia por parte del Ministerio Fiscal. Sirva de ejemplo la Ley Procesal Penal alemana que posibilita, en los casos de peligro por el retraso, la intervención telefónica ordenada por el Fiscal aunque condicionada a la posterior confirmación por el Juez en el plazo de tres días (art. 100 b.1 StPO).

[1083] Cf. Gimeno Sendra, V., Las intervenciones electrónicas y la Policía judicial…, op. cit., p. 4.

gordiano al trasponer la DCD al ordenamiento español exigiendo autorización judicial para la cesión de todos los datos cualquiera que sea su naturaleza. Tal opción se opone a lo que quizás resultaría más complejo pero jurídicamente más correcto: la delimitación del régimen jurídico de la conservación y cesión en función de la categoría de datos de que se trate y del tipo de delito que se esté investigando.

Así las cosas, la reserva de resolución judicial en el acceso y cesión de la información contenida en los ficheros de datos relativos a las comunicaciones electrónicas se muestra como algo incuestionable en la LCD, tal como se deduce de los categóricos términos en que se ha redactado el art. 1.1 LCD —"siempre que les sean requeridos a través de la correspondiente autorización judicial", con carácter de simple enunciado— y en el art. 7.1 y 2 LCD, con mayor detalle:

> "1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.
>
> 2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados".

De un cuidadoso examen de estos preceptos se concluye que corresponde al Juez decidir *en toda ocasión* sobre el hecho de la cesión y el contenido de lo que ha de cederse, siempre en función de los principios de necesidad y proporcionalidad y de modo semejante a como se exige para la intervención de las comunicaciones telefónicas. Sólo cuando se observen todas estas condiciones la utilización de estos datos podrá tener la debida eficacia probatoria en el proceso penal.

El hecho de que corresponda siempre al Juez la decisión de la cesión y su extensión hace que la aplicación de la LCD suscite algunas dudas sobre el régimen que debe informar la obtención por la Policía Judicial de algunos datos listados en el art. 3 LCD. En concreto, resulta dudosa la necesidad de someter a autorización judicial la obtención

de las claves IMSI[1084] e IMEI[1085] y de los protocolos de acceso a internet, que pueden ser obtenidos directa y fácilmente por la Policía. No obstante, es claro que en el supuesto de las comunicaciones electrónicas realizadas en canal abierto, cuyos datos son accesibles públicamente, y que, por tanto, quedan fuera del ámbito del art. 18.3 CE, la aprehensión de los mismos puede hacerse por la Policía sin necesidad de una resolución judicial expresa. Sea suficiente recordar al respecto que el art. 11.h) de la Ley Orgánica 2/1986, de Cuerpos y Fuerzas de Seguridad, les encomienda captar, recibir y analizar cuantos datos tengan interés para la seguridad pública, así como estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia. Para llevar a cabo estas funciones pueden utilizarse tanto las técnicas de información habituales —los confidentes o los agentes infiltrados— como el rastreo por internet de todos aquellos datos que son absolutamente accesibles al público a través de la red.

En todo caso, retomando lo dicho, el punto de partida y el principio general del art. 18.3 CE es la plena jurisdiccionalidad de la medida. El Juez es la única autoridad a la que está constitucionalmente conferida la facultad y la responsabilidad para determinar la oportunidad de la medida y el mejor modo de tutelar los derechos de quien la sufre[1086]. Esta doctrina legal ha tenido su sanción por parte del legislador a través de la promulgación, no sólo de la LCD, sino también de la Ley Orgánica 2/2002, de 6 de mayo, relativa al Control Judicial Previo del Centro Nacional de Inteligencia —complementaria de la Ley 11/2002, de 7 de mayo—, que con objeto de posibilitar y asegurar la jurisdiccionalidad de la intervención de las comunicaciones realizadas a instancias del CNI, reserva la misma a un Magistrado de la Sala de lo Penal del TS.

[1084] IMSI es el acrónimo de International Mobile Subscriber Identity (Identidad Internacional del Abonado a un Móvil). Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

[1085] El IMEI (del inglés International Mobile Equipment Identity, Identidad Internacional de Equipo Móvil) es un código pre-grabado en los teléfonos móviles GSM. Este código identifica al aparato unívocamente a nivel mundial, y es transmitido por el aparato a la red al conectarse a ésta. Esto quiere decir, entre otras cosas, que la operadora que usemos no sólo conoce, quién y desde dónde hace la llamada (SIM) si no también desde qué terminal telefónico la hizo. El IMEI de un aparato habitualmente está impreso en la parte posterior del equipo, bajo la batería.

[1086] Cf. ATS 811/2009, de 2 de abril.

Las mismas garantías legales y jurisprudenciales fijadas en relación con las intervenciones y observaciones postales y telefónicas rigen en materia de intervención y observación de comunicaciones mantenidas por vía de correo electrónico, tanto en sus requisitos o régimen de autorización y control judicial, como en los de adveración y correcta introducción en el procedimiento para su definitiva validez como prueba[1087]. La resolución judicial ha de ser previa y no meramente confirmatoria o revocatoria de otra anterior no jurisdiccional, lo que garantiza que sólo un órgano independiente pueda acordar el acto de injerencia[1088].

En cuanto a la necesidad de *motivación*, ésta se deduce tanto de la consolidada doctrina en materia de interceptación de comunicaciones como de los mismos preceptos de la LCD antes citados —que la reflejan claramente— y en los que se aprecia la necesaria valoración del Juez de determinados principios y finalidades que necesariamente habrían de quedar reflejadas en la resolución habilitante.

En cuanto al *tipo o forma que debe adoptar la decisión*, la necesidad de motivación hace preciso el empleo —en principio— de la fórmula de Auto, en la medida en que este tipo de resolución expresa por sí misma todos los elementos necesarios para considerar fundamentada la medida limitativa del derecho. El TC ha señalado que la exigencia de resolución judicial a efectos de limitar un derecho fundamental posee carácter material, pues han de ser los Jueces y Tribunales los que autoricen el levantamiento del secreto de las comunicaciones y controlen su ejecución. De este modo, se concluiría que una Providencia no es, por su estructura, contenido y función, la forma idónea para autorizar la limitación de un derecho fundamental. La falta de un Auto motivado, en el que no se haya hecho una mínima ponderación de los derechos fundamentales en juego, así como de la idoneidad, necesidad y proporcionalidad de la medida, o que tampoco establezca el correlativo régimen de garantías para su obtención

[1087] Cf. SAN de 30 de abril de 2009.

[1088] Cf. Asencio Mellado, J. M., Prueba prohibida y prueba preconstituida…, op. cit., p. 106.

y adecuada incorporación al procedimiento de su resultado, determinará la nulidad de la prueba practicada[1089].

Ello no obstante, no podemos dejar de mencionar la existencia de una cierta jurisprudencia tanto del TC como del TS algo permisiva con la fórmula de la simple Providencia en ciertos supuestos[1090]. Se ha admitido que una resolución judicial de este tipo pueda considerarse motivada si, integrada con la solicitud de la autoridad a la que se remite —la Policía—, contiene todos los elementos necesarios para entender satisfechas las exigencias para poder llevar a cabo con posterioridad la ponderación de la proporcionalidad de la restricción de los derechos fundamentales que la proporcionalidad de la medida exige[1091]. Desde esta perspectiva, puede considerarse que también una providencia —aun no siendo el medio idóneo— cumpliría las exigencias constitucionales.

42.3 Proporcionalidad

Resulta claro que la limitación de los derechos fundamentales afectados por la LCD —a saber, los relativos al secreto de las comunicaciones y la protección de datos— sólo puede fundarse en la concurrencia de otros bienes jurídicos constitucionalmente protegidos que, por su importancia, justifiquen el sacrificio de los mencionados derechos fundamentales, y en la medida en que aquella resulte proporcionada y necesaria[1092].

[1089] Así lo ha entendido la Sentencia de la Audiencia Nacional de 30 de abril de 2009, donde el Juez Instructor, en lugar de dictar un Auto autorizando la intervención de ciertos correos electrónicos, emitió simples providencias solicitando la información necesaria a la operadora.

[1090] Baste para ello con recordar la trascendental STC 123/2002, de 20 de mayo, y las SSTS 1168/1995, de 23 de noviembre, 1231/2003, de 25 de septiembre, 1243/2003, de 3 de octubre, 249/2004, de 26 de febrero, y 1219/2004, de 10 de diciembre.

[1091] Cf. SSTC 166/1999, de 27 de septiembre, y 299/2000, de 11 de diciembre.

[1092] En concreto, el art. 8.2 CEDH funda las restricciones de derechos fundamentales en la necesidad de proteger la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden, la prevención del delito, la protección de la salud o de la moral, así como la protección de los

Ya adelantamos que, de acuerdo con la asentada jurisprudencia del TC —que sigue a su vez la del TEDH—, la observancia del principio de proporcionalidad se concreta en tres condiciones: "si tal medida es susceptible de conseguir el objetivo propuesto —*juicio de idoneidad*—; si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia —*juicio de necesidad*—; y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto —*juicio de proporcionalidad en sentido estricto*—"[1093].

Las tres condiciones del principio de proporcionalidad a cumplir por la medida deben inspirar y ser ponderadas tanto por la actuación del legislador —al elaborar y aprobar la norma, previendo la posible limitación de derechos fundamentales en abstracto— como por el Juez a la hora de aplicarla en el caso concreto.

---

derechos y las libertades de los demás. En análogo sentido se manifiesta la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que se refiere, entre otros, a los fines de la prevención, investigación, descubrimiento y persecución de los delitos.

[1093] Cf., entre otras muchas, STC 89/2006, de 27 de marzo, FJ 3. No basta además que la injerencia, en cuanto a medida limitativa de un derecho fundamental, esté prevista en una ley de singular precisión y que exista autorización judicial. Además, lo que es igual o más importante, la medida debe justificarse objetivamente para obtener el cumplimiento de los fines constitucionales que la legitiman. El principio de proporcionalidad debe inspirar tanto la actuación del Juez en el caso concreto como la actuación del legislador al prever la posible limitación en abstracto. Desde un punto de vista sustantivo, la limitación del derecho fundamental al secreto de las comunicaciones y a la protección de datos exige que el objeto de la instrucción esté integrado por un hecho punible grave para cuya investigación y esclarecimiento se considere necesaria la medida. Nuestra vigente LECrim no establece un criterio legal expreso que determine los delitos que autorizan la práctica de este acto instructorio, ni cuantitativo, en función de la pena, ni cualitativo. En materia de interceptación de las comunicaciones, nuestro TC se funda en la especial gravedad de los hechos punibles, si bien dicha gravedad no puede estar determinada únicamente por la calificación de la pena legalmente prevista, esto es, por el criterio penológico.

42.3.1 Proporcionalidad de la autorización judicial

La proporcionalidad de las medidas habilitadas por la LCD ha de ponderarse en el momento en que el Juez autoriza la intervención, con base en los datos disponibles en ese momento y no *ex post* a la vista del resultado obtenido[1094]. La LCD no ha sido ajena a esta circunstancia, y así, para la cesión por autorización judicial de los datos conservados, la observancia de los *principios de idoneidad y necesidad* en la misma están previstos por la propia norma, si bien se entremezclan —como ya es habitual en nuestro legislador— en la voz *necesidad* recogida en el art. 7.2 LCD; necesidad que viene directamente asociada a la idea de utilización de la información que realmente sea estrictamente precisa para el buen fin de la investigación criminal o de inteligencia. Tal principio de necesidad, tan escuetamente enunciado en la norma, presupone que la cesión de los datos permitirá previsiblemente obtener la información que se pretende recabar —*juicio de idoneidad*—, pero que para ello habrán de accederse sólo aquellos datos que sean estrictamente destinados a tal finalidad, huyendo por tanto de requerimientos indiscriminados[1095] o excesivos[1096].

El juicio de necesidad implica que las medidas contenidas en la LCD resulten *imprescindibles* o *necesarias*, esto es, *que no existan otras medidas menos gravosas* que, sin imponer sacrificio alguno de derechos fundamentales o con un sacrificio menor, sean igualmente aptas para dicho fin[1097].

Por su parte, el *juicio de proporcionalidad en sentido estricto* viene encuadrado, no solamente por razón de su cita en el art. 7.2 LCD, sino también por la determinación de los fines públicos concretos que habrán de prevalecer sobre los derechos individuales

---

[1094] Cf. STC 126/2000, de 16 de mayo.

[1095] Habría sido conveniente una redefinición íntegra del precepto que especificara las categorías de infracciones criminales susceptibles de permitir el acceso a los datos, estableciendo niveles de acceso en función a la gravedad del delito y las necesidades concretas de la investigación.

[1096] Si se pretende saber si el investigado, presunto autor de llamadas maliciosas, realizó concretas llamadas a la víctima en determinada franja horaria, resultaría claramente excesivo recabar el historial de todo el tráfico de llamadas emitidas en un determinado día, y a su vez localización del lugar desde el que se hicieron.

[1097] Cf. SSTC 234/1997, de 18 de diciembre, FJ 9; 70/2002, de 3 de abril, FJ 10; y 25/2005, de 14 de febrero, FJ 6.

concernidos, que en el enjuiciamiento criminal serían la detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en leyes penales especiales, y en la actuación del Centro Nacional de Inteligencia las exigencias de las investigaciones de seguridad sobre personas y entidades de acuerdo con su legislación específica — art. 6.2 c)—. La incidencia del presupuesto habilitante, la constatación de concretos hechos que sirven de base para determinar la superación del juicio de proporcionalidad, debe deducirse de forma implícita de la remisión en bloque que se hace en el art. 7.2 LCD a la LECrim. y como presupuesto lógico de la motivación de cualquier resolución restrictiva de derechos fundamentales.

Superada la primera cuestión acerca de qué delitos deben ser considerados graves y, en consecuencia, su detección, investigación y enjuiciamiento permite el acceso a los ficheros de datos relativos a las comunicaciones, surge un segundo momento de evidente implicación del principio de proporcionalidad, cual sería el de la selección de aquellos datos que se consideran precisos para el buen fin de la investigación. A mayor volumen o detalle de la cesión de datos, más se verán afectados en concreto los derechos a la protección de datos de carácter personal e intimidad de la persona concernida. La mayor gravedad del hecho investigado permitirá un acceso más profundo en los entresijos de tales datos almacenados; acceso que además se verá mediatizado por los parámetros que definen el principio de necesidad de la medida, en concreto por los principios de la excepcionalidad en su exigencia y utilidad en cuanto a los datos que se reclaman. Por ello, en aquellos supuestos en los que se haga uso del principio de la menor intensidad de la injerencia, la autoridad judicial deberá cuidar de exigir la cesión de aquellos datos que sean absolutamente indispensables para el fin perseguido, renunciando a recabar aquellos que pudieran considerarse accesorios de la finalidad concreta que se persiga. Por poner un ejemplo, si lo que se pretende es determinar la identidad oculta de persona que realiza una concreta llamada amenazante constitutiva de delito, recabar el listado de llamadas de todo el día y su concreta localización geográfica, sería sin duda contrario al principio de proporcionalidad; si lo es para fijar los movimientos de un narcotraficante antes de constatarse un operativo de entrega de drogas, y a la vez localizar a los posibles destinatarios de la entrega, la medida sin duda respetará los cánones de proporcionalidad.

42.3.2 Juicios de idoneidad y necesidad en la LCD

Como ya hemos afirmado en innumerables ocasiones, no basta que la medida esté prevista en la ley y sea adoptada por un Juez, sino que resulta imprescindible que objetivamente se justifique para obtener el cumplimiento de los fines constitucionales que la legitiman, debiéndose adoptar, en cualquier otro caso, la alternativa menos gravosa para el derecho fundamental[1098]. La regulación de la LCD de estar sometida al más estricto cumplimiento de los principios de idoneidad, necesidad y proporcionalidad *stricto sensu*. Entre los requisitos que debe cumplir la norma en aplicación del principio de proporcionalidad se cuentan la idoneidad y la necesidad de la medida, lo que implica, de un lado, que sea apta para conseguir el fin perseguido —la investigación del hecho punible y la determinación de su autor—; y, de otro, imprescindible para alcanzarlo, sin que puedan determinarse tales extremos a través de otro mecanismo[1099].

Al respecto, hemos de señalar que frente a la conservación de datos establecidos por la DCD y la LCD, existen, en efecto, otros procedimientos menos invasores, como los de preservación de datos, siendo el más conocido entre ellos el procedimiento de "quick freeze" o congelación rápida: mediante este mecanismo, ni los proveedores de comunicación ni los prestadores de servicios de internet están obligados a almacenar datos relativos al tráfico[1100]. Por ejemplo, en casos justificados, los operadores notificados con una orden judicial están obligados a conservar los datos relativos únicamente a determinados individuos sospechosos de actividad delictiva a partir de la fecha de la orden de preservación. La preservación de datos es uno de los instrumentos de investigación previstos y utilizados por los Estados participantes en el Convenio del Consejo de Europa sobre ciberdelincuencia[1101]. Sin embargo, al parecer, no todas las

---

[1098] Cf. art. 8.2 CEDH.

[1099] Cf. STC 202/2001, de 15 de octubre.

[1100] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 9.

[1101] Cf. art. 16 del Convenio sobre la Ciberdelincuencia —Conservación inmediata de datos informáticos almacenados—: "1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.

partes del Convenio han previsto la preservación de datos, y todavía no se ha realizado una evaluación sobre la eficacia del modelo en la lucha contra la ciberdelincuencia. Recientemente se ha desarrollado un tipo de preservación de datos, denominado "congelación rápida plus". Este modelo va más allá de la preservación de datos, en el sentido de que un juez puede también conceder acceso a datos de tráfico que aún no hayan sido suprimidos por los operadores. Además, se establecería una exención muy limitada por ley de la obligación de suprimir, por un breve período de tiempo, determinados datos de comunicación que no se almacenan normalmente, como datos de localización, datos de conexión a internet y direcciones IP dinámicas de usuarios que tienen una suscripción de tarifa plana, y cuando no es preciso almacenar tales datos a efectos de facturación.

Quienes abogan por la preservación de datos consideran que atenta menos a la intimidad que la conservación de datos. Sin embargo, la mayoría de los Estados miembros no están de acuerdo con que alguna de las variaciones de preservación de datos pueda sustituir adecuadamente a la conservación, alegando que mientras que la conservación tiene como resultado la disponibilidad de datos históricos, la preservación no garantiza la capacidad para establecer pistas de pruebas antes de la orden de preservación, no permite realizar investigaciones si el objetivo es desconocido y no

---

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos – que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente – durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15".

permite obtener pruebas sobre los movimientos de, por ejemplo, las víctimas o testigos de un delito[1102].

Finalmente, como adelantamos, se exige que la injerencia, tal como queda delineada por la LCD, sea ponderada o equilibrada, por derivarse de ella más ventajas o beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto, lo que constituye el juicio de proporcionalidad en sentido estricto[1103]. Para valorar la observancia de este principio por el legislador, debemos ponderar con detenimiento y de manera individualizada los aspectos centrales de la LCD, a saber: el deber de conservación generalizada de datos de las comunicaciones electrónicas, su finalidad —la represión de delitos graves y, concretamente, lo que ha de enterderse por tales—, y por último, los plazos establecidos para la conservación de los datos. Sólo así podremos concluir si nos hallamos o no ante una ley constitucionalmente admisible.

A esta última ponderación dedicaremos las siguientes páginas.

42.3.3 Proporcionalidad en el deber de conservación generalizada de datos

Como ya advertimos, la creación *ex lege* de un deber general de conservación de datos constituye la cuestión central de la LCD en lo que a la proporcionalidad de la injerencia en los derechos fundamentales se refiere. La Ley —en aplicación de la DCD— establece un mandato legal dirigido a los proveedores en virtud del cual se erige un deber de retención de forma generalizada, con independencia del supuesto de hecho concreto que en el futuro pueda fundamentar la obligación de cesión de dichos datos a instancia de la autoridad judicial.

[1102] Este hecho también fue reconocido por el Tribunal Constitucional alemán en su sentencia por la que se anula la legislación alemana que transpone la Directiva. Cf. *Bundesverfassungsgericht*, 1 BvR 256/08, de 2 de marzo de 2010, p. 208.

[1103] Cf. STC 198/2003, de 10 de noviembre.

El deber de retención persigue así conservar unos datos que eventualmente pueden ser útiles en la investigación de una concreta infracción penal de carácter grave. En consecuencia, se trata de conservar de forma generalizada sin individualizar ni los sujetos ni las comunicaciones concretas que pueden verse afectadas por la medida. El deber de conservación se funda en un mandato legal dirigido a todos los proveedores, con independencia del supuesto de hecho concreto que en el futuro pueda justificar la obligación de cesión de dichos datos a instancia de la autoridad judicial. Tal deber persigue conservar unos datos que eventualmente pueden ser útiles en la investigación de una infracción penal, sin individualizar ni los sujetos ni las comunicaciones concretas que pueden verse afectadas por la medida. En palabras de PÉREZ GIL, en duros términos: "la extensión de las medidas preventivas facilitadas por esta técnica determina que todos nos hayamos transformado en sospechosos"[1104].

Expuesto de una manera más técnica, esta línea de argumentación viene a criticar que el deber de conservación generalizada de datos no cumpla con el principio de intervención indiciaria que nuestro sistema constitucional exige a las medidas restrictivas de los derechos fundamentales orientadas a la prevención o persecución de los delitos[1105]. Esto es, estamos ante una medida que se apoya en el riesgo —completamente genérico— de que cualquier ciudadano pueda cometer delitos graves para cuyo esclarecimiento y castigo puedan resultar útiles los datos de tráfico de sus

[1104] Cf. Pérez Gil, J., Investigación penal y nuevas tecnologías: algunos retos pendientes, en Revista Jurídica de Castilla y León, n. 7, oct. 2005, p. 219. Para GÓNZALEZ LÓPEZ, este tipo de medidas de conservación generalizada de datos resultan inconstitucionales "la armonización comunitaria y actual transposición no suponen sino una plasmación normativa de un instrumento esencialmente ineficaz, claramente irreconciliable con las exigencias propias de los derechos fundamentales en el marco de la prevención y represión delitos e implantado sobre la base de un debate mínimo y sesgado, amparado en un clima generalizado de miedo e inseguridad". Cf. González López, J. J., Comentarios a la Ley…, op. cit., op. cit. p. 28.

[1105] Cf. Martín Morales, R., El principio constitucional de intervención indiciaria: test de alcoholemia, videovigilancia, cacheos, redadas y controles policiales, hallazgos casuales, intervenciones domiciliarias, telefónicas, penitenciarias, aduaneras y otras, Grupo Editorial Universitario, Granada, 2000. Sobre este principio, por el mismo autor, El principio constitucional de intervención indiciaria, en *Revista de la Facultad de Derecho de la Universidad de Granada*, n. 2, 1999.

comunicaciones, lo que hace que se determine *ex lege* la conservación masiva de los mismos.

Frente a esta crítica, podría argumentarse que en nuestro sistema existen ya supuestos de intervención inindiciaria, tales como los registros en los aeropuertos o las videocámaras de seguridad de los bancos. Sin embargo, como bien observa LÓPEZ-BARAJAS, en tales supuestos concurren circunstancias especiales de potencial peligro que concurren en esos lugares y que justifican la intervención o el control[1106]. Así, el presupuesto básico para autorizar el uso de videocámaras en espacios públicos consiste en que exista un riesgo razonable para el mantenimiento de la seguridad pública en una situación compleja. Frente a estas medidas, el uso habitual de las redes de comunicaciones no es en sí mismo un peligro y, por añadidura, no se trata de una situación concreta, sino de un aspecto intrínsecamente ligado a la vida cotidiana de todos los ciudadanos.

Para algunos autores[1107], este riesgo es tan genérico que no justifica la legitimidad del deber de conservación generalizada impuesto por el legislador. Otros en cambio, como GUERREIRO PICÓ o RUIZ MIGUEL han justificado el deber de conservación generalizada de los datos vinculados a las comunicaciones electrónicas al entender que existen otros supuestos de intervención indiciaria constitucionalmente admitidos[1108]. Pero no se puede olvidar que también en estos casos, como por ejemplo los registros en los aeropuertos o las videocámaras en los bancos, la falta de indicios concretos se compensa por las especiales circunstancias que concurren en el lugar que hacen razonable la intervención o control.

En respuesta a este argumento, el otro gran experto en la materia, GONZÁLEZ LÓPEZ, replica que la finalidad perseguida por la Ley en presencia tiene una finalidad

---

[1106] Cf. López-Barajas, I. La intervención de las comunicaciones electrónicas, La Ley, Madrid, 2011, p. 197.

[1107] Cf. López-Barajas, I. La intervención…, op. cit., p. 217.

[1108] Cf. Guerrero Picó, M. C., El impacto de internet en el derecho fundamental a la protección de datos de carácter personal, Thomson-Civitas, Navarra, 2006, pp. 464 y 465; o también Ruiz Miguel, C., El derecho a la protección de los datos personales en la Carta de los Derechos Fundamentales de la Unión Europea: análisis crítico, en Revista de Derecho Comunitario Europeo, n. 14, enero-abril, 2003, p. 41.

preventiva de delitos en la medida que la conservación de los datos no esta destinada a la investigación criminal de modo directo sino indirecto, ya que se lleva a cabo antes de la comisión del hecho delictivo e incluso antes de la sospecha de que pueda cometerse en un período determinado[1109]. Por tanto, no se puede hablar de una finalidad procesal inmediata en cuanto se lleva a cabo al margen de actuaciones derivadas de una *notitia criminis*.

Todo ello sitúa el deber de conservación en el ámbito de las *medidas prospectivas* —o de prevención desligadas de la realización de un hecho delictivo— cuya legitimidad, como es bien sabido, ha sido excluida por el TC[1110]. Para que una intervención de este tipo sea válida en nuestro sistema, hemos de hallarnos en todo caso ante una medida *post delictum*, dictada una vez que ha llegado al Juez la *notitia criminis* y, normalmente tras haber recaído el auto de incoación del sumario[1111]. Así, verbigracia, no cabe decretar una intervención telefónica para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos, toda vez que el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan en la mente de los encargados de la investigación penal, por muy legítima que sea esta aspiración, pues de otro modo se desvanecería la garantía constitucional[1112]. A este respecto, nada mejor que citar la opinión del Tribunal Constitucional Federal Alemán, que en su Sentencia de 2 de marzo de 2010 afirmó que el deber de conservación de datos aumenta el peligro de que los ciudadanos se vean expuestos a posteriores investigaciones desvinculadas de la realización de hechos delictivos. La conservación de los datos asociados al tráfico de

---

[1109] Cf. González López, J.J, La retención de datos de tráfico de las comunicaciones en la Unión Europea: una aproximación crítica, Diario La Ley, num. 6456, 5 de abril de 2006.

[1110] Cf. STC 171/1999, de 27 de septiembre.

[1111] Cf. Jiménez Campo, J., La garantía constitucional del derecho al secreto de las comunicaciones…, op. cit., p. 70. En relación con esto, hay que recordar que, no cabe decretar una intervención telefónica para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos, toda vez que el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan en la mente de los encargados de la investigación penal, por muy legítima que sea esta aspiración, pues de otro modo se desvanecería la garantía constitucional .

[1112] Cf. STC 49/1999, de 5 de abril.

telecomunicaciones puede crear una sensación de amenaza, es decir, de estar siendo vigilado, que afecta al libre ejercicio de varios derechos fundamentales[1113].

Además, la obligación de conservación tiene una finalidad *preventiva*, ya que la conservación de los datos no está destinada a la investigación criminal de modo directo, sino indirecto; se lleva a cabo antes de la comisión del hecho delictivo e incluso antes de la sospecha de que pueda cometerse en un período determinado. Por tanto, no se puede hablar siquiera de una finalidad procesal inmediata, en cuanto se ejecuta al margen de actuaciones derivadas de una *notitia criminis*.

42.3.4 Concepto de delito grave en la LCD

Como vimos en un capítulo anterior, la interpretación literal del art. 1.1 LCD, en lo que se refiere a la correcta delimitación de la noción que de "delito grave" maneja la LCD, conduce a resultados y conclusiones notablemente insatisfactorias. Por las razones que allí se expusieron, tal criterio interpretativo debe ser rechazado tanto por su insuficiencia como por su inadecuación a los fines perseguidos por la propia LCD.

La cuestión de fondo —y un grave defecto de la presente norma— radica en el hecho de que nuestro legislador, cediendo bien al afán de armonización de la Directiva, bien a la mera desidia, se ha apartado completamente del régimen legal y constitucional conforme al cual se regulan en España las injerencias en los derechos fundamentales en el proceso penal, como veremos seguidamente. Retomamos por tanto a partir de este punto nuestra argumentación, pero enlazándolo con lo que ya llevamos dicho sobre el análisis constitucional de la norma.

Ya hemos explicado cómo nuestro sistema constitucional exige para toda injerencia en el ámbito de los derechos fundamentales una habilitación legal [1114] entre cuyas condiciones debe concurrir la calidad de la Ley, esto es, que la norma sea accesible y previsible, o como ha manifestado nuestro TC, que sea una "ley de singular

[1113] Cf. Ortiz Pradillo, Juan Carlos, Tecnología versus Proporcionalidad…, op. cit., p. 10.

[1114] Cf. STC 49/1999, de 5 de abril.

precisión"[1115], lo que comporta el uso de términos suficientemente claros para indicar en qué circunstancias y —sobre todo, en lo que aquí interesa— bajo qué condiciones se habilita a los poderes públicos para autorizar con fines penales una medida como la prevista en la LCD, consistente en conservar y ceder los datos externos de las comunicaciones electrónicas[1116]. Entre estas condiciones se encuentra el deber para el legislador de delimitar expresamente las infracciones susceptibles de dar lugar a la medida limitadora, tal como se deriva de las exigencias del art. 8 CEDH en materia de previsibilidad de la ley y la jurisprudencia del TEDH y de nuestro TC al respecto[1117].

Es sabido que esta concreta exigencia difiere de lo que durante décadas ha venido siendo una indeseable pauta de nuestro Derecho. Como ha puesto de relieve ORTIZ PRADILLO, el legislador español, en materia de interceptación de las comunicaciones, ha huido tradicionalmente de "concreciones y catálogos delictivos"[1118], remitiéndose de "un modo genérico, excesivamente raquítico, a la alusión a los principios de necesidad y proporcionalidad"[1119]. De esta manera, nuestra vigente LECrim no establece un criterio legal expreso que determine los delitos que autorizan la práctica de la interceptación; ni cuantitativo —en función de la pena—, ni cualitativo —en función de los tipos penales—. La necesaria pero fallida intervención del legislador ha obligado al TC a suplir las insuficiencias legales precisando los requisitos necesarios para garantizar la legitimidad de las injerencias.

Así, a la hora de delimitar los delitos cuya investigación legitima un acto de injerencia en el derecho al secreto de las comunicaciones, nuestro TC funda la limitación en que el objeto de la instrucción esté integrado por un hecho punible grave, para cuya

---

[1115] Cf. SSTC 49/1999, de 22 de febrero; 123/1997, de 1 de julio; 54/1996, de 26 de marzo; 49/1996, de 26 de marzo, y 85/1994, de 14 de marzo.

[1116] España ha sido condenada en numerosas ocasiones por el TEDH por la insuficiencia del art. 579 LECrim.

[1117] Cf. entre otras, la STC 49/1999, de 5 de abril.

[1118] "…y la actual normativa y jurisprudencia referidas a la intervención de las comunicaciones telefónicas es el mejor ejemplo de ello". Cf. Ortiz Pradillo, Juan Carlos, Tecnología versus Proporcionalidad…, op. cit., p. 8.

[1119] Ibíd.

investigación y esclarecimiento se considere necesaria la medida[1120]. Sin embargo, dicha gravedad no está determinada únicamente por la calificación de la pena legalmente prevista, esto es, por el puro criterio penológico. De hecho, en España nunca ha existido un concepto unívoco de lo que debe entenderse por delito grave a los efectos de acordar medidas de investigación limitativas de los derechos fundamentales. Delito grave según el Código Penal y admisibilidad de ciertos medios de investigación son nociones estrechamente relacionadas pero que no se identifican. De este modo, el concepto del delito grave empleado por el legislador en la LCD ha de ser interpretado dentro de este marco de la jurisprudencia del TC y del TS, que acepta el criterio penológico pero también admite y requiere un ponderado análisis y justificación en aquellos supuestos en que el tipo penal no respondiera a tal cualificación formal de "delito grave". De esta manera se ha equiparado desde hace años la figura del delito grave según la definición del Código Penal con otros criterios más amplios que el literal, como la posibilidad de que existan fines superiores capaces de superar, en términos de proporcionalidad de la medida, el sacrificio impuesto a la persona sometida al concreto acto de injerencia, como serían las ya clásicas relevancia social del hecho o del bien jurídico protegido, y —desde la STC 104/2006, de 3 de abril— la idoneidad de determinadas medidas de investigación basadas en las nuevas tecnologías para investigar aquellos delitos perpetrados a través o con ayuda de las telecomunicaciones.

Como es natural, el TC ha encontrado la interpretación literal perfectamente apta por sí misma para fundamentar la existencia de un hecho lo suficientemente grave como para justificar, junto con los demás elementos integrantes del juicio de proporcionalidad, la autorización de una intervención de las comunicaciones. Es claro en nuestra jurisprudencia que un delito penado con privación de libertad superior a cinco años goza de sobradas razones para justificar las correspondientes injerencias en ciertos derechos fundamentales con fines de su averiguación y castigo. Así, de acuerdo con lo afirmado en la STC 82/2002, de 22 de abril, la sola "calificación de un delito como grave en los casos en los que la pena con la que se castiga el delito sea calificada de tal por el Código Penal" exime de atender a criterio suplementario diverso al de la propia pena. En este sentido, y aplicado al objeto de nuestro estudio, la interpretación literal

[1120] Cf. SSTC 104/2006, de 3 de abril; 82/2002, de 22 de abril, y 299/2000, de 11 de diciembre.

del art. 1.1 LCD es hasta este punto correcta, pero no cubriría todos los supuestos de legítimo uso de las medidas de la LCD.

Ya hemos adelantado que al criterio de la gravedad formal del delito —lo definido por el Código— se han añadido dos criterios más, que no hacen sino ampliar la noción de delito grave a otros factores, como son el bien jurídico protegido y la relevancia social de los hechos[1121]. En cierto modo, ambas modalidades representan no tanto fines diversos al de prevención y persecución de los delitos —considerados graves por el legislador—, como criterios diferentes para definir la gravedad del delito en términos de ponderación del conflicto de intereses. El TC ha abierto así las puertas para extender el concepto jurídico estricto de gravedad más allá de la decisión del legislador, llevado por criterios retributivos —la pena se define, por regla general, en consideración a la relevancia social y la gravedad del hecho tipificado como infracción criminal— o de prevención general, acudiendo para ello a la fuente del bien jurídico protegido, de la finalidad de protección de bienes jurídicos concretos, conforme a los principios ponderativos a que responde la tipificación de la infracción criminal, más allá de la graduación de sus consecuencias jurídicas frente al infractor, o de la necesidad más o menos imperiosa de salir al paso en la persecución de infracciones criminales que hayan producido una mayor indignación en el sentir común de la sociedad o afectado a un importante número de personas o a un grupo reducido en forma infamante, intolerable según el sentir social.

La línea expansiva del TC ha encontrado así un nuevo campo de superación del concepto estricto de delito grave, como por ejemplo en su STC 104/2006, de 3 de abril. La Sentencia analiza el supuesto de un fraude de terminales de telecomunicaciones —en concreto, facilitación de descodificadores no autorizados de canales de televisión por satélite—, y la posibilidad de realizar una investigación que había de incluir una intervención de comunicaciones. Pese a la escasa gravedad de la pena que podría corresponder al delito, la trascendencia esencialmente patrimonial del bien jurídico protegido y la escasa relevancia social del hecho, el Alto Tribunal llega a definir un cuarto criterio de determinación del fin público susceptible de ser opuesto al derecho de

[1121] Tesis, entre otras, sostenida por las SSTC 299/2000, de 11 de diciembre, FJ 2, 14/2001, de 18 de enero, FJ 3, 202/2001, de 15 de octubre, FJ 3, citadas todas por la STC 167/2002, de 18 de septiembre.

la persona invadida en su derecho al secreto de las comunicaciones, con pleno respeto del principio de proporcionalidad: la potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito. Tal criterio se basa en dos razones muy concretas, como son tanto la posibilidad de expansión de determinados delitos por las redes de comunicaciones, y la grave dificultad de su persecución por los medios tradicionales de investigación. De esta suerte, la implicación del principio de necesidad de la medida y la lucha contra auténticos santuarios de impunidad abren un campo hasta ahora inexplorado para el empleo de técnicas de investigación basadas en la injerencia sobre contenidos o datos de tráfico de comunicaciones, y por ende, sin duda sobre los datos almacenados por mandato de la LCD.

En conclusión, la interpretación del concepto de delito grave usado por el legislador de la LCD debe estar abierto a todos estos matices y criterios y no al meramente literal de nuestro código criminal[1122]. Es la autoridad judicial quien, en última instancia ha de

[1122] Tratándose de investigaciones de ilícitos penales —*zur Verfolgung von Straftaten*—, el BVerG concluye que las exigencias constitucionales derivadas del principio de proporcionalidad imponen la necesaria existencia de ciertos hechos que fundamenten por lo menos la sospecha razonable de un delito grave, y si bien reconoce que el legislador dispone de cierto margen de discrecionalidad —Beurteilungsspielraum— para remitirse a un catálogo existente o crear un catálogo propio separado —recordemos que el art. 100g StPO se refiere a "entre otros, los mencionados en el catálogo del apartado 2 del art. 100»—, exige una mayor concreción a la hora de la calificación de un delito como grave, que debe encontrar una expresión objetiva en la norma penal, en particular a través de sus penas. Y así, el Tribunal germano considera que una cláusula general o la sola referencia a "delitos de significativa importancia» no es suficiente —F.J. núm. 228—, porque la normativa impugnada no solo permite la utilización de los datos en conexión con delitos graves, sino que entiende suficiente, independientemente de un catálogo delimitado, que se trate de delitos generales con una «significativa importancia" —F. J. 279—, o de delitos cometidos por medios de telecomunicación, lo que significa en la práctica, según el BVerG, que con esta regulación, los datos almacenados son prácticamente utilizables en relación con todos los delitos.Su uso pierde de vista su carácter excepcional frente a la importancia actual de las telecomunicaciones en la vida cotidiana. El legislador no se limita aquí a permitir el uso de los datos almacenados para el enjuiciamiento de delitos graves, sino que va demasiado lejos sobre esto –incluso con respecto a la Directiva europea en cuanto al objetivo de la conservación de datos, que la limita por su parte solo para la persecución de delitos graves, sin incluir ninguna cláusula general de prevención de riesgos. No obstante, el BVerG excluye de dicha censura el uso de las direcciones IP, para cuya regulación legal se requieren menores exigencias constitucionales, por lo que admite su empleo, con independencia de establecer un catálogo de delitos o de bienes jurídicos, tanto para la investigación

valorar, en función de los intereses en conflicto, si para avanzar en la investigación de cualquier delito puede o no tenerse acceso, y en qué medida, a los ficheros de datos relacionados con las comunicaciones electrónicas conservados por las operadoras de telecomunicaciones, y si, por tanto, estamos o no ante un delito grave a efectos del art. 1.1 LCD. Teniendo en cuenta la doctrina ya asentada del Tribunal Constitucional sobre la caracterización del concepto de delito grave como aquel que sea susceptible de superar el juicio de proporcionalidad en las injerencias en el derecho al secreto de las comunicaciones, la expansión de tal doctrina en la posible utilización procesal de la información almacenada sobre datos relativos a las comunicaciones es incuestionable, y

---

criminal, la seguridad pública o la salvaguarda de las tareas de inteligencia, como para la persecución de otras infracciones legales —vg. derechos de autor—, siempre que se justifique a partir de una ponderación especial y tan solo en los casos legalmente previstos —FF.JJ. 254 y 255—.

Si se trata de utilizar los datos de tráfico conservados de cara a evitar serias amenazas a la seguridad pública —*zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit*— o para cumplir los deberes legales de las autoridades de protección constitucional de los Gobiernos Federal y Estatales, el Servicio Federal de Inteligencia y la Inteligencia Militar —*zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes*—, el Tribunal germano considera que permitir el acceso a los datos en función de los catálogos de determinados delitos, cuyo impedimento debe permitir la utilización de los datos, no es una técnica apropiada de regulación, sino que se inclina por tomar en consideración legalmente y de manera directa los bienes jurídicos cuya protección debe legitimar una utilización de los datos, así como la intensidad de la amenaza a esos bienes jurídicos —F. J. núm. 230—, y concluye que la recuperación de los datos de tráfico almacenados solo debe permitirse para "contrarrestar las amenazas a la vida, la integridad física o libertad de una persona, a la población o la seguridad de la Federación o de un Estado o para evitar un peligro común» (*Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr*) —F.J. 231—, recuperando así los fundamentos de su célebre sentencia de 27 de febrero de 2008 —BverfG, 1 BvR 370/2007— sobre los denominados "registros remotos" de equipos informáticos —*Online Durchsuchung*—.

En este punto, entiende ORTIZ PRADILLO que el BVerG ido demasiado lejos a la hora de exigir una regulación extraordinariamente detallada y descriptiva de los supuestos en los que resultará admisible la utilización de los datos de tráfico de las telecomunicaciones conservados, y el grado de detalle legal requerido es tan sumamente exigente, que si procediéramos a trasladar sus argumentos al ordenamiento español, daría al traste con la actual legislación, así como con la vigente línea jurisprudencial referida a la misma. Cf. Ortiz Pradillo, J. C., Tecnología versus Proporcionalidad…, op. cit., p. 9.

habrá de permitir sin duda su aplicación a importantes campos de la investigación criminal que quedarían si no fuera de los límites fijados por los arts. 13.1 y 33.2 CP[1123].

Todo ello, sin perder de vista que sigue resultando constitucionalmente necesaria la determinación por el legislador de los concretos tipos penales que pueden dar lugar al empleo de las medidas de la LCD.

Estas conclusiones quedan reforzadas si analizamos la cuestión tanto desde la perspectiva estricta de nuestro sistema constitucional de derechos como desde el punto de vista del Derecho europeo.

42.3.4.1 Análisis desde el Derecho constitucional español

Como se ha demostrado en el apartado anterior, el concepto de "delito grave" usado por la LCD no se identifica con el recogido en el Código Penal sino con criterios de proporcionalidad constitucional: delito grave es aquel que supera el juicio de proporcionalidad con respecto a la injerencia de derechos fundamentales en su proceso de averiguación y enjuiciamiento[1124].

Ya hemos visto cómo la jurisprudencia constitucional exige la gravedad del delito como presupuesto objetivo para la adopción de medidas que afectan al secreto de las comunicaciones. La intervención de las comunicaciones telefónicas solo puede

---

[1123] La fuerza expansiva de la doctrina desarrollada por la STC 104/2006, de 3 de abril, permite en nuestro caso la apertura de líneas de investigación respecto de modalidades delictivas que se prevalgan de las posibilidades de anonimato que brinda internet para su comisión y difusión, aunque siempre dentro de un contexto de mínima gravedad o relevancia social.

[1124] No determinar los delitos que justifiquen la cesión de los datos conservados genera una gran inseguridad jurídica a los titulares de dichos datos. Señalaba PÉREZ LÓPEZ, por ejemplo, que los usuarios de redes P2P pueden convertirse en potenciales sospechosos con la excusa de investigar posibles delitos contra la propiedad intelectual: "cuando, el uso de redes P2P no implica, en modo alguno, que se deba estar vulnerando ningún derecho de autor pues, existen multitud de contenidos en dichas redes cuyos autores ceden sus derechos de explotación para que sus creaciones puedan ser copiadas, modificas o distribuidas. Es el caso, por ejemplo, de las licencias de tipo Copyleft". Cf. Pérez López, Elena, Secreto de las comunicaciones, Sánchez-Crespo Abogados, Madrid, 9 de abril de 2007, p. 3.

considerarse constitucionalmente legítima cuando se ejecuta con observancia del principio de proporcionalidad, como sucede cuando se adopta para la investigación de delitos calificables de graves[1125].

Sin embargo, admitiendo las teorías expuestas sobre los derechos fundamentales afectados por la LCD, hemos de notar que la conservación y cesión de datos de tráfico y de localización es una medida menos agresiva —en lo que se refiere al derecho al secreto de las comunicaciones— que la intervención telefónica, en la medida en que ésta permite conocer el contenido de la comunicación, mientras que aquéllas —las medidas previstas en la LCD— no alcanzan a desvelar ese contenido, lo que queda expresamente excluido por el art. 1 LCD. En consecuencia, el principio de proporcionalidad habría de llevar a no exigir la misma gravedad del delito investigado cuando el ataque al derecho —o su amenaza— no reviste la misma entidad que en el caso de la intervención telefónica.

En este punto, cabe recordar la doctrina ya apuntada de la STC 70/2002, sobre la separación del ámbito de protección constitucional del derecho al secreto de las comunicaciones —que alcanza al proceso de comunicación mismo—, en relación con los ámbitos de protección de otros derechos —"finalizado el proceso en que la comunicación consiste", en que la protección constitucional se canaliza por otros cauces—. No es ocioso recordar aquí que también el Tribunal Supremo ha entendido que no debe equipararse la entrega de un listado de las llamadas efectuadas desde un determinado número a una intervención telefónica[1126], y que "no hay equiparación posible entre una conversación intervenida y la mera indicación del teléfono y titular al que se efectuó la llamada"[1127].

A la vista de ello, la cuestión que nos ocupa merece también ser examinada desde la perspectiva del derecho a la protección de datos que, como se apuntó, ha quedado perfilado como derecho autónomo por la jurisprudencia constitucional. Desde la configuración del derecho en la LOPD, su art. 6.1 exige el consentimiento inequívoco

---

[1125] Cf. STC 146/2006, de 8 de mayo, y las que en ella se citan.

[1126] Cf. STS de 22 de marzo de 1999.

[1127] Cf. STS de 7 de diciembre de 2001.

del afectado para el tratamiento de datos de carácter personal, "salvo que la ley disponga otra cosa" y el art. 11.2.a) LOPD excluye la exigencia de consentimiento para la comunicación de los datos cuando la cesión esté autorizada en una ley. En su Sentencia 292/2000, de 30 de noviembre, recordaba el Tribunal Constitucional que "el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos [...], no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos". Insistía además el Tribunal en que los derechos fundamentales pueden ceder ante bienes, e incluso intereses constitucionalmente relevantes, 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", lo que se decía después de recordar que "en numerosas ocasiones este Tribunal ha dicho que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana"[1128].

A la vista de todo lo anterior, no parece que pueda plantearse objeción a que la LCD extendiera su objeto a la detección, investigación y enjuiciamiento de todo tipo de delitos, graves o no según el CP. Dicha previsión no implicaría, por sí misma, una vulneración de los derechos protegidos por el art. 18 CE, sin perjuicio de que su aplicación, en cada caso, haya de respetar las exigencias propias que legitiman una injerencia en los derechos aludidos y, muy especialmente, al principio de proporcionalidad.

[1128] Añade el Tribunal Constitucional que el art. 9 CEDH y el TEDH también han tenido en cuenta estas exigencias, habiéndose referido este último a la garantía de la intimidad individual y familiar del artículo 8 CEDH, aplicable también al tráfico de datos de carácter personal, "reconociendo que pudiera tener límites como la seguridad del Estado —STEDH, caso Leander, de 26 de marzo de 1987, 47 y ss.—, o la persecución de infracciones penales" —*mutatis mutandis*, STEDH, casos Z, de 25 de febrero de 1997, y Funke, de 25 de febrero de 1993—, habiéndose exigido que tales limitaciones "estén previstas legalmente y sean las indispensables en una sociedad democrática, lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito"; todo ello con cita de diversas sentencias del TEDH.

No obstante, tampoco puede dejar de notarse que la posibilidad de una reforma de la LCD que aclarara este estado de cosas supondría, al mismo tiempo, una contravención por parte del Derecho interno español de lo indicado en la DCD, que limita sus medidas explícitamente a los *delitos graves, tal como se definan en la legislación nacional de cada Estado miembro*. Esto nos obliga a examinar la posibilidad también desde la perspectiva estricta del Derecho de la Unión.

42.3.4.2 Análisis desde el Derecho europeo

La extensión de las medidas de la LCD a los delitos que no tengan la consideración de graves en nuestra legislación no supondría una vulneración de lo dispuesto en el art. 1 DCD.

Para dar razón de tal afirmación, hemos de empezar recordando que 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* —la Directiva sobre la privacidad y las comunicaciones electrónicas— regula en sus arts. 5, 6 y 9 un principio general de confidencialidad de las comunicaciones, conforme al cual los Estados miembros han de garantizar, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, deben prohibir la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados[1129]. La obligación se extiende a los datos de localización distintos de los datos de tráfico[1130]. Puesto que la obligación de conservar datos que la DCD impone para los casos de delitos graves constituye una excepción a lo previsto en los arts. 5, 6 y 9 DPCE —tal y como expresamente indica el art. 3 de aquella norma comunitaria—,

[1129] Cf. arts. 5 y 6, Directiva 2002/58/CE.

[1130] Cf. art. 9, Directiva 2002/58/CE.

cabría pensar que extender esa excepción más allá de lo expresamente previsto en la DCD supondría una vulneración de lo dispuesto en la Directiva 2002/58/CE, y estaría, por tanto, vedado por el Derecho europeo. Sin embargo, puede entenderse —como ya manifestó el Consejo de Estado— que un correcto entendimiento de la relación entre ambas directivas no conduce a tal conclusión[1131].

Para ello, debe tenerse en cuenta que, junto a la excepción que la Directiva 2006/24/CE supone respecto de lo previsto en los artículos 5, 6 y 9 DPCE, el artículo 15 de esta última prevé expresamente que los Estados miembros pueden adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6 y en el artículo 9 de la Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos; y se añade que, para ello, "los Estados miembros 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"[1132].

En consecuencia, también desde el punto de vista del Derecho de la Unión Europea, la LCD podría haber extendido legítimamente sus previsiones a la investigación, detección y enjuiciamiento de cualquier delito, grave o no, siempre dentro de las coordenadas dictadas por la jurisprudencia del TEDH y del TC en materia de limitación de derechos fundamentales que ya hemos expuesto. Además, ha de hacerse hincapié en que, en tal caso, la LCD no sólo estaría incorporando a nuestro ordenamiento la DCD, sino simultáneamente una medida legal de las previstas en el citado art. 15 de la vigente Directiva 2002/58/CE[1133].

[1131] Cf. Dictamen del Consejo de Estado…, op. cit., III.A).1.a).

[1132] Cf. art. 15, Directiva 2002/58/CE.

[1133] "Así, si se mantiene la actual solución —razonaba el Consejo de Estado respecto del Anteproyecto— es conveniente que se incorpore una referencia al artículo 15 de la Directiva 2002/58/CE, en concreto, al final del apartado I de la exposición de motivos. En todo caso, el expediente no refleja la justificación o razones que llevan a adoptar ahora esta medida, sino que ello se hace con ocasión de la incorporación de

Al hilo de lo anterior, cabe señalar que los considerandos de la DCD ponen de manifiesto que la norma trata de armonizar las disposiciones adoptadas por distintos Estados en aplicación del art. 15 DPCE[1134]; pero que con ello no impide la adopción de otras medidas adicionales al amparo de este mismo artículo. Concretamente, el considerando 12 de la DCD parece tratar de aclarar cualquier duda sobre este punto al indicar que el art. 15.1 DPCE "sigue aplicándose a los datos, incluidos los datos [...] cuya conservación no se prescribe específicamente en la presente Directiva y que, por consiguiente, quedan fuera del ámbito de aplicación de la misma, así como a la conservación a efectos, incluidos judiciales, diferentes de los contemplados en la presente Directiva"[1135].

42.3.4.3 Extensión de las medidas de la LCD a delitos no graves

Para hacer más completo y sistemático nuestro análisis, una vez fijado lo que creemos ha de entenderse por delito grave en la LCD —y por tanto, delimitada con precisión una parte importante de su objeto y proporcionalidad—, cabe preguntarse seguidamente cuál será entonces el régimen de conservación de datos para aquellos delitos que no puedan calificarse como graves a efectos de la aplicación de la LCD. El legislador parece haber considerado a este respecto que la restricción del acceso a información sobre comunicaciones puede solventarse por la aplicación ordinaria de la LECrim en aquellos supuestos en los que no se abarcara el concepto de delito grave que maneja; pero ello no sería correcto.

Si bien la interceptación de comunicaciones al amparo de lo dispuesto en el art. 579 LECrim[1136] permite en concretos supuestos de delitos que no alcancen la categoría de

---

una Directiva que tiene un menor alcance". Cf. Dictamen 32/2007 del Consejo de Estado…, doc. cit., apart. III.A.c).

[1134] Cf. Considerandos 4, 5 y 6, DCD.

[1135] Cf. Considerando 12, DCD.

[1136] Por su interés, transcribimos aquí el tenor del artículo (redacción según Ley Orgánica 4/1988, de 25 de mayo): "1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que

delitos graves la captación y retención en origen de datos de tráfico e incluso el aprovechamiento de las potencialidades técnicas de los operadores por razón de la obligación de conservación de unos datos que no tendrían por qué generarse siquiera si no fuera por mandato de la LCD —como sucede con el ejemplo de los datos de localización—, quedarían excluidos los datos ya generados bajo la disciplina de la LCD. Por otra parte, el recabo de datos almacenados por las operadoras relacionados con las comunicaciones electrónicas quedaría al margen de la norma general del art. 11.2 d) LOPD[1137], y como es de imaginar, con más motivo, de las normas sobre documentos establecidas para la fase de instrucción en la LECrim —en concreto, los arts. 334.1[1138] y 574[1139]—, que difícilmente podrían sobrepasar la frontera protectora

---

el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

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

4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación".

[1137] Cf. art. 11.2.d) LOPD: "El consentimiento exigido en el apartado anterior no será preciso: […] d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas".

[1138] Dispone el artículo que "el Juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida. El Secretario judicial extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo".

impuesta por la LCD. La Ley establece la creación de unos determinados ficheros de datos de carácter personal que solamente pueden ser utilizados para específicos fines relacionados con la investigación de los delitos graves. Por tanto, el Juez solamente podrá acceder a aquellos datos que, coincidentes con los que se almacenen por mandato de la LCD, se conserven en ficheros distintos por los operadores de telecomunicaciones de conformidad con la legislación específica contenida en el art. 38 LGT. La decisión judicial deberá especificar la fuente de los datos que se recaben para no transgredir la norma establecida en el art. 1.1 LCD —cuyas consecuencias podrían irradiar a otros medios de prueba derivados, si es que la transgresión llegara a alcanzar relevancia constitucional[1140]—.

Por último, resulta casi obvio añadir que queda absolutamente vedada la posibilidad de aplicar las medidas de la LCD a los hechos que desde un primer momento sean calificadas como simples faltas.

42.3.4.4 Extensión de las medidas de la LCD a causas civiles

Está fuera de duda que los datos a los que se refieren los deberes de retención impuestos por la LCD no pueden ser requeridos judicialmente en el marco de un proceso civil, laboral o contencioso-administrativo. De este modo, los casos por incumplimientos o por la responsabilidad civil contractual o extracontractual que puede derivarse de una contratación electrónica quedan excluidos de la aplicación de esta Ley, y por ello, los datos electrónicos de meras comunicaciones contractuales mercantiles o

---

[1139] El art. 574 LECrim dispone que "El Juez ordenará recoger los instrumentos y efectos del delito y también los libros, papeles o cualesquiera otras cosas que se hubiesen encontrado, si esto fuere necesario para el resultado del sumario. Los libros y papeles que se recojan serán foliados, sellados y rubricados en todas sus hojas por el Secretario judicial, bajo su responsabilidad".

[1140] Cf. art. 11 LOPJ, que establece que "no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales".

civiles no pueden ser puestas a disposición de la autoridad competente en tanto su ámbito cae fuera de la obligación impuesta por los arts. 6 y 7 LCD[1141].

No obstante, no puede negarse que los datos generados en las comunicaciones electrónicas pueden resultar de vital importancia para acreditar hechos relevantes en un proceso civil. Pensemos, por ejemplo, en un litigio en el que interesara dilucidar si ha existido relación comercial entre dos empresas o se tratara de conocer la identidad, para demandarlos, de infractores de derechos de propiedad intelectual que descargan de modo ilegal programas, música, etc., sin estar autorizados ni retribuir a sus autores.

Ante esta perspectiva, ORMAZÁBAL SÁNCHEZ cree que el legislador español debería replantearse la restricción del deber de comunicación de datos al marco del proceso penal por delito grave y ampliarlo a otros ámbitos, atendiendo, por ejemplo, a la cuantía de las pretensiones ejercitadas en el proceso o al hecho de ventilarse en el mismo cuestiones de orden público —familia, estado civil de las personas, etc.—, o incluso que se confiase a la ponderación de los Tribunales resolver en cada caso si la medida de requerir la aportación de datos retenidos o conservados guarda o no la debida proporcionalidad[1142].

Tal propuesta no carece de fundamento, puesto que cuenta con el apoyo de la Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 29 de enero de 2008 que se pronunció expresamente sobre la adecuación al Derecho europeo de la normativa española que consagraba la referida limitación a las causas penales de los deberes de conservar y comunicar datos por requerimiento judicial respecto de la normativa

---

[1141] Así lo entendemos nosotros con RODRÍGUEZ DELGADO, quien pone por ejemplo la obtención de datos personales por parte de los operadores de telecomunicaciones ante el incumplimiento de algún cliente por el impago de determinadas facturas. Cf. Rodríguez Delgado, J. P., La ley 25/2007 sobre conservación de comunicaciones…, op. cit., p. 7.

[1142] Cf. Ormazábal Sánchez, G., Los deberes de conservación de datos por parte de los operadores de telecomunicaciones y su aportación al proceso mediante requerimiento judicial (Reflexiones a la luz de la legislación española y de la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea), Diario La Ley, n. 7055, Sección Doctrina, 13 Nov. 2008, Año XXIX, Ref. D-322, Editorial La Ley.

española aplicable en el momento[1143]: el art. 12 LSSI —posteriormente derogado por la LCD—. La exclusión de los procesos no penales en lo relativo al deber de conservar y comunicar datos a requerimiento judicial es idéntico en ambos textos legales, si bien el art. 12 LSSI venía a incorporar al ordenamiento interno las disposiciones de otras directivas, en concreto, del art. 13.1 de la *Directiva 95/46/CE, del Parlamento Europeo*

[1143] Promusicae es una asociación sin ánimo de lucro que agrupa a productores y editores de grabaciones musicales y audiovisuales. Mediante escrito de 28 de noviembre de 2005, promovió diligencias preliminares ante el Juzgado de lo Mercantil núm. 5 de Madrid contra Telefónica, sociedad cuya actividad consiste, entre otras, en prestar servicios de acceso a Internet. Promusicae solicitó que se ordenase a Telefónica revelar la identidad y la dirección de determinadas personas a las que ésta presta un servicio de acceso a Internet y de las que se conoce su dirección «IP» y la fecha y hora de conexión. Según Promusicae, estas personas utilizan el programa de intercambio de archivos denominado KaZaA, —conocido como *peer to peer* o P2P—, y permiten el acceso, en una carpeta compartida de su ordenador personal, a fonogramas cuyos derechos patrimoniales de explotación corresponden a los asociados de Promusicae. Esta última alegó ante el órgano jurisdiccional remitente que los usuarios de KaZaA están cometiendo actos de competencia desleal y vulneran los derechos de propiedad intelectual. Por consiguiente, solicitó que se le facilitase la información referida para poder ejercitar contra los interesados las correspondientes acciones civiles. Mediante auto de 21 de diciembre de 2005, el Juzgado de lo Mercantil núm. 5 de Madrid estimó la solicitud de diligencias preliminares presentada por Promusicae. Telefónica formuló oposición contra este auto afirmando que, conforme a la LSSI, la comunicación de los datos solicitados sólo estaba autorizada en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y de la defensa nacional y no en el marco de un procedimiento civil o como medida preparatoria de un procedimiento civil. Por su parte, Promusicae alegó que el artículo 12 de la LSSI debía interpretarse conforme a diversas disposiciones de las Directivas 2000/31, 2001/29 y 2004/48, y a los artículos 17, apartado 2, y 47 de la Carta, textos que no permiten a los Estados miembros restringir únicamente a los fines a los que se refiere el tenor de esta Ley el deber de comunicar los datos de que se trata. En estas circunstancias, el Juzgado de lo Mercantil núm. 5 de Madrid decidió suspender el procedimiento y plantear al Tribunal de Justicia la siguiente cuestión prejudicial: «El Derecho comunitario y, concretamente, los artículos 15, apartado 2, y 18 de la Directiva 2000/31, el artículo 8, apartados 1 y 2, de la Directiva 2001/29, el artículo 8 de la Directiva 2004/48, y los artículos 17, apartado 2, y 47 de la Carta [...], ¿permiten a los Estados miembros restringir al marco de una investigación criminal o para la salvaguardia de la seguridad pública y de la defensa nacional, con exclusión, por tanto, de los procesos civiles, el deber de retención y puesta a disposición de datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, que recae sobre los operadores de redes y servicios de comunicaciones electrónicas, proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamientos de datos?».

y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[1144] y del art. 15.1, penúltimo inciso, de 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*[1145]. La sentencia —respondiendo a la cuestión prejudicial

---

[1144] Cf. Artículo 13 —*Excepciones y limitaciones*—: "1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 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 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.

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas".

[1145] Cf. artículo 15 —*Aplicación de determinadas disposiciones de la Directiva 95/46/CE*—: "1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, 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 del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del rtículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros 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. Todas las medidas

planteada— afirma que es compatible con el Derecho de la Unión Europea el modo de proceder del legislador español al ceñir al marco del proceso penal el referido deber de conservación y comunicación de datos. El legislador español es por tanto libre de extender a cualquier clase de procesos los deberes de conservación de datos y su comunicación por requerimiento judicial, o puede, como efectivamente había hecho, limitarlos a la represión de la criminalidad grave. Indica además el Tribunal que la Directiva 2002/58 "no excluye la posibilidad de que los Estados miembros impongan el deber de divulgar datos personales en un procedimiento civil"[1146], si bien "el tenor del artículo 15, apartado 1, de esta Directiva no puede interpretarse en el sentido de que obliga a los Estados miembros a imponer tal deber en las situaciones que enumera", de manera que:

> "las Directivas 2000/31, 2001/29, 2004/48 y 2002/58 no obligan a los Estados miembros a imponer, en una situación como la del asunto principal, el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. Sin embargo, el Derecho comunitario exige que dichos Estados miembros, a la hora de adaptar su ordenamiento jurídico interno a estas Directivas, procuren basarse en una interpretación de éstas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario"[1147].

A este razonamiento hemos de añadir que existe ciertamente una tendencia en el Derecho español a hacer prevalecer la intimidad personal sobre la posibilidad de obtener medios de prueba necesarios para hacer prosperar pretensiones civiles que pueden ser de gran importancia para quien las promueve[1148]. Además, es cierto que, una vez que el legislador ha llevado a cabo una injerencia en el derecho fundamental con la obligación de la conservación generalizada, la revelación de dichos datos —previa autorización judicial— supone, en cualquier caso, una afectación de derecho fundamental considerablemente menos agresiva que, por ejemplo, la tradicional posibilidad de entrada y registro en un domicilio con el fin de ocupar títulos y

---

contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea".

[1146] Cf. STJUE de 29 de enero de 2008, fundamento 54.

[1147] Cf. STJUE de 29 de enero de 2008, fundamento 55.

[1148] Cf. Ormazábal Sánchez, G., Los deberes de conservación…, op. cit., p. 6.

documentos cuya aportación al proceso se ha pedido mediante diligencias preliminares[1149] —supuesto este en el que cabe además tomar conocimiento tanto de la identidad de los sujetos de las comunicaciones como del contenido de lo comunicado[1150]—.

No obstante, no podemos olvidar que el legislador no tiene obligación alguna, derivada del art. 24 CE, de proporcionar o facilitar medios de prueba al litigante en un proceso civil imponiendo a los operadores de telecomunicaciones deberes de retención y conservación de los datos generados en la prestación de sus servicios[1151]. Si efectivamente los establece, le resulta constitucionalmente lícito —y, como se acaba de ver, ajustado al Derecho de la Unión Europea— restringir su uso al ámbito del proceso penal y, en concreto, al proceso penal por delito grave. Una vez establecido el deber de conservar y retener los datos generados en las telecomunicaciones a los efectos de su posible utilización en el proceso penal, nada impide, en conclusión, que por la vía de la Directiva 2002/58/CE el legislador abra simultáneamente el deber de comunicación al juez civil, social o del contencioso-administrativo en relación con ciertas pretensiones.

En todo caso, nada parece apuntar a que esta posibilidad esté en la actualidad entre los planes del legislador español.

[1149] Dispone el art. 261 LECrim, en la redacción dada por Ley 19/2006, de 5 de junio, que si "la persona citada y requerida no atendiese el requerimiento ni formulare oposición, el tribunal acordará, cuando resulte proporcionado, las siguientes medidas, por medio de un auto, en el que expresará las razones que las exigen: […] 2. Si se hubiese solicitado la exhibición de títulos y documentos y el tribunal apreciare que existen indicios suficientes de que pueden hallarse en un lugar determinado, ordenará la entrada y registro de dicho lugar, procediéndose, si se encontraren, a ocupar los documentos y a ponerlos a disposición del solicitante, en la sede del tribunal.

3. Si se tratase de la exhibición de una cosa y se conociese o presumiese fundadamente el lugar en que se encuentra, se procederá de modo semejante al dispuesto en el número anterior y se presentará la cosa al solicitante, que podrá pedir el depósito o medida de garantía más adecuada a la conservación de aquélla".

[1150] Cf. Ormazábal Sánchez, G., Los deberes de conservación…, op. cit., p. 5.

[1151] Como reconoce ORMAZÁBAL SÁNCHEZ, el legislador, al impedir la comunicación de los datos a los efectos de un proceso civil, no está lesionando el derecho a obtener la tutela judicial efectiva de los justiciables. Ibíd.

42.3.5 El plazo de conservación

El plazo de conservación de los datos se halla vinculado a la propia medida de conservación y plantea la necesidad de ponderación entre la finalidad perseguida —el aseguramiento de la eventual puesta a disposición de los datos conservados, cediéndolos a los agentes facultados— y el gravamen que para el derecho a la protección de los datos de carácter personal supone la prolongación en el tiempo del tratamiento de los datos. Si bien podrían parecer más justificadas las previsiones de distintos plazos de conservación en virtud de la finalidad a que se adscriba la cesión —vg. represión de delitos sin especificaciones o represión de delitos concretos especialmente graves—, como ha sido el caso de Italia, no ha sido ha sido para la LCD[1152].

La cuestión de la proporcionalidad de los plazos no es, sin embargo, tan sencilla, pues —como expone GONZÁLEZ LÓPEZ— al ser inindiciaria, la justificación de la medida en atención a la finalidad perseguida no se manifiesta en el momento de llevar a cabo la conservación, sino cuando se presenta la conveniencia de ceder los datos[1153]. Ello supone que, aunque la cesión de datos sólo tenga lugar cuando se vincule a la represión de delitos graves, la conservación se efectuará igualmente respecto de la totalidad de datos —ya que todos deberán estar disponibles—, sin que se produzca ninguna matización en la afección que implica el plazo de conservación de los datos, que será igual para todos los datos, con independencia de que sólo se revelen durante el segundo período aquellos cuya cesión se justifique por la particular gravedad del delito investigado. En definitiva, la duración de la conservación sólo admite su ponderación atendiendo a la gravedad del perjuicio que comporta la extensión temporal de la conservación, por un lado, y la finalidad inmediata como un "todo", esto es, contemplada como el aseguramiento de la puesta a disposición con vistas al fin de la cesión.

De esta manera, para establecer el plazo de duración debe atenderse al supuesto más acuciante al que se apela para legitimar la conservación —la cesión para la

---

[1152] Acerca de la normativa italiana, Cf. González López, J. J., Los datos de tráfico..., op.cit., p.404 y ss.

[1153] Cf. González López, J. J., en Comentarios a la Ley 25/2007…, op. cit., p. 12.

investigación de delitos graves—, sin que resulte admisible refugiarse en la supuesta modulación de la afección al derecho que implicaría la previsión de distintos plazos en atención a lo que, en realidad, es la finalidad mediata. Así pues, la única posibilidad de introducir variaciones en la afección al derecho a la protección de los datos de carácter personal operando sobre el plazo de conservación es establecer distintos plazos de conservación en función de las categorías de datos que se conserven, opción no elegida por la LCD. La única posibilidad al respecto es que, si bien el período de conservación se fija en doce meses, éste resulta ampliable a dos años o reducible a seis meses mediante reglamento y previa consulta a los operadores [1154] pero sólo "para determinados datos o una categoría de datos" y tomando en consideración los únicos factores relevantes para fijar el plazo de conservación: el coste de almacenamiento y conservación y el interés de dichos datos para las finalidades mediatas[1155].

No obstante, no puede dejar de señalarse que esta habilitación para variar el plazo de conservación —calificada de "desconcertante" por RODRÍGUEZ LAINZ [1156] — fue rechazada en las alegaciones de ONO, S.A.U. y la Asociación de Operadores de Cable al Anteproyecto, que se inclinaban por fijar un plazo "objetivo e inamovible, excluyéndose la posibilidad de modificación posterior"[1157]. Sin duda, la necesidad de seguridad jurídica frente a las eventuales veleidades de la Administración Pública pesó en este caso más que la necesidad de ponderación en la materia u otros intereses.

En todo caso, se constata una tendencia a considerar los actuales plazos permitidos por la LCD y la DCD como excesivos. Si, como vimos, para el Tribunal constitucional alemán el plazo de seis meses constituía el borde de lo constitucionalmente proporcional, en el no muy diferente caso de España, el actual plazo de la normativa española sería claramente inconstitucional por su exceso[1158]. Es preciso recordar aquí que en la Comunicación de la Comisión de 26 de enero de 2001 —Comunicación e-

[1154] Como señala dos veces el art. 5.1 LCD, frente a la única referencia que se hacía en el Proyecto.

[1155] Cf. art. 5.1 LCD.

[1156] Cf. Rodríguez Lainz, J.L., "El principio de proporcionalidad... (I)", op.cit., p.8.

[1157] Cf. Dictamen 32/2007 del Consejo de Estado…, doc. cit., antecedente quinto, b).

[1158] Nos referimos a la Sentencia del Tribunal Constitucional alemán, de 2 de marzo de 2010, que añade en su F.J. núm. 209 que se trata, sin embargo, de un almacenamiento sobre un peligro grave con una extensión tal, como hasta ahora el ordenamiento no había conocido previamente.

Europe 2002— se hablaba de un plazo de tres meses[1159], y que en su Dictamen de 19 de enero de 2006, el CESE expresaba su inquietud con respecto a los derechos fundamentales relativos a la conservación de datos electrónicos, el uso e intercambio de los mismos, la proporcionalidad de la medida, y en particular, los períodos de conservación por considerarlos excesivamente largos[1160].

Así las cosas —y con la perspectiva de una anunciada reforma de la DCD en éste y otros puntos— parece que una mejor ponderación de los plazos, efectuada sobre datos empirícos, podría dar lugar en el futuro a una revisión a la baja de los plazos de conservación permisibles.

[1159] "El Parlamento Europeo es sensible a las cuestiones de la intimidad, y se inclina generalmente a favor de una protección fuerte de los datos personales. Sin embargo, en los debates sobre la lucha contra la pornografía infantil en Internet, el Parlamento Europeo se ha expresado en el sentido de favorecer una obligación general de conservar datos sobre tráfico durante un período de tres meses". Cf. Comunicación de la Comisión de 26 de enero de 2001, Comunicación e-Europe 2002, p. 20.

[1160] Cf. Dictamen del CESE…, doc. cit., punto 1.2.

QUINTA PARTE. RÉGIMEN DE LOS SERVICIOS DE TELEFONÍA MEDIANTE TARJETAS PREPAGO

43 Presentación y ámbitos objetivo y subjetivo del régimen

En esta quinta y última parte de la presente Tesis expondremos el particular régimen de los servicios de telefonía mediante tarjetas prepago diseñado por la Disposición Adicional Única —en adelante, DAU— de la LCD. Si bien dicho régimen dista en buena medida de lo dispuesto en el articulado de la norma, aplicaremos en donde sea posible u oportuno algunas de las conclusiones que hemos extraído del análisis de la normativa en los bloques anteriores.

Como decíamos, sin base en previsión alguna de la DCD, la DAU de la LCD introduce en nuestro ordenamiento a través sus ocho apartados una regulación especial para los servicios de telefonía mediante tarjetas de prepago, cuyo examen es necesario abordar en esta Quinta Parte, si queremos dar cuenta exacta de cuál es la vigente normativa española en materia de conservación de datos.

Para ello, debemos hacer primeramente algunas consideraciones sobre la necesidad de este régimen especial que el legislador nacional ha tenido a bien configurar. En concreto, hemos de empezar recordando que, dado que el objetivo último de la conservación generalizada de datos es permitir o contribuir a la identificación de los autores de hechos delictivos en relación con los cuales las comunicaciones electrónicas constituyen el medio de comisión o una fuente de información, "la eficacia de esta medida —señala GONZÁLEZ LÓPEZ— corr[ía] el riesgo de quedar anulada, de no establecerse una serie de medidas que, desvirtuando las posibilidades de "anonimización" del proceso comunicativo, permitan relacionar los datos conservados y, en su caso, cedidos, con sus titulares"[1161]. Existía en consecuencia un "refugio"

[1161] Cf. González López, J. J., Comentarios a la Ley 25/2007…, op. cit. p. 28.

electrónico para ciertos delitos[1162]. En este sentido, la identificación de los usuarios de tarjetas inteligentes con modalidad de prepago establecida por la DAU ha pretendido romper con la puerta abierta al anonimato en las comunicaciones telefónicas que brindaban estas populares y económicas tarjetas.

De hecho, hasta la entrada en vigor de la regulación en presencia, no se solicitaba al cliente para la contratación de estos servicios ningún tipo de dato personal que le identificase, como sí se hacía —y se hace— para la contratación de un sistema de postpago. De ahí que se desconocieran las tarjetas que se encontraban en funcionamiento o en desuso en España. Con la norma introducida por la DAU, se pretendía en definitiva crear una base de datos por cada operador telefónico de manera que cada número de teléfono concedido estuviera asociado a una identidad personal —física o jurídica—. La finalidad perseguida es, por tanto, evitar la falta de identificación de los usuarios que disponen de este servicio y prevenir y perseguir delitos que hasta ahora quedaban impunes por la falta de control de estos medios telefónicos, obligándose por ley a dejar constancia de la personalidad del adquiriente de dicho servicio, al igual que se hace en el resto de servicios telefónicos y de comunicación.

De este modo, volviendo ahora nuestra mirada sobre la concreta regulación aprobada, ha de señalarse que el primer epígrafe de la DAU establece por vez primera en la historia del Derecho español de las telecomunicaciones el deber para los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago de llevar un libro-registro en el que conste la identidad de los clientes que adquieran una de estas tarjetas[1163]. La norma precisa asimismo el modo en que la identificación del cliente ha de efectuarse, concretamente, mediante documento acreditativo de la personalidad, tras cuya presentación habrá de hacerse constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento

[1162] Piénsese por ejemplo en los atentados de Madrid de 11 de marzo de 2004, donde gran parte de la organización del atentado se produjo gracias al uso de tarjetas telefónicas de prepago en las que no era necesaria la identificación de los sujetos adquirientes de las mismas.

[1163] De dudosa eficacia, otrosí de enormemente costosa para los operadores, se consideró esta medida por parte de la Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España. Cf. Dictamen 32/2007 del Consejo de Estado…, doc. cit., antecedente quinto, e).

identificativo utilizado y la naturaleza o denominación de dicho documento —DNI, pasaporte, tarjeta de residencia, etc.—. En el supuesto de las personas jurídicas, tal identificación se realiza aportando la tarjeta de identificación fiscal, dejando constancia en el libro-registro de la denominación social y el código de identificación fiscal[1164].

La anterior información se complementa con la obligación para los operadores de conservar también el número de abonado y la fecha y la hora de la primera activación del servicio, así como etiqueta de localización desde la que se ha activado el servicio[1165]. Además —como no puede ser de otra manera por ser principio general de la normativa sobre protección de datos—, los operadores deben informar a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, su disponibilidad en los términos expresados por la Disposición, y de los derechos recogidos en el art. 38.6 LGT[1166]. De esta manera, la previsión permite satisfacer —como ha indicado GONZÁLEZ LÓPEZ[1167]—, por una parte, las exigencias relativas al derecho de información de los titulares de los datos de carácter personal en la recogida de datos que se formulan en el art. 5.1 LOPD —actividad que implica la obtención por los operadores de los datos identificativos que pasan a formar parte de un fichero, denominado "libro-registro" por la LCD— y, por otra, permite asegurar el conocimiento por el titular del tratamiento que se dará a los datos más allá de la publicidad propia de la Ley. Aunque la norma no lo indique expresamente, es obvio que la negativa del cliente a facilitar los datos para este registro impedirá la celebración

---

[1164] Cf. apart. 1, DAU, LCD.

[1165] Cf. art. 3.1.e) LCD.

[1166] Dispone el precepto que "la elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia, garantizándose, en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías. A tal efecto, las empresas que asignen números de teléfono a los abonados habrán de dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento".

[1167] Cf. González López, J. J., Comentarios a la Ley 25/2007…, op. cit. p. 30.

del contrato de servicio telefónico dado el carácter necesario de la identificación y registro[1168].

En cuanto a los *sujetos obligados* a cumplir con el deber que acabamos de describir, estos son —de conformidad con lo dispuesto en el primer apartado— "los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago". El ámbito subjetivo coincide así en buena medida con el trazado por el art. 1 LCD para la conservación de datos. Sin embargo, esta previsión resulta ciertamente criticable.

A este respecto, hemos de señalar que el legislador parece no haber reparado en que —en la práctica cotidiana— la recepción de tales datos recaerá en su mayor parte en personas que nada tienen que ver con los operadores concernidos, y a quienes indirectamente se hace poseedores y responsables de la conservación de datos sensibles sobre la identificación de los clientes. Por añadidura, como veremos, la norma somete la información almacenada a los mismos principios de calidad, conservación, no manipulación y acceso limitado a los mismos que los demás datos de la LCD. Como es sabido, la mayor parte de las tarjetas de prepago llegan a los usuarios a través de los establecimientos expendedores abiertos al público, que no tienen una vinculación a la empresa operadora más allá de un posible contrato de exclusiva en la distribución. La regulación en este punto se muestra así manifiestamente imperfecta, pues el legislador ha obviado a un importante sujeto en este mercado. En la práctica, la aplicación de la DAU comporta diferir la entrega de los datos al operador concernido, dado que los

[1168] Telefónica abogó en sus alegaciones durante la tramitación por la supresión de la obligación de llevar un libro-registro en el que constara la identidad de los clientes de tarjetas prepago y veía razonable que se ampliara a dieciocho meses el plazo que se establecía para que los operadores estuvieran en disposición de cumplir las obligaciones previstas en la ley. También sugería que se trasladara a la Disposición Adicional Única la concreta y estricta definición de "agente facultado" contenida en el artículo 6, la unificación del régimen sancionador en el establecido en la Ley General de Telecomunicaciones y de las competencias sancionadoras en el Ministerio de Industria. Insistía en que la petición de los datos de identificación del titular de una tarjeta prepago con origen en una comunicación (listado de llamadas) estaba protegido por el secreto de las comunicaciones, por lo que el requerimiento de información debería realizarse mediante mandamiento judicial. Cf. Dictamen 32/2007 del Consejo de Estado…, doc. cit., antecedente quinto.

vendedores directos han de proceder a la obtención de los datos y a su inmediata cesión a la empresa de telecomunicaciones, que es el verdadero destinatario de la norma. Como no existe una compartición de ficheros —al no existir una relación de dependencia—, el dato captado por el expendedor ha de ser cedido, irremisiblemente y *ministerio lege*, al sujeto obligado a la llevanza del libro-registro, con aplicación por tanto de lo establecido en el art. 11.2.a) LOPD[1169]. No puede dejar de señalarse que los establecimientos expendedores de tarjetas no integrados en el círculo empresarial del operador concernido —salvo consentimiento del usuario y bajo el principio de calidad de los datos, en sus variantes de adecuación, pertinencia y no excesividad en relación con la finalidad de su conservación a que se refiere el art. 4.1 LOPD— carecen de legitimidad para conservar los datos, que necesariamente deben remitir al único obligado de la norma: el operador de servicios de telefonía móvil. De otro modo, la conservación de tales datos conculcaría abiertamente el derecho a la protección de datos de carácter personal de los compradores.

Así pues, la solución pasa necesariamente, bien por la respuesta práctica empleada por las operadoras —que recaban del expendedor los datos en soporte de papel, que los remite a éstas sin quedarse copia—, bien por establecer sistemas de almacenamiento temporal a los solos efectos de su pronta remisión al destinatario real de la norma de conservación y ulterior cancelación.

44 Agentes facultados

Dando un paso más en nuestro análisis, hemos de señalar que, conforme al apartado segundo de la norma en estudio, desde la activación de la tarjeta de prepago y hasta que

---

[1169] Dispone el art. 11 —*comunicación de datos*—: "1. 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.

2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley".

cese la obligación de conservación [1170], los operadores deben ceder los datos identificativos que acabamos de describir cuando les sean requeridos para el cumplimiento de sus fines por los agentes facultados —los mismos a que se refiere el art. 6.2 LCD[1171]— así como a "los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública en el curso de las investigaciones de seguridad sobre personas o entidades". Los operadores deben ceder los datos identificativos previstos en el ya meritado apartado primero —esto es, la información almacenada en los libros-registro: nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento— a todos estos agentes, si bien la cesión se somete a la condición de que les "sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales"[1172].

A pesar de que del tenor de la disposición parece deducirse de que nos encontramos ante un círculo de agentes facultados más amplio que el señalado en el art. 6.2 LCD, lo cierto es que esta actuación de investigación del delito previa a la actuación judicial entraña igualmente una actuación propia del concepto de Policía Judicial —como

---

[1170] El apartado segundo de la DAU en la versión del Anteproyecto establecía que los operadores debían estar en disposición de proporcionar los datos identificativos "desde la fecha de la activación y durante la vigencia de la tarjeta". La AEPD puso de manifiesto que parecía desprenderse de ello el que los datos identificativos serían cancelados en el momento mismo en que la tarjeta deje de estar activada, al haber concluido su "vigencia". El Consejo de Estado consideró que ese efecto se producía también en el Anteproyecto, sin que el inciso inicial ("sin perjuicio de lo dispuesto en el artículo 5 de la presente Ley") sirviera para evitarlo, puesto que la evidente diferencia entre el plazo de doce meses previsto en el artículo 5 y el plazo a que se refiere explícitamente el apartado 2 DAU llevarían a aplicar éste —y no el de doce meses—, aplicando en lo demás las previsiones del artículo 5 (destrucción, bloqueo, etc.). Para impedir aquella interpretación, el Consejo sugirió una redacción similar a la que finalmente se ha aprobado. Cf. Dictamen 32/2007 del Consejo de Estado…, doc. cit., apart. D.1.

[1171] Puesto que el personal del Centro Nacional de Inteligencia y los funcionarios de la Dirección Adjunta de Vigilancia Aduanera están incluido entre quienes tienen la consideración de "agentes facultados" —art. 6 LCD—, resulta redundante mencionarlo en este apartado 2 DAU —observación aplicable también a su apartado 4—.

[1172] Cf. apart. 4 DAU, LCD.

fácilmente se puede comprobar de la sola lectura del art. 282 LECrim[1173]—, por lo que en realidad se trata del mismo conjunto de sujetos que están autorizados en virtud de la LCD para acceder a los datos conservados ex art. 5 LCD.

De este modo, sobre la conveniencia de autorizar a este círculo de sujetos para las finalidades indicadas por la DAU, nos remitimos nuevamente y para evitar reiteraciones a todas las consideraciones expuestas sobre este particular en anteriores capítulos de esta Tesis.

45 Infracciones penales habilitantes de la cesión

Otra diferencia crucial de la DAU frente a la regulación contenida en la LCD radica en el tipo de infracciones penales que habilitan el acceso a los datos conservados, pues frente a la necesidad de investigación de *delitos graves* en el primer caso, en el segundo se reduce la exigencia a *cualquier delito del Código Penal o de las leyes penales especiales*. Obviamente, tal ampliación de la finalidad justificativa del acceso abre el abanico ya no sólo a los delitos graves o muy graves, sino también a los leves, dado que, al emplear el término genérico de "delito", caen bajo el amparo de la Disposición todos los tipos y subtipos penales codificados —excepto las faltas—.

De esta manera, el legislador español ha pretendido apartarse de la disciplina de la DCD, habilitando el acceso a la información almacenada en los libros-registro de adquirentes de tarjeta telefónica de prepago a la investigación de toda clase de delitos, en contraste con lo señalado en la normativa general, donde el beneficio obtenido de la cesión de datos del usuario —la represión de los delitos graves— era mayor que la afectación en los derechos fundamentales concernidos. Así pues, el efecto inmediato de esta ampliación es que el dato identificador del adquirente —en concreto: nombre y

[1173] Establece el artículo 282 LECrim que "la Policía judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la Autoridad Judicial".

apellidos o denominación social, nacionalidad y número de identificación del documento de identidad exhibido, al menos en tanto en cuanto se conserve en tal concepto— será accesible para la investigación de cualesquiera actividades delictivas. Puestos a ser exigentes, resulta curioso que las faltas hayan quedado excluidas de tan amplio marco, dado que tal omisión puede generar igualmente situaciones de impunidad, ante la imposibilidad de conocer la identidad de quienes estafen en cuantía inferior a cuatrocientos euros, amenacen, vejen, insulten o coaccionen a través de la telefonía de prepago.

Por si esto fuera poco, a diferencia de lo que sucede en el caso de la cesión de datos de las comunicaciones en el articulado de la LCD, la DAU habilita soterradamente la cesión con fines preventivos, superando el ámbito exclusivamente procesal penal que presenta la cesión en el caso del art. 1 LCD[1174]. En concreto, el apartado segundo de la DAU es susceptible de una lectura aún más extensiva por lo que respecta a las finalidades de la cesión en tanto que, allí donde el apartado cuarto señala como finalidades de la cesión "la investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales", el apartado segundo se limita a establecer el deber de cesión "para el cumplimiento de sus fines" de las autoridades indicadas. La amplitud con que están formuladas las finalidades de la cesión permite que ésta no sólo se restrinja a la finalidad de identificar a los titulares de los datos conservados, sino que haga posible su comunicación para cualquier otra investigación o actividad de detección de delitos.

Las funciones de Policía Judicial, frente a las de policía de seguridad, son de tipo procesal, en tanto las competencias vinculadas a la seguridad pública son de tipo preventivo-administrativo. De ello se deriva que, al margen de la cesión al CNI —que se sitúa en el ámbito de la seguridad nacional—, la cesión de datos de las comunicaciones electrónicas únicamente podrá efectuarse, atendidos los sujetos

[1174] Esta afirmación se ve respaldada por la referencia como destinatarios a "los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y para el mantenimiento de la seguridad pública", ya que, siguiendo a PEDRAZ PENALVA, la función de policía de seguridad incluye "el desempeño de tareas preventivas y de indagación". Cf. Pedraz Penalva, E., Notas sobre policía..., op.cit., p. 46.

facultados, con fines de persecución penal, en tanto la de "datos identificativos" será susceptible —a la luz de los sujetos legitimados como cesionarios— de ser empleada con fines de prevención de delitos.

En definitiva, ambos tipos de cesión difieren tanto en lo que respecta a la reserva jurisdiccional como a los fines que puede perseguir la medida. Las divergencias expuestas no responden a exigencias específicas derivadas del tipo de datos de carácter personal a que se refiere la cesión en uno y otro caso, ya que en ambos concurre la especial cualificación que, desde el punto de vista del derecho a la protección de los datos de carácter personal, implica el tratamiento previo a la revelación. Tampoco cabe apelar a la especial "sensibilidad" de los datos de las comunicaciones frente a los identificativos, pues, abstractamente considerados, los datos identificativos son mucho más reveladores que los vinculados a las comunicaciones electrónicas —cuestión distinta es que los datos identificativos cobren trascendencia desde la óptica de los fines perseguidos con la cesión por la vinculación que quepa establecer entre éstos y los datos de las comunicaciones revelados previamente—. La explicación de esta divergencia en el régimen regulador de la cesión de datos parece hallarse en la concepción del ámbito de cobertura del derecho al secreto de las comunicaciones que subyace a la LCD —de la que ya nos ocupamos—, en virtud de la cual las mayores garantías que rodean la cesión de datos obedecerían a la restricción que —considera el legislador— se lleva a cabo en el derecho al secreto de las comunicaciones en el supuesto de cesión de los datos de las comunicaciones. La ausencia de dicha limitación motivaría, por el contrario, que la cesión de "datos identificativos" no deba sujetarse a resolución judicial previa.

46 Reserva de autorización judicial

Quizás el aspecto más censurable de la regulación contenida en la DAU sea el que la cesión de los datos conservados en el libro-registro no precisa verse sometida al régimen de autorización judicial previa, como se deduce de que el articulado omita cualquier mención a tal requisito. Ya el Consejo General del Poder Judicial, en su

Informe al Anteproyecto de Ley, opinaba al respecto que esta garantía resultaba innecesaria, al ser el registro de los datos de identidad previo a la activación, y no generados en los procesos de comunicación, como sí lo son los cubiertos por el art. 7 LCD[1175].

A nuestro entender, resulta totalmente rechazable la diversidad de regímenes aplicables a la cesión de datos que resulta de la DAU, exigiendo autorización judicial para la cesión de los datos del art. 5 LCD pero no para los de los usuarios de telefonía prepago. El legislador parece olvidar el gravamen que comporta la actividad prevista en relación tanto con los datos de las comunicaciones como con los identificativos de telefonía prepago. Es más, si trasladamos el debate al ámbito de la proporcionalidad de la medida, se echa de ver que la cesión de estos datos identificativos resulta más gravosa que los generales del art. 5 LCD, por ser los primeros susceptibles de identificar claramente a su titular.

En consecuencia, creemos que la interpretación del apartado cuarto de la DAU no puede llevarnos a concluir que no se precisa la autorización judicial para el acceso y cesión de tales datos. Bastaría con recordar una constante jurisprudencia de nuestro TC, representada, entre otras, por las SSTC 37/1989, de 15 de febrero, 207/1996, de 16 de

---

[1175] En este sentido, el Consejo de Estado consideró que la cesión de estos datos no precisaba verse sometida al régimen de autorización judicial previa debido a que el registro de los datos era previo a la activación de la tarjeta y no son generados en el proceso de comunicación. Cf. Dictamen 32/2007 del Consejo de Estado…, doc. cit., apart. III.D.1.

Por el contrario, RODRÍGUEZ LAINZ sostiene que el apartado cuarto de la DAU no puede interpretarse como no exigente de autorización judicial, por oponerse la ausencia de este requisito a la reserva de ley orgánica para la restricción del derecho a la protección de los datos de carácter personal y al principio de monopolio de decisión jurisdiccional en la restricción individual de derechos fundamentales, si bien, matiza, en este segundo caso ello se debe a que no concurren motivos de urgencia que permitan prescindir de ella, postura con la que no podemos estar de acuerdo —al igual que con las consideraciones que efectúa acerca de la no necesidad de autorización judicial para acceder a los registros de llamadas en un teléfono móvil— por los argumentos expuestos en GONZÁLEZ LÓPEZ. En todo caso, el citado autor considera que la necesidad de autorización judicial para el acceso a estos datos puede desprenderse de lo dispuesto en los artículos 6.1 y 7.1 LCD, a pesar de que el tenor de la disposición no contiene dicha exigencia. Cf. Rodríguez Lainz, J.L., "El principio de proporcionalidad... (I)", op.cit., pp. 6 y 7, y González López, J.J., Los datos de tráfico..., op.cit., p. 337 y ss.

diciembre, 70/2002, de 3 de abril —o por citar entre las más recientes, la ya mencionada STC 206/2007, de 24 de septiembre—, que advierte que nuestra Constitución no establece taxativamente un principio de reserva jurisdiccional para la restricción de derechos fundamentales, más allá de aquellos específicos supuestos en que así se establezca en su texto o en que la gravedad de la afectación del derecho así lo exija taxativamente[1176]. Fuera de tales ámbitos, la sola existencia de una norma legal habilitante en los términos anteriormente definidos puede permitir la atribución competencial a favor de poderes públicos distintos de la autoridad judicial[1177].

Ahora bien, tal posibilidad de actuación es entendida en términos de acreditadas razones de urgencia y necesidad en el desempeño de tal facultad de actuación, tal y como puede comprobarse en el supuesto de hecho analizado por la STS 1235/2002, de 27 de junio[1178], que hace suya la doctrina constitucional iniciada por la STC 70/2002, de 4 de abril, al considerar que la intervención del teléfono móvil de un detenido en el curso de una lícita diligencia de entrada y registro y el examen de mensajes acumulados en su memoria no supondría un atentado al derecho al secreto de las comunicaciones, considerando que el derecho entonces afectado no sería otro que el derecho a la intimidad personal de la persona investigada, vulnerable por tanto a actuaciones de injerencia proporcionadas a las circunstancias del hecho y de la investigación —incluso sin la previa expresa autorización judicial— cuando se trata de actuaciones policiales

---

[1176] En similares términos, ORTELLS RAMOS, M., Exclusividad jurisdiccional para la restricción de derechos fundamentales y ámbitos vedados a la injerencia jurisdiccional, en *Medidas restrictivas de derechos fundamentales*, Cuadernos de Derecho Judicial, Escuela Judicial-Consejo General del Poder Judicial, Madrid, mayo 1996, p. 46.

[1177] Nótese que el art. 8.2 CEDH incluye un concepto extenso de la excepción a la regla general de la injerencia en su ámbito de protección, al hablar no de autoridad judicial, sino de autoridad pública.

[1178] La STS 1649/2002, de 1 de octubre, vuelve a hacerse eco implícitamente de tal posibilidad, cuando no llega a poner reparo alguno en el acceso, en el contexto de un registro y detención a un sospechoso, a la memoria de teléfono móvil de uno de los detenidos, en el que se descubriera la anotación de varias matrículas de vehículos policiales camuflados, y en los archivos de un ordenador portátil, en el que se descubriera, perfectamente reseñada la ruta que llevaría el paquete postal que fuera objeto de una entrega vigilada. Sobre este ejemplo, en concreto, puede examinarse en trabajo de MAGRO SERVET, V., Intervención de mensajes SMS y eficacia de las Juntas Provinciales de Policía judicial, en Diario La Ley, año XXVIII, nº 6764, de 26 de julio de 2007.

en el ejercicio de urgentes o apremiantes funciones de prevención e investigación de actividades criminales.

El acceso policial a las bases de datos de los libros-registros de adquirentes de tarjetas telefónicas de prepago no respondería por definición a ese concepto de urgencia y necesidad en que el Tribunal Constitucional enmarca la licitud constitucional de tales normas habilitantes. En consecuencia, debería ser interpretado en el sentido de exigir la previa autorización judicial como regla general —pauta normal de actuación—, salvo en aquellos supuestos en que la urgencia en la obtención de tal información fuera tal que no pudiera esperarse a la obtención de la necesaria previa autorización judicial.

A la misma conclusión se llegaría interpretando el confuso art. 7.1 LCD, que dispone que los operadores "estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el art. 3 LCD concernientes a comunicaciones que identifiquen a personas". Así pues, podríamos interpretar que lo que realmente lleva a cabo la DAU es la creación de un fichero de datos de carácter personal con un contenido concreto que se integra en el art. 3 LCD, es decir: impone a los operadores el deber de identificar al adquirente de tarjetas de prepago; y esa información que ha de recabarse *ministerio lege* se integra plenamente en las normas comunes relacionadas con los deberes impuestos a los operadores concernidos.

Por las razones expuesta, la solución a tan grave problema de legalidad constitucional ha de encontrarse a nuestro modo de ver en la extensión natural de la reserva de autorización judicial contenida en el art. 6.1 LCD[1179] a los datos conservados en el libro-registro de clientes de tarjetas de prepago. Si, como hemos sugerido, la DAU no es sino un apéndice específico de la LCD —en la que se dispone la obligación de creación de un determinado fichero de datos de carácter personal, precisamente sobre unos datos, los de identidad del titular o abonado de determinado terminal telefónico, que son objeto de deber de conservación para su posible cesión como dato relativo a las comunicaciones electrónicas— se comprenderá que nada debe obstaculizar la extensión

[1179] "Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos [...] previa autorización judicial".

de tal reserva de autorización judicial al acceso a los datos contenidos en dicho libro-registro.

47 Protección y seguridad de los datos identificativos

Desplazando ahora nuestra atención a las cuestiones de conservación y seguridad de los datos almacenados en virtud de la DAU, cabe señalar que la llevanza del libro-registro previsto en su apartado primero supone —indudablemente— un tratamiento de datos que en todo punto debe resultar conforme con lo dispuesto en la LOPD. Así lo confirmaron la AEPD y el Consejo de Estado durante la tramitación de la LCD[1180], y así ha quedado reflejado indirectamente en el apartado tercero de la DAU al disponer que los datos identificativos afectados por la misma estarán sometidos a las disposiciones de la LCD respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada. Tales medidas son aplicables tanto para los datos de las tarjetas prepago como para los datos de tráfico de las comunicaciones electrónicas en general, y por tanto, se someten a las disposiciones del art. 8 LCD —*Protección y seguridad de los datos*—.

No obstante, tampoco puede dejar de subrayarse el hecho de que el régimen de conservación establecido por la DAU se distancia claramente del régimen del art. 3 LCD, al imponer el deber de llevanza de un libro registro de clientes[1181] que adquieran las tarjetas prepago. Aunque la propia LOPD permite establecer mediante ley

---

[1180] Cf. Dictamen del Consejo de Estado…, op. cit., apart. III.D).

[1181] La DAU matiza que se considera cliente al comprador, persona física o jurídica que adquiere el producto. Evidentemente, el operador cumplirá con registrar los datos correspondientes a quien aparezca o se identifique como comprador, no teniendo obligación de indagar si dicha persona interviene a nombre de un tercero. Para eludir la finalidad de la norma, bastaría con buscar un intermediario, casi profesional, dedicado a adquirir tarjetas de prepago a su nombre que después vendería a terceras personas anónimas con quien contactara. La norma en este punto no puede pecar de una mayor ingenuidad. Habría resultado conveniente establecer un régimen de previa comunicación de cambios de titularidad, o de imposición de sanciones por la adquisición a nombre de terceros no declarada.

especialidades o excepciones en algunos aspectos —cf., al respecto, los arts. 6.1[1182] y 11.2.a)[1183] LOPD—, no deja de resultar un tanto artificiosa la distinción formulada por el legislador al diferenciar las finalidades propias de los datos relativos a las comunicaciones y los datos de identificación de adquirentes de tarjetas telefónicas de prepago, por cuanto que el dato obtenido en base a dicha norma habilitante finalmente pasa a integrarse entre los datos relativos a las comunicaciones que deben ser conservados a los fines dispuestos con carácter general por el art. 1.1 LCD.

48 Régimen sancionador

Para mayor garantía de la aplicación efectiva de las medidas de la DAU —incluyendo aquellas relativas a la seguridad—, sus apartados quinto y sexto regulan un breve y específico régimen sancionador.

Por una parte, el tratamiento de los datos a que se refiere la Disposición queda sometido al régimen de la LOPD, y, por tanto, también al sistema de sanciones establecido en la misma[1184], como es natural. Por otra parte, la norma dispone una serie de infracciones a nivel administrativo claramente emparentadas con las que se definen respecto de los datos relacionados con las telecomunicaciones en general, constituyendo como *infracciones muy graves* —apart. a)— tanto el incumplimiento de la llevanza del libro-

[1182] Dispone el precepto que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".

[1183] El tenor literal del artículo establece lo siguiente: "1. 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.

2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley".

[1184] En su Informe del Anteproyecto, insistía la AEPD que la exigencia de identificación de los titulares de las tarjetas de prepago estaba recogida en las legislaciones de otros Estados europeos y que no podía considerarse que el tratamiento de estos datos fuera contrario al principio de proporcionalidad previsto en el art. 4.1 LOPD; ahora bien —añadía— la llevanza del libro-registro previsto supondría un tratamiento de datos que en todo punto debía resultar conforme a lo dispuesto en la citada ley.

registro referido, como la negativa a la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición. Además, se consideran *infracciones graves* —apart. b)— la llevanza incompleta de dicho libro-registro así como la demora injustificada, en más de setenta y dos horas, en la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición. A estas infracciones les es de aplicación el régimen sancionador establecido en la LGT[1185], correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información[1186]. El procedimiento se ha de iniciar por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar la incoación[1187]. En todo caso, se debe recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador[1188].

[1185] Cf. De la Quadra Salcedo, T., Derecho de la Regulacion Economica, Tomo IV: Telecomunicaciones, Iustel, Portal Derecho, 2009; Cremades, J., y Rodriguez-Arana Muñoz, J., Comentarios a la Ley General de Telecomunicaciones, La Ley, 2004; y, Garcia de Enterria, E., Comentarios a la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, Civitas Ediciones, 2004.

[1186] Cf. apart. sexto, DAU.

[1187] Ibíd., párrafo segundo.

[1188] Ibíd. párrafo tercero. Resultaba llamativo en el Anteproyecto que, en relación con estas infracciones, se establecía la aplicabilidad del régimen sancionador establecido en la LGT pero atribuyendo la competencia para la imposición de las sanciones al Ministro del Interior o al Secretario de Estado de Seguridad según los casos. La solución adoptada —régimen sancionador de la Ley General de Telecomunicaciones pero con atribución de competencia al Ministerio del Interior— podría ocasionar dificultades prácticas y desigualdades en la aplicación de un mismo régimen sancionador —como señaló el Consejo de Estado—. Así, los criterios habitualmente seguidos por la Secretaría de Estado de Telecomunicaciones, en la aplicación de ese régimen sancionador, podrían ser diferentes de los que prime el Ministerio del Interior. Se sugería, por tanto, "una reconsideración del régimen previsto, ponderando otras posibles soluciones y, en particular, la posibilidad de mantener la aplicabilidad del régimen sancionador previsto en la Ley General de Telecomunicaciones, pero también las atribuciones resolutorias allí previstas, aunque estableciendo alguna especialidad procedimental, en la incoación o en la tramitación del expediente sancionador, a fin de dar intervención en el mismo a los órganos del Ministerio del Interior que pueda corresponder —otra posibilidad que podría valorarse, si se quiere mantener la competencia del Ministerio del Interior, consistiría en articular el régimen aquí previsto con las disposiciones de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana—". Cf. Dictamen 32/2007 del Consejo de Estado…, doc. cit., apart. III.D.1.

Asimismo, las sanciones para estas infracciones son las previstas en el art. 56 LGT[1189], que dispone —siendo sucintos— el siguiente régimen.

[1189] El tenor literal del artículo 56, bajo la rúbrica de *Sanciones*, establece:

"1. El Ministerio de Ciencia y Tecnología o la Comisión del Mercado de las Telecomunicaciones impondrán, en el ámbito de sus respectivas competencias, las siguientes sanciones:

a) Por la comisión de infracciones muy graves tipificadas en los párrafos q y r del artículo 53 se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción. En caso de que no resulte posible aplicar este criterio o que de su aplicación resultara una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: el 1 % de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio en la rama de actividad afectada o, en caso de inexistencia de éstos, en el ejercicio actual: el 5 % de los fondos totales, propios o ajenos, utilizados en la infracción, o 20 millones de euros.

Por la comisión de las demás infracciones muy graves se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción. En caso de que no resulte posible aplicar este criterio, el límite máximo de la sanción será de dos millones de euros.

b) Las infracciones muy graves, en función de sus circunstancias, podrán dar lugar a la inhabilitación hasta de cinco años del operador para la explotación de redes o la prestación de servicios de comunicaciones electrónicas.

Por la comisión de infracciones graves se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio, el límite máximo de la sanción será de 500.000 euros.

c) Las infracciones graves, en función de sus circunstancias, podrán llevar aparejada amonestación pública, con publicación en el Boletín Oficial del Estado y en dos periódicos de difusión nacional, una vez que la resolución sancionadora tenga carácter firme.

d) Por la comisión de infracciones leves se impondrá al infractor una multa por importe de hasta 30.000 euros.

Las infracciones leves, en función de sus circunstancias, podrán llevar aparejada una amonestación privada.

2. En todo caso, la cuantía de la sanción que se imponga, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, lo siguiente:

a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

En primer lugar, por la comisión de las *infracciones muy graves,* se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la

---

c) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

d) El daño causado.

Además, para la fijación de la sanción se tendrá en cuenta la situación económica del infractor, derivada de su patrimonio, de sus ingresos, de sus cargas familiares y de las demás circunstancias personales que acredite que le afectan.

El infractor vendrá obligado, en su caso, al pago de las tasas que hubiera debido satisfacer en el supuesto de haber realizado la notificación a que se refiere el artículo 6 o de haber disfrutado de título para la utilización del dominio público radioeléctrico.

3. Sin perjuicio de lo establecido en el apartado 1 de este artículo, el Ministerio de Ciencia y Tecnología o la Comisión del Mercado de las Telecomunicaciones, en el ámbito de sus respectivas competencias, podrán adoptar las siguientes medidas:

a) Las infracciones a las que se refieren los artículos 53 y 54 podrán dar lugar a la adopción de medidas cautelares, que de conformidad con el artículo 136 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrán consistir en el precintado y, en su caso, la retirada del mercado de los equipos o instalaciones que hubiera empleado el infractor por un plazo máximo de seis meses, y en la orden de cese inmediato de la actividad presuntamente infractora, siendo, en su caso, aplicable el régimen de ejecución subsidiaria previsto en el artículo 98 de dicha Ley.

b) Cuando el infractor carezca de título habilitante para la ocupación del dominio público o su equipo no haya evaluado su conformidad, se mantendrán las medidas cautelares previstas en el párrafo anterior hasta la resolución del procedimiento o hasta la evaluación de la conformidad.

c) Las sanciones impuestas por cualquiera de las infracciones comprendidas en los artículos 53 y 54, cuando se requiera título habilitante para el ejercicio de la actividad realizada por el infractor, podrán llevar aparejada, como sanción accesoria, el precintado o la incautación de los equipos o aparatos o la clausura de las instalaciones en tanto no se disponga del referido título.

d) Asimismo, podrá acordarse, como medida de aseguramiento de la eficacia de la resolución definitiva que se dicte, la suspensión provisional de la eficacia del título y la clausura provisional de las instalaciones, por un plazo máximo de seis meses.

4. Además de la sanción que corresponda imponer a los infractores, cuando se trate de una persona jurídica, se podrá imponer una multa de hasta 60.000 euros a sus representantes legales o a las personas que integran los órganos directivos que hayan intervenido en el acuerdo o decisión.

Quedan excluidas de la sanción aquellas personas que, formando parte de órganos colegiados de administración, no hubieran asistido a las reuniones o hubieran votado en contra o salvando su voto.

5. Las cuantías señaladas en este artículo podrán ser actualizadas por el Gobierno, teniendo en cuenta la variación de los índices de precios de consumo.

infracción. En caso de que no resulte posible aplicar este criterio, el límite máximo de la sanción es de dos millones de euros. Las infracciones muy graves, en función de sus circunstancias, pueden dar lugar a la inhabilitación hasta de cinco años del operador para la explotación de redes o la prestación de servicios de comunicaciones electrónicas.

En segundo lugar, por la comisión de *infracciones graves* se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o —en caso de que no resulte aplicable este criterio— el límite máximo de la sanción será de quinientos mil euros. Las *infracciones graves,* en función de sus circunstancias, pueden llevar aparejada amonestación pública, con publicación en el Boletín Oficial del Estado y en dos periódicos de difusión nacional, una vez que la resolución sancionadora tenga carácter firme.

49 Régimen transitorio

Antes de concluir el examen de las previsiones de la DAU, es preciso mencionar algunos aspectos relativos al establecimiento de un régimen transitorio específico respecto de la eficacia retroactiva de la norma y a su entrada en vigor. Así, en concreto, su apartado séptimo dispuso que la obligación de inscripción en el libro-registro de los datos identificativos de los compradores que adquieran tarjetas inteligentes, así como el resto de obligaciones contenidas en el precepto, comenzaría a ser exigibles a partir de la entrada en vigor de la LCD que, como indicamos, tuvo finalmente lugar el 8 de noviembre de 2007.

No obstante, por lo que se refería a las *tarjetas adquiridas con anterioridad a esta fecha,* la DAU previó que los operadores de telefonía móvil dispondrían de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las obligaciones de inscripción en el libro-registro, esto es: el 8 de noviembre de 2009. Transcurrido el plazo, los operadores estaban obligados a anular o a desactivar aquellas tarjetas de prepago respecto de las que no se hubiera podido cumplir con las obligaciones de

inscripción del apartado primero, sin perjuicio —añadía el apartado octavo— de la compensación que, en su caso, corresponda al titular de las mismas "por el saldo pendiente de consumo"[1190].

De esta manera, el resultado final es que, a día de hoy, las previsiones de la DAU se aplican plenamente a la totalidad de la telefonía de prepago adquirida en territorio español.

50 Valoración final

Sin duda, el contenido de la DAU puede conceptuarse como una de las disposiciones más importantes de la LCD, en la medida en que regula es la posibilidad de identificación de los sujetos que usan las tarjetas de telefonía de prepago, uno de los servicios de telecomunicaciones más demandados en nuestro país.

Quisiéramos añadir aquí una serie de consideraciones sobre la parcial consecución del propósito. Por una parte, conviene recordar que el anonimato emerge como una de las posibles —y legítimas— razones de la contratación del servicio de telefonía mediante tarjeta de prepago, por lo que la protección del derecho a que terceros no puedan acceder a la información sobre la persona adquirente de la tarjeta debía entenderse aún más incuestionable. Precisamente, la citada STS 130/2007, de 19 de febrero, habla de un *plus* de reserva en la protección constitucional de la información —o dato— sobre la identidad del titular de la tarjeta, "pues la relación de pertenencia a un determinado titular resulta desconocida incluso para el propio operador que dispensa el servicio"; plus de reserva que pierde su razón de ser tras la imposición legal del deber de registro.

[1190] El apartado 9 DAU del Anteproyecto determinaba que "la obligación de inscripción a que se refiere el apartado anterior no es de aplicación a las tarjetas actualmente existentes, inclusive en los supuestos de recarga de las mismas". Aparte de que su literalidad no era consistente con lo dispuesto en otros apartados del borrador, la cuestión más relevante radicaba en la vía que este apartado 9 ofrecía para escapar del control que con esta ley se quería establecer, mediante la adquisición de una tarjeta prepago antes de que resulten aplicables las medidas y obligaciones correspondientes. Finalmente la redacción final subsanó este defecto.

Indica acertadamente GONZÁLEZ LÓPEZ que la principal objeción que cabe realizar a este tipo de medidas es que constituye una agravación de la inindiciariedad que ya comporta la medida a que sirven instrumentalmente:

> "merced a un proceso en cadena ocasionado por la necesidad de asegurar la eficacia de la conservación de datos, la ausencia de indicios de comisión de hechos delictivos o de su previsible comisión no se limita a la medida originaria, sino que, consecuentemente, se proyecta a sus medidas instrumentales, que añaden nuevas restricciones al derecho a la protección de los datos de carácter personal sin contar, igualmente, con una base indiciaria que las justifique. Es decir, a fin de obtener la supuesta eficacia de la conservación generalizada de datos, en que se ha pretendido sustentar su necesidad, se incrementa la limitación indiscriminada de un derecho fundamental (al extender la conservación inindiciaria a nuevas categorías de datos de carácter personal) con carácter secundario y, por ende, aún más alejada de la finalidad perseguida (la prevención e investigación de delitos)"[1191].

Además, debe destacarse la absoluta divergencia respecto de la recomendación formulada por el GT29, de acuerdo con la cual no debe existir ninguna obligación de identificación en los casos en que la identificación no sea necesaria a efectos de facturación u otros fines en cumplimiento del contrato[1192]. En definitiva, "si rechazable resulta la conservación generalizada de datos, aún más lo es este elenco de medidas al servicio de la misma"[1193].

Por otra parte, resulta evidente que la finalidad perseguida por la DAU ha sido lograda parcialmente. Estamos ante una norma que resuelve un segmento muy concreto del espectro de posibilidades de navegación anónima a través de las redes de telecomunicaciones. Sin referirnos a las posibilidades de navegación por entornos de internet que garantizan el casi total anonimato del comunicante, en el campo mismo de las comunicaciones telefónicas clásicas nos enfrentamos a otras formas de atribución de números de abonado que escapan del control de identidad, como son las ya existentes atribuciones temporales, previo pago de determinadas cantidades, de líneas telefónicas sin utilizar el soporte físico de las tarjetas SIM. Así pues, quien busque el anonimato como forma de eludir el control previo de la conservación de datos simplemente habrá

[1191] Cf. González López, J. J., Comentarios a la Ley 25/2007…, op. cit. p.29.

[1192] Cf. Dictamen 4/2005, del GT29…, doc. cit., p. 10.

[1193] Cf. González López, J. J., Comentarios a la Ley 25/2007…, op. cit. p.29.

de adquirir productos distintos que garanticen la posibilidad de no ser identificado. La capacidad innovadora de las tecnologías de las comunicaciones y el interés de los operadores para hacerse con un tipo de clientes que ven en el anonimato la mejor garantía de unos derechos reconocidos en los arts. 18.1 y 18.4 CE, posiblemente conviertan a la norma en una rémora que sólo afecte los derechos de personas de escaso nivel económico o conocimiento de las posibilidades que ofrecen las tecnologías de la comunicación.

El legislador tal vez haya pecado de excesiva ingenuidad al no establecer una cláusula genérica que incluyera el concepto que ya se utiliza en la norma de servicios anónimos de pago por adelantado. De este modo, no sería de extrañar que la imposición de tal deber de registro posiblemente convierta a corto plazo esta regulación en un instrumento obsoleto, ante la inminente irrupción de otras formas de comunicación telefónica en las que no es necesaria la identificación del abonado[1194].

[1194] Ibíd.

CONCLUSIONES

Conclusiones de la Primera Parte. La conservación de datos en el Derecho de la Unión Europea.

I. Las circunstancias políticas y legislativas que rodearon la gestación de la DCD en el seno de la Unión Europea son particularmente relevantes para evaluar la necesidad y proporcionalidad de tal medida. La aprobación de la DCD es el resultado de un largo proceso en el que la Unión Europea fue tomando conciencia —en buena medida, empujada por los acontecimientos— de la relevancia que la conservación de datos presenta como instrumento para la represión de los delitos relacionados con el terrorismo internacional. Por otra parte, puede afirmarse que la DCD vino a enmarcarse dentro de la corriente de políticas legislativas antiterroristas que muchos Estados occidentales emprendieron como consecuencia de los atentados de Nueva York, Madrid y Londres en la primera década del siglo XXI. A partir de estos acontecimientos, algunos países desarrollados empezaron a mostrar una gran preocupación por la amenaza del terrorismo internacional y la seguridad nacional, prestando particular atención al ámbito de internet y las telecomunicaciones electrónicas como medios idóneos para la comisión de atentados. Fruto de esta alarma fue la aprobación de numerosas normas comunitarias sobre cooperación policial, judicial y penal. La interceptación de los datos de las telecomunicaciones pasó así en breve tiempo de considerarse un asunto de interés secundario —que ocupaba la atención principalmente de un reducido círculo de expertos en seguridad— a constituir una de las piezas claves de la política comunitaria en seguridad.

II. La tramitación de la DCD presenta un enorme interés para su estudio en profundidad. Esto se debe a que muchas de las polémicas jurídicas y políticas en torno a la Directiva, sus defectos y carencias, surgieron durante este período de preparación, dando origen a un intenso debate que se prolonga hasta nuestros días.

III. Sobre las razones que llevaron a la Comisión Europea a elegir la directiva como el concreto instrumento jurídico para regular la conservación de datos y

—correlativamente y como consecuencia— sobre el modo en que ésta viene a respetar la observancia del principio de subsidiariedad, cabe señalar que se optó por una medida del Primer Pilar por considerarse que ningún otro instrumento sería igualmente adecuado, así como porque la opción de una propuesta de directiva proporcionaba el nivel de armonización necesario en el mercado interior a nivel comunitario. La directiva dejaba suficiente margen a los Estados miembros para adaptarse a las exigencias nacionales.

IV. Las numerosas consultas y dictámenes emitidos durante la tramitación de la DCD pusieron de manifiesto, en primer lugar, el gran interés de las fuerzas y cuerpos de seguridad en la aprobación de la normativa, puesto que la conservación de los datos de las comunicaciones se consideraba una herramienta esencial para combatir la delincuencia y, particularmente, la amenaza del terrorismo. Por su parte, y en segundo lugar, las organizaciones europeas del sector de las telecomunicaciones no se opusieron a la proyectada legislación, pero abogaron por períodos de conservación no superiores a seis meses. Finalmente, en una tercera posición, las autoridades de protección de datos y las asociaciones de derechos civiles sostuvieron que la conservación de datos suponía una interferencia en la vida privada de los ciudadanos y que, por tanto, la finalidad y los objetivos de la conservación debían ser definidos con precisión.

La Propuesta elaborada por la Comisión quiso presentarse por parte de la misma como "un planteamiento equilibrado" a estas tres posiciones.

V. Los dictámenes emitidos sobre esta Propuesta de Directiva por parte del GT29, el SEPD, el Parlamento Europeo y del CESE pueden en general calificarse como una dura censura al texto proyectado, siendo la principal y común objeción el considerar que no tutelaba suficientemente los derechos fundamentales afectados por la medida. Algunas de estas críticas se tradujeron en enmiendas parlamentarias que contribuyeron a mejorar el texto finalmente aprobado, si bien otra porción de aquellas fueron obviadas y siguen resultando poderosos argumentos contra la vigente normativa. En este sentido, la difícil tramitación de la DCD no sirvió para armonizar todos los intereses en conflicto satisfactoriamente.

VI. La Directiva obliga a los Estados miembros a adoptar medidas para garantizar que un determinado conjunto de datos externos de las comunicaciones electrónicas sean conservados y se hallen disponibles durante un plazo de entre seis y veinticuatro meses para los fines de investigación, detección y enjuiciamiento de delitos graves, según lo definido por cada Estado miembro en su Derecho nacional. La necesidad de armonización a través de una directiva sobre la materia concernida venía dada por la urgencia de adoptar en el seno de la Unión disposiciones uniformes sobre aquella, ante la dispersión normativa en determinados casos, o la ausencia de regulación, en otros. Las grandes diferencias entre las disposiciones legislativas, reglamentarias y técnicas de cada Estado miembro en materia de conservación de datos de tráfico planteaban obstáculos ciertos para el mercado interior de las comunicaciones electrónicas, en la medida en que los prestadores de servicios se enfrentaban a requisitos diferentes en cuanto a los tipos de datos que debían conservarse. Esta falta de armonización dificultaba el intercambio de información entre las autoridades policiales de los Estados miembros.

VII. Con el paso del tiempo la transposición de la DCD ha revelado cómo lo que se entiende por delitos graves a la hora de legitimar el acceso a los datos varía ampliamente en las legislaciones nacionales de cada país de la Unión. La pretendida armonización ha sido un notable fracaso en este importante aspecto. En los momentos actuales, cada país permite la cesión de datos de acuerdo con finalidades penales completamente divergentes. Como es natural, tales contrastes han perjudicado el volumen y la frecuencia de las solicitudes de cesión de datos entre Estados miembros —un objetivo también perseguido por la Comisión— e, incluso, incrementado los costes generados para las compañías de telecomunicaciones por el cumplimiento de las obligaciones establecidas en la DCD.

VIII. El fracaso de la armonización se extiende también al ámbito subjetivo de la Directiva. El art. 1.1 DCD indica quiénes son los sujetos obligados por la norma, esto es, los operadores que deben cumplir la obligación de conservación de datos, describiéndolos como “los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones”. A la hora de la transposición de la Directiva en los ordenamientos de los diferentes Estados, la concreción de cuáles

son los proveedores concretamente afectados por la norma ha dado lugar una vez más a una indeseable disparidad de criterios. Las disparidades entre las legislaciones nacionales sobre qué operadores están o no obligados conlleva necesariamente discriminaciones en el marco del mercado único.

IX. La obligación de conservar los datos externos de las comunicaciones electrónicas constituye el núcleo de la normativa en estudio, al tiempo que se presenta como una amplísima excepción a los arts. 5, 6 y 9 de la directiva sobre la privacidad y las comunicaciones electrónicas, que consagraron unas firmes garantías de privacidad a favor de los usuarios de las comunicaciones electrónicas. El resultado es la inversión de la situación legislativa: en la práctica, la excepción pasa a ser la regla general.

X. El apartado 5.1 DCD agrupa los datos a retener en seis categorías, dentro de cada cual se especifican los datos que deben ser retenidos. Estas categorías establecidas en la Directiva deben interpretarse como una relación *numerus clausus*, por lo que no permite imponer a los operadores obligaciones adicionales de conservación de datos. La lista exhaustiva de las categorías de los datos del art. 5 DCD ha sido uno de los puntos de la regulación en los que se ha alcanzado un alto nivel de armonización.

XI. El período de conservación de los datos obtenidos sigue siendo uno de los puntos más discutidos de la DCD, tanto más cuanto que guarda directa relación con la proporcionalidad de las medidas de conservación adoptadas y, consecuentemente, con su legalidad. Los debates sobre la idoneidad de este plazo ordinario de conservación giran en torno a dos intereses contrapuestos. Nos hallamos, por un lado, ante la pretensión de las autoridades represivas de garantizar un período suficientemente amplio para llevar a cabo sus investigaciones con la mayor expectativa posible de éxito y, por el otro, la de los titulares de los datos y de las empresas de telecomunicaciones de que los plazos sean lo más breves posible, con el fin de que reducir la injerencia en el derecho a la intimidad y los costes de almacenamiento, respectivamente. La transposición de la Directiva en los Estados miembros ha puesto de manifiesto que unos márgenes tan amplios —que pueden variar hasta en dieciocho meses— son claramente inidóneos para alcanzar la finalidad de armonización

pretendida por la norma. Una vez transpuesta la DCD, se constanta que los Estados miembros aplican períodos de conservación que varían considerablemente entre sí, aun hallándose dentro de los límites del art. 6 DCD.

XII. En relación con los plazos, resulta criticable la previsión del art. 12 DCD, que prevé que todo Estado miembro que deba hacer frente a "circunstancias especiales" que "justifiquen una ampliación limitada del período máximo de conservación recogido en el artículo 6" —dos años— podrá adoptar las medidas "que se impongan" (*sic*). Por la vía del art. 12 DCD se confiere a los Estados unas prerrogativas que abren la puerta a ampliar aún más las facultades de retención previstas originalmente. Nos encontramos sin duda ante una de las previsiones más censurables de la DCD, tanto por los problemas de interpretación que presenta como por su dudosa legalidad. A la expectativa de un pronunciamiento del TJUE que pueda eventualmente anular su contenido, creemos que el hecho de que no se haya puesto nunca en práctica ha mantenido esta disposición al margen de mayores polémicas.

XIII. Otro de los puntos más criticables de la DCD es el referente al modo en que ésta regula las medidas de protección y seguridad para los datos conservados, cuyo régimen se contiene en los arts. 7 y 8 DCD. Su análisis demuestra cómo lo que realmente ha guiado la redacción de la DCD por parte de la Comisión Europea no es la protección de la privacidad —que debería ser de prioridad absoluta— sino, por el contrario, el que las medidas de cesión de los datos conservados se apliquen eficazmente. La transposición y aplicación de la DCD ha puesto en evidencia el resultado de una regulación marcada por la desidia y por una defectuosa técnica legislativa en lo que se refiere a la protección de datos. Sólo quince países han transpuesto todos estos principios en la legislación pertinente.

XIV. El art. 4 DCD, bajo la rúbrica de "acceso a los datos", dispone que los Estados miembros deben adoptar medidas para garantizar que los datos conservados de conformidad con la Directiva solamente se accedan de acuerdo con tres condiciones concurrentes: 1) que se proporcionen a las autoridades nacionales competentes; 2) en casos específicos, y 3) de conformidad con la legislación nacional.

XV. En lo que se refiere a las "autoridades nacionales competentes", la principal crítica se centra en la excesiva vaguedad del término para evitar divergencias en su interpretación. La remisión a tales autoridades resultaba excesivamente genérica. Las graves omisiones del art. 4 DCD sobre las condiciones de acceso han hecho sentir sus consecuencias en la forma en que los Estados miembros han incorporado las previsiones a su legislación interna, causando el correlativo perjuicio a los objetivos de armonización en la materia. Los regímenes de acceso a los datos presentan la mayor variedad imaginable, en una escala que oscila desde aquellos países que sólo confían el acceso a la autoridad judicial bajo firmes garantías procesales hasta aquellos que autorizan el acceso a una panoplia de órganos policiales, judiciales y administrativos bajo requisitos de mero trámite. Ante tal disparidad, no puede sino afimarse que la DCD ha vuelto a fracasar en su pretensión armonizadora.

De cara a una eventual reforma, debería hacerse constar expresamente que sólo podrán proporcionarse los datos almacenados a unas autoridades que garantizasen la calidad, la confidencialidad y la seguridad de los datos obtenidos así como que el acceso a los datos se autorizase en todos los supuestos por una autoridad judicial o bajo supervisión independiente.

XVI. El art. 10 DCD establece el deber para los Estados miembros de facilitar cada año a la Comisión Europea las estadísticas sobre la conservación de datos *generados o tratados* en el marco de la prestación de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones. No deja de resultar parádojico que el fracaso de armonización de la norma se haya extendido también a esta tarea de evaluación. En el cumplimiento de la previsión legal, la Comisión Europea pidió a los Estados miembros que facilitasen información detallada sobre los casos de solicitudes individuales de datos. Sin embargo, como la propia institución reconoció, las estadísticas proporcionadas diferían ampliamente en alcance y detalle.

XVII. El grave impacto que la regulación de la DCD produce en la normativa comunitaria en materia de protección de datos de las comunicaciones electrónicas ha forzado a la propia DCD a incluir entre sus previsiones un artículo con el que se

pretende recomponer la armonía hasta entonces presente en este sector del ordenamiento. En concreto, el art. 11 DCD dispone la modificación de la directiva sobre privacidad y comunicaciones electrónicas, añadiendo un apartado 1.*bis* en el art. 15 de la misma.

La principal crítica que puede formularse a la modificación que lleva a cabo el art. 11 DCD es su insuficiencia. Dado que la DCD priva a la Directiva 2002/58/CE de una buena parte de su contenido y eficacia, la relación entre ambas debería haber sido aclarada con mayor detalle. En concreto, creemos que habría sido mejor suprimir las referencias en el artículo 15.1 al artículo 6 y al artículo 9 de esa misma directiva, o por lo menos modificarlas para aclarar que los Estados miembros ya no son competentes para adoptar legislación en relación con infracciones penales. En definitiva, habría sido conveniente eliminar toda ambigüedad en sus competencias restantes, por ejemplo por lo que se refiere a la retención de datos a efectos de infracciones penales "no graves". Nos encontramos ante otra de las grandes fallas de la DCD, cuyas consecuencias en este concreto punto extienden sus efectos a la totalidad del ámbito en que se enmarca su regulación.

XVIII. Respecto de la previsión conforme a la cual la DCD había de transponerse por los Estados miembros a más tardar el 15 de septiembre de 2007, hemos de destacar que tal plazo resultaba demasiado breve, sobre todo si tenemos en cuenta la complejidad de la materia en presencia. No hay mejor prueba de esta insuficiencia que el hecho de que dieciséis de los veinticinco Estados miembros establecieron, en el momento de adopción de la Directiva, excepciones conforme al art. 15.3 DCD para retrasar dieciocho meses la transposición en lo referido a la conservación de los datos de comunicaciones de acceso a internet, telefonía por internet y el correo electrónico.

XIX. El cumplimiento de las prescripciones de la Directiva comporta una notable carga económica para los proveedores de servicios de comunicaciones electrónicas, sin que tales gastos supongan beneficio alguno para estas compañías. Aunque el vigente articulado de la DCD no prevea ningún tipo de compensación económica, descargar sobre los operadores la totalidad de los costes comportaría consecuencias negativas. En primer lugar, puede suponer el que las medidas de

seguridad no estén siendo todo lo apropiadas y necesarias que deberían, para ahorrar gastos. En segundo lugar, el incremento de los costes para las empresas de telecomunicaciones está siendo finalmente repercutido contra los propios usuarios europeos.

XX. La transposición de la DCD ha sido *problemática* e *insatisfactoria*. El aspecto problemático del proceso se pone de manifiesto en el hecho de que, a fecha de junio de 2011, la legislación de transposición sólo estaba en vigor en veintitrés de los veintisiete Estados miembros; un Estado aún tiene que transponerla —Suecia— y otros tres han visto su legislación de transposición anulada por sus tribunales constitucionales —Alemania, República Checa y Rumanía—. Aparte de estas sentencias, la transposición de la DCD ha dado lugar adicionalmente al pronunciamiento de otros tribunales constitucionales, sin graves consecuencias ulteriores. Tal es el caso de Bulgaria, cuya ley de transposición hubo de revisarse; Chipre, donde se consideró que las resoluciones judiciales dictadas con arreglo a la ley transposición eran inconstitucionales; y Hungría, donde está pendiente un asunto relativo a la omisión de los fines legales del tratamiento de datos en la legislación de transposición.

Ante la alta litigiosidad que a la que la DCD ha dado lugar, no es de extrañar que la propia Comisión Europea —en su Informe de Evaluación de 2011— haya manifestado su *voluntad* de estudiar todos los aspectos problemáticos apuntados por las jurisdicciones constitucionales en su futura propuesta para revisar el marco de la conservación de datos. En cualquier caso, la incesante actividad jurisdiccional —a nivel comunitario y estatal— originada en torno a la DCD es probablemente la mejor prueba de la existencia de numerosos defectos en el texto en vigor, lo que nos lleva de la mano a la otra nota que predicábamos acerca de la transposición, a saber: su carácter insatisfactorio.

XXI. La transposición puede calificarse de insatisfactoria en la medida en que, como ha reconocido la propia Comisión, la DCD no ha armonizado plenamente el enfoque en cuanto a la conservación de datos y no ha creado unas condiciones equitativas para los operadores. Se constata la existencia de considerables diferencias entre las legislaciones de transposición en relevantes aspectos, tales como la limitación

de la finalidad de la conservación, el acceso y la seguridad de los datos, los períodos de almacenamiento y la fiabilidad de las estadísticas recabadas.

XXII. Si bien es cierto que la DCD ha dado lugar a que en casi todos los países de la Unión exista una normativa que impone medidas de conservación de datos de las comunicaciones electrónicas, no lo es menos que el resultado ha sido que buena parte de estas normativas presentan serias fallas que ponen en riesgo, cuando no vulneran claramente, la adecuada protección de los derechos fundamentales. La propia Comisión ha reconocido que la Directiva no garantiza por sí misma que los datos conservados se almacenen, recuperen y utilicen con pleno respeto del derecho a la intimidad y la protección de los datos personales. No obstante, la institución ha querido descargar en cierta medida su tanto de culpa por estos resultados al afirmar que la responsabilidad de garantizar estos derechos corresponde a los Estados miembros así como que la Directiva sólo busca una armonización parcial de los enfoques sobre conservación de datos.

En todo caso, los defectos e insuficiencias que hemos puesto de manifiesto a lo largo de este análisis del articulado explican que, a la hora de la transposición, no exista un enfoque común ni respecto de disposiciones específicas de la Directiva —como la limitación de las finalidades o los períodos de conservación— ni respecto de aspectos no incluidos en su ámbito de aplicación, como el reembolso de los gastos. Más allá del grado de variación previsto expresamente por la DCD, las diferencias en la aplicación nacional de la conservación de datos han presentado considerables riesgos para los ciudadanos europeos, así como dificultades para los operadores.

Conclusiones de la Segunda Parte. Derechos fundamentales en la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos.

XXIII. Ya desde su primera hora, la regulación examinada ha sido objeto de disputa acerca de si su contenido vulnera derechos fundamentales tales como la protección de datos, la intimidad o el secreto de las comunicaciones. La legalidad de la DCD queda condicionada a que sus previsiones sean compatibles con la CDF, que en virtud del art. 6 TUE ha pasado a formar parte del denominado Derecho primario de la

Unión Europea. Cualquier norma o acto perteneciente al Derecho secundario —entre ellas, las directivas— deben ser conformes al contenido de la Carta so pena de su nulidad. aquel texto.

XXIV. Existe un acuerdo general en que el contenido de la DCD supone una limitación de ciertos ámbitos de libertad que los individuos poseen en un sistema democrático. La propia Comisión Europea así lo reconoció al presentar la Propuesta de Directiva, si bien aseveró que las limitaciones de estos derechos eran proporcionadas y necesarias para alcanzar los objetivos generalmente reconocidos de prevenir y combatir la delincuencia y el terrorismo. Algunas de las instituciones que durante la tramitación de la DCD emitieron dictamen —en particular, el CESE, el GT29 y el SEPD—, se mostraron muy críticos con el tratamiento dado en la norma a los derechos fundamentales en lo que respecta particularmente a la protección de datos de carácter personal (art. 8 CDF) y el respeto de la vida privada y familiar (art. 7 CDF). De todas estas declaraciones se concluye que existe un acuerdo general en cuanto al reconocimiento del hecho de que buena parte de las medidas contenidas en la DCD sí suponen una relevante limitación de ciertos derechos fundamentales.

XXV. Concretamente, el hecho de que la medida de conservación de datos impuesta por la norma constituye una limitación del derecho a la intimidad y al secreto de las comunicaciones (arts. 7 y 8 CDF) ha sido reconocido por la propia Comisión Europea tanto en el Preámbulo de la DCD como en el Informe de Evaluación, al tiempo que había sido subrayado por diversos órganos dictaminantes. La DCD tiene un impacto directo sobre la protección a la intimidad si se contempla desde la jurisprudencia del TEDH, que ha considerado que el almacenamiento de información sobre un individuo es una injerencia en la vida privada, incluso aunque no contuviera ningún dato sensible.

XXVI. En lo referido al secreto de las comunicaciones, la jurisprudencia del TEDH reconoce expresamente la posibilidad de que tal derecho pueda resultar violado por el empleo de un artificio técnico que permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma.

XXVII. Además del derecho a la intimidad, la DCD también supone una incisiva afectación del derecho fundamental a la protección de datos, el grupo de garantías protectoras de la intimidad recogidas ahora el art. 8 CDF y el art. 16 TFUE.

XXVIII. Aparentemente, las disposiciones de la DCD pretendieron respetar y enmarcarse en esta sólida red de normas y garantías legales que tradicionalmente ha rodeado el derecho a la protección de datos, si bien a la postre la Directiva sigue teniendo un impacto enorme sobre estos principios reconocidos por el Derecho comunitario. Los datos se retienen durante un plazo mucho más largo que los plazos que son habituales para la retención por los proveedores de servicios de las comunicaciones electrónicas públicamente disponibles o por una red de comunicaciones públicas, llegando a alcanzar los veinticuatro meses. Por otra parte, mientras la Directiva 2002/58/CE garantiza la seguridad y la confidencialidad, la introducción por la DCD de la obligación de retener datos se traduce en la creación de bases de datos sustanciales que conlleva riesgos particulares para los titulares de esos datos. Tal normativa corre el riesgo de permitir las denominadas "fishing expeditions", esto es, investigaciones policiales completamente aleatorias en las que los investigadores revisan documentación y cualesquiera enseres personales sin tener claro el tipo de prueba que buscan o el crimen que persiguen.

XXIX. Expuesta y demostrada en los términos anteriores la manera en que la obligación de conservación y el deber de cesión de los datos retenidos establecidos por la DCD constituye una limitación del derecho a la intimidad y la protección de los datos personales, resta examinar si tal afectación es o no legítima, esto es, si se produce dentro de los límites autorizados por el Derecho europeo.

XXX. Tanto el art. 52.1 CDF como la jurisprudencia del TEDH y del TJUE han especificado en qué casos y bajo que condiciones resulta admisible una injerencia de la autoridad pública en el ejercicio de los derechos fundamentales. En concreto, cualquier limitación debe, en primer lugar, la medida, aun persiguiendo un fin de interés público, debe estar *establecida por la ley* y expresada de una manera precisa, de modo que provea convenientemente contra la acción arbitraria del poder público y dé a

conocer a los ciudadanos la posibilidad de injerencias en su esfera de libertades. En segundo lugar, la finalidad de la interferencia debe ser *legítima*, es decir, debe ser necesaria para alcanzar un objetivo de interés general o para proteger los derechos y libertades de otros y estar relacionada con alguna de las categorías reconocidas en el art. 8 CEDH: "que 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". En tercer lugar, la injerencia en los derechos debe ser proporcional al objetivo perseguido y ajustarse al contenido esencial de los derechos fundamentales en cuestión. La proporcionalidad se concreta a su vez en dos elementos: a) la búsqueda de medios alternativos, menos agresivos, para alcanzar el fin propuesto; y, b) una ponderación de la importancia del derecho en cuestión en comparación con la finalidad pública que se persigue. Si el derecho es suficientemente importante y hay medios alternativos de alcanzar el fin público, no se podrá apreciar la proporcionalidad.

XXXI. El requisito de la previsión legal se desdobla en dos vertientes. Por un lado, la cuestión de la base legal empleada por la Unión para aprobar la norma; por otro, el de la calidad de la norma aprobada. Analizado desde ambas vertientes, no cabe sino concluir que las medidas limitadores de derechos introducidas por la DCD cumplen satisfactoriamente con el requisito de previsión legal requerido en el marco de la Unión Europea.

XXXII. En cuanto a la calidad para aprobar la DCD, debe subrayarse que, en lo que se refiere al requisito del art. 52.1 CDF y del art. 8 CEDH, lo cierto es que cualquier norma comunitaria o nacional sería satisfactoria en tanto que fuera precisa, previsible y accesible al público. Aplicado estos parámetros a la DCD, se comprueba que nuestra norma regula con suficiente previsión todos los aspectos relativos a la medida impuesta, al fijar su "objetivo y ámbito" (art. 1 DCD), las definiciones de los conceptos que emplea (art. 2 DCD), la propia "obligación de conservar datos" (art. 3 DCD), el "acceso a los datos" (art. 4 DCD), las "categorías de datos que deben conservarse" (art. 5 DCD), los "períodos de conservación" (art. 6 DCD), la "protección y seguridad de los datos" (art. 7 DCD), los "requisitos de almacenamiento para los datos conservados" (art. 8 DCD) y otros tantos aspectos de la medida de conservación,

en abundancia suficiente para superar el canon de calidad impuesto por la jurisprudencia del TEDH.

XXXIII. Respecto de la cuestión de la base legal, ha de decirse que el contenido de la DCD reemplazaría a las normas nacionales divergentes, al especificar las circunstancias conforme a las cuales los proveedores eran requeridos a conservar los datos con fines de perseguir delitos. Cualquier interferencia, incluida la retención y uso de los datos de tráfico para ayudar a las investigaciones penales, tenía que ser autorizada por la ley y así se ha producido.

XXXIV. Pasando a la siguiente condición, para satisfacer las exigencias del art. 8 CEDH, la medida objeto de nuestro estudio debe necesariamente perseguir una finalidad legítima. Al respecto, hemos de indicar que el art. 1.1 DCD establece como fin de la conservación de datos su disponibilidad en el contexto de la investigación, detección y enjuiciamiento de delitos graves, entendiendo por éstos los que se definan en la legislación nacional de cada Estado miembro. El art. 82 TFUE y siguientes otorgan a la Unión Europea competencias en materia de cooperacion judicial en asuntos penales, entre las cuales la investigación, detección y enjuiciamiento de delitos graves del art. 1 DCD es sin duda un objetivo de interés general reconocido por la Unión (art. 52.1 CDF), tal como requiere el juicio de proporcionalidad.

XXXV. Antes de abordar la proporcionalidad *stricto sensu*, hemos de hacer brevísima referencia a otros dos parámetros que, en el caso de la DCD, resultan poco relevantes por ser fácilmente determinables: los criterios de necesidad y adecuación.

El requisito de adecuación sólo requiere que la medida no sea manifiestamente inadecuada, tal como una sólida línea jurisprudencial del TEDH pone de manifiesto. Aplicado a nuestro caso, la conservacion de datos, tal como está regulada por la DCD, es adecuada para lograr el objetivo expresado en el art. 1.1 DCD, pues resulta evidente que la misma resulta útil para su consecución.

En cuanto al requisito de necesidad de la medida, la conservación de datos sólo puede ser considerada necesaria si se trata de la medida menos invasiva disponible de entre las que existan para lograr el objetivo expresado en el art. 1.1 DCD, que es la

"investigación, detección y enjuiciamiento de delitos graves". De los tres fines, es el primero —la detección— el que permite a la DCD pasar con éxito el test de necesidad. Mientras la intervención de las telecomunicaciones de concretos sospechosos o los procedimientos "quick freeze", podrían ser suficientes para la investigación y el enjuiciamiento de delitos graves, los mismos no son alternativas adecuadas para la detección de estos delitos, ya que estos dos procedimientos requieren que el delito o al menos un potencial perpetrador haya sido ya detectado. Así pues, la detección de delitos graves hace que las medidas de conservación de la DCD puedan ser calificadas como "necesarias" a efectos del test de legalidad.

XXXVI. Es un principio general del Derecho europeo que toda limitación de un derecho fundamental debe ser proporcionada al interés general, necesaria y respetuosa de unas garantías mínimas. Cuando el derecho implicado es —como en este caso— la protección de datos, tal juicio se guía por las más específicas garantías de la referida Convención 108. En todo caso, las implicaciones del principio de proporcionalidad sólo pueden ser evaluadas a la luz de sus concretas manifestaciones, que, en lo que a la DCD se refiere, se concretan a nuestro entender en tres aspectos: la proporcionalidad de la medida de conservación generalizada de datos, los plazos de su conservación y el conjunto de la información que ha de retenerse.

XXXVII. Las razones que justifican la proporcionalidad de la DCD están sujetas a los más diversos cambios, dado que la medida se ordena a perseguir delitos en un ámbito en constante evolución como es el tecnológico. La introducción de medios de vigilancia general de los ciudadanos puede dar lugar a estrategias por parte del terrorismo y de la delincuencia organizada para no utilizar ciertos medios. Esto daría lugar a la necesidad de desarrollar nuevos métodos de vigilancia aún más estrictos, iniciándose así una espiral de posibles infracciones de los derechos fundamentales de los ciudadanos que sería difícil detener, al tiempo que cambiaría el carácter de la sociedad que tratamos de proteger. De ahí la necesidad de que las consideraciones de proporcionalidad deban al menos evaluarse periódicamente y publicarse los resultados.

XXXVIII. Otro de los aspectos más controvertido del debate sobre la proporcionalidad de la DCD se halla tanto en el período de conservación como en la cantidad de datos a ser retenidos. En cuanto al primero, el plazo de conservación de los datos se encuentra

estrechamente vinculado a la propia medida de conservación y plantea la necesidad de ponderación entre la finalidad perseguida —el aseguramiento de la eventual puesta a disposición de los datos conservados, cediéndolos a los agentes facultados— y el gravamen que para el derecho a la protección de los datos de carácter personal supone la prolongación en el tiempo del tratamiento de los datos. Si bien podrían parecer más justificadas las previsiones de distintos plazos de conservación en virtud de la finalidad a que se adscriba la cesión —vg. represión de delitos sin especificaciones o represión de delitos concretos especialmente graves— no ha sido el caso de la DCD. En todo caso, de acuerdo con las argumentaciones esgrimidas al respecto durante la tramitación de la DCD, el mejor parámetro de la proporcionalidad de los períodos máximos para la conservación obligatoria y general de los datos marcados en la DCD sólo puede venir dado que una justificación precisa de los mismos y respaldada claramente con pruebas.

XXXIX.En cuanto a la proporcionalidad de las medidas de la DCD en lo que se refiere a las categorías de datos que han de ser retenidos, la selección de los mismos no es una decisión neutra. Informaciones tales como la identidad de los emisores y receptores de las comunicaciones, la duración y frecuencia de éstas, la localización física, etc. son elementos que invaden la vida privada de las personas y, en muchos casos, también pueden dañar otros derechos como el secreto profesional o la asistencia jurídica debida, por lo que su selección por el legislador y, posteriormente, por el Juez, debe someterse a una razonado test de proporcionalidad, en atención a las circunstancias generales y específicas concurrentes.

XL. Por lo que respecta a la selección hecha en abstracto por el legislador europeo, debe criticarse el que la lista de datos a retener sea una lista cerrada y obligatoria en cada uno de sus puntos, en lugar de una de máximos de la cual los Estados pudieran exonerar aquellos que tengan a bien.

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

XLI. El deber general de conservación de datos del tráfico electrónico no es completamente novedoso en nuestro Derecho nacional, pues ya el art. 12 LSSI previó un régimen similar que no llegó a entrar en vigor por falta del necesario desarrollo reglamentario.

XLII. El contenido de la LCD ubica la norma, por una parte, dentro del Derecho de las telecomunicaciones —en tanto que establece un conjunto de obligaciones jurídico-públicas que los operadores deben cumplir—, y, por el otro, del Derecho procesal penal, dado que tales obligaciones se ordenan a la persecución y enjuicimiento de delitos graves. El resultado es una normativa de Derecho público que podría comportar una grave afectación de derechos fundamentales de creciente relevancia en nuestros días.

XLIII. La aprobación de la LCD supuso la irrupción de una amplia e incisiva excepción a todas las previsiones que concretaban el principio general de libre disposición de los datos por parte de los abonados contemplado en la LGT. La gravedad de esta excepción llevó al legislador a añadir a través de la Disposición Final Primera, apartado segundo de la LCD, un nuevo párrafo al art. 38.5 LGT, que ahora advierte que lo establecido en las dichas letras —a) y d) del apartado 3— se entiende sin perjuicio de las obligaciones establecidas en la LCD.

XLIV. Desde la perspectiva del Derecho procesal penal, hemos de destacar que el legislador español ha mostrado tradicionalmente cierta reticencia o falta de disposición al establecimiento de una regulación pormenorizada de la injerencia sobre contenidos de comunicaciones, incluso con anterioridad a la era digital. España ha ido siempre a remolque bien de las iniciativas, bien de las imposiciones de la Unión Europea y su prolija regulación del sector de las telecomunicaciones. Al menos, eso sí, nuestro legislador ha sabido dar buen uso al amparo ofrecido por una legislación comunitaria muy preocupada por los riesgos del anonimato en las redes de telecomunicaciones y la potencialidad de ser instrumento idóneo para la realización de actividades criminales a través de la red.

XLV. La preparación de la transposición de la DCD fue llevada a cabo por parte del Gobierno español sin el cuidado y precisión necesarios, siendo las principales faltas el que en el expediente del Anteproyecto no figuraban la totalidad de alegaciones presentadas por el sector, así como que no se dejara constancia en el expediente de las razones que llevaron al órgano instructor a aceptar o rechazar en cada caso las propuestas, sugerencias y observaciones formuladas por los distintos órganos y entidades que habían emitido su parecer sobre el Anteproyecto. La memoria justificativa se limitó a hacer una rápida referencia, de carácter general, a la necesidad y oportunidad del Anteproyecto, en función de la necesaria incorporación de la DCD, sin detenerse a explicar las razones que llevaron a adoptar una concreta solución frente a otras posibles.

XLVI. También es criticable en el expediente remitido por el Gobierno a las Cortes la ausencia de datos relativos a los efectos económicos que las medidas previstas habían de tener sobre los sujetos obligados. Aunque en la memoria económica se incluyó un tercer epígrafe sobre la incidencia económica sobre el sector, su contenido se reducía a distinguir entre los costes de adaptaciones técnicas y los de actividades administrativas —sin cuantificar unos ni otros— y a concluir que se tendría en consideración la necesaria proporción entre los objetivos a conseguir y los costes en que se incurra. Es claro que para que las Cortes Generales pudieran haber tenido en cuenta la proporción que existe entre una determinada exigencia y el coste que habría de tener para los sujetos obligados —con eventual repercusión en los usuarios finales—, las Cortes deberían haber contado con una información económica más detallada.

XLVII. La medida central de la LCD viene a configurarse como lo que se ha dado en denominar "conservación generalizada de datos", puesto que opera cuando la comisión delictiva es meramente hipotética y no consta sospecha inicial ni indicio alguno. De lo que se trata es de "congelar" datos que, una vez archivados, podrán ser elevados a la categoría de fuentes de prueba aunque eso suceda únicamente en un porcentaje infinitesimal de ocasiones. Tal tipo de herramientas supone una quiebra para el monopolio estatal de la persecución del delito, al tratarse de la "externalización" —outsourcing— de partes esenciales de la tarea de prevenir y perseguir el delito que comporta la obligación de conservación impuesta a los operadores.

XLVIII. En el caso español, el concreto instrumento legal configurado en la LCD presenta dos finalidades, una inmediata y otra mediata. La primera consiste en el deber para los operadores de conservar las categorías de datos enunciadas en la Ley, que opera como presupuesto de la finalidad mediata, a la que también alude el artículo 1.1 LCD: la eventual cesión a los agentes facultados con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

XLIX. El concepto de delito grave manejado por el art. 1.1 LCD no puede ser objeto de una interpretación literal ex arts. 13.1 y 33.2 del vigente Código Penal. En primer lugar, tal interpretación es insuficiente porque nos llevaría a usar las medidas de la LCD sólo para perseguir aquellos delitos castigados con penas superiores a cinco años de prisión, en tanto quedaría prohibida su aplicación en campos de la investigación criminal ciertamente idóneos, tales como la posesión y difusión de pornografía infantil, el tráfico de sustancias estupefacientes que no causaran grave daño a la salud, los delitos contra el patrimonio de cierta trascendencia social —piénsese en los atracos a bancos, etc.—, la protección del patrimonio histórico, etc.

En segundo lugar, el recurso estricto a lo dispuesto en los arts. 13.1 y 33.2 CP resulta claramente inadecuado en tanto que nos hace aplicar un criterio arbitrario para saber cuándo las herramientas de la LCD pueden ser empleadas. La razón efectiva por la que el actual sistema penal español considera como delitos graves los castigados con penas superiores a cinco años no depende de la gravedad sustantiva de los hechos, sino que —de acuerdo con la explicación que nos da la Exposición de Motivos de la Ley Orgánica 15/2003, de 25 de noviembre— el motivo por el cual el legislador ha fijado el parámetro en la prisión superior a cinco años descansa en la voluntad del legislador de diferenciar los delitos cuyo enjuiciamiento corresponde a las Audiencias Provinciales frente a los que competen a los Juzgados de lo Penal. Si el legislador optó definitivamente por el camino fácil, esto es, por trasladar la voz delito grave utilizada en la Directiva 2006/20/CE, es obvio que no pretendía establecer una relación directa, racional y excluyente entre las medidas de investigación provistas por la LCD y los delitos que son de conocimiento exclusivo de las Audiencias Provinciales o de la Sala de lo Penal de la Audiencia Nacional. Admitir lo contrario resultaría

bastante paradójico, toda vez que los restantes delitos "no graves", incluidos parte de los delitos contra la salud pública, y en general delitos relacionados con el crimen organizado —vg. tráfico de inmigrantes, contrabando— o que emplean la red para su expansión o garantía de la impunidad de sus autores —vg. difusión de pornografía infantil, estafas vía telemática, etc.—, y que pueden sin ningún género de duda ser objeto de una plena interceptación de los contenidos de comunicaciones, quedan prácticamente excluidos del recurso a la interceptación de los datos de tráfico conservados en virtud de la LCD. En consecuencia, el criterio de la estricta literalidad para interpretar qué ha de entenderse por "delito grave" conforme al art. 1.1 LCD no cabe sino ser rechazado.

L. Del examen del art. 3 LDC se constata que el listado de datos que han de ser objeto de conservación es casi una fiel transcripción del art. 5 de la norma comunitaria, de la que solamente difiere en pequeñas modificaciones de finalidad aparentemente didáctica o de simple redundancia.

LI. La LCD abandona con esta regulación el clásico concepto de dato de tráfico al que trasciende por dos frentes. En primer lugar, el abandono de la idea de dato de tráfico como elemento *dinámico*, en el sentido de su captación en el curso de una comunicación intervenida judicialmente: el legislador no diferencia entre el dato de tráfico captado conforme se está generando y el dato de tráfico almacenado como dato de carácter personal. En segundo lugar, la LCD utiliza un amplio concepto de dato, que incide no solamente en los componentes esenciales del dato de tráfico —terminales conectados, identificación de los usuarios y datación de la comunicación—, sino también en los que por regla general no serían sino servicios de valor añadido —en concreto, la localización del usuario— cuando tal localización no fuera indispensable para el buen fin de la comunicación o a efectos de su facturación, así como en relación con una serie de datos tendentes a perfilar la persona física o jurídica titular o usuaria del servicio. Los datos de tráfico clásicos se entremezclan así con datos de carácter personal ajenos a éstos, sometiéndose unos y otros al mismo régimen jurídico en tanto en cuanto son objeto de almacenamiento para su eventual utilización ulterior.

LII. Otro aspecto relevante del listado del art. 3 LCD es el apartamiento u olvido por parte del legislador español de la doble dimensión formal y material que la jurisprudencia constitucional constata en el contenido de cada comunicación. La ausencia de esta distinción puede plantear dificultades, como en el caso de los datos de localización geográfica, cuya adscripción a uno u otro tipo de contenido es suceptible de variar. La necesidad de minimizar estos eventuales problemas es lo que invita a que la relación de datos a retener del art. 3 LCD deba considerarse taxativa, sin que quepa su aplicación flexible o analógica.

LIII. El deber general para los operadores obligados de conservar los datos procedentes de las comunicaciones electrónicas (art. 4 LCD), supone una incisiva excepción a los principios generales del Derecho de las telecomunicaciones reflejados en el ya tratado Cap. III del Tít. III de la LGT que, para proteger los derechos a la intimidad, la protección de datos de carácter personal y el secreto de las comunicaciones, sustrae a los proveedores la facultad de disponer de estos datos a su voluntad, sometiendo cualquier tratamiento al consentimiento previo e informado del cliente, y de igual modo, consagra el derecho a que se hagan anónimos o se cancelen cuando ya no sean necesarios a los efectos de la transmisión de una comunicación.

LIV. El legislador ha apostado decididamente por la implicación de los operadores de telecomunicaciones en su deber de colaboración con la investigación criminal, imponiéndoles un complejo y costoso deber de facilitación de medios tecnológicos y humanos en las labores de almacenamiento y facilitación de información sobre comunicaciones. Aquí radica precisamente y en buena medida el mérito de la Ley, en la extensión del ámbito del deber de colaboración a una actuación preventiva, más allá del concepto clásico de la protección de datos de carácter personal, que tiene su propia fuente en unos datos que han de ser conservados por los operadores por mandato legal. Ya no será necesario, con la LCD, imponer al operador un deber de colaboración, almacenando, o incluso captando, unos datos a los que no podría acceder, ni someter a tratamiento o cesión, como no fuera por imposición de una autoridad judicial. La información, simplemente, debe conservarse durante un plazo de tiempo delimitado, a los efectos de que resulte útil para alguno de los fines públicos superiores concretamente tasados. Pero el mérito va aún más allá, cuando por fin tan concretos

deberes de colaboración en el ámbito de la injerencia sobre comunicaciones han adquirido el carácter de norma con rango de ley formal, evitando en buena parte el riesgo de superación de los límites de la potestad reglamentaria.

LV. De hecho, la LCD ha recogido una serie de fuentes de investigación que en buena parte fueron anticipadas por la práctica jurisdiccional y avaladas por la jurisprudencia tanto del Tribunal Supremo como del Tribunal Constitucional. Tras su entrada en vigor, las nuevas herramientas a disposición de los agentes facultados y de la autoridad judicial o del CNI abarcan ya a todo el espectro de posibilidades de actuación, desde la preambular, tomando como fuente los datos almacenados por mandato de la norma, como la actuación conjunta en el contexto de una interceptación de comunicaciones.

LVI. La imposibilidad para los operadores de aprovechar o utilizar los registros generados ha dado lugar a la coexistencia de dos regímenes diversos. El primero, basado en una norma legal —la LCD— que impone una concreta restricción de determinados derechos relacionados con la protección de datos de carácter personal al objeto de su posible utilización para específicos fines públicos. El segundo, plenamente integrado en la normativa general sobre protección de datos de carácter personal —la LOPD— y su concreta aplicación en el tráfico de comunicaciones electrónicas —la LGT—. Esta situación es susceptible de crear ámbitos de compleja coexistencia entre el extenso deber de conservación *ministerio legis* y las posibilidades de conservación a efectos de tránsito y facturación o al amparo del consentimiento del usuario o abonado. Dicha coexistencia, además, casa difícilmente con las exigencias de calidad y seguridad en la conservación de tales datos a los efectos de lo establecido en la LCD.

LVII. El art. 5 LCD establece que la obligación de conservación de datos cesa a los doce meses desde la fecha en que se haya producido la comunicación. Nos encontramos así dentro de los parámetros que establece la DCD. El plazo establecido por el legislador español coincide además con el que venía dispuesto —a la espera de su fallida concreción reglamentaria— por el art. 12 LSSI, que permitía a los operadores retener hasta un máximo de doce meses los datos necesarios para la localización del

terminal empleado por el usuario para transmitir cualquier comunicación por vía electrónica a título oneroso. Se echa en falta en todo caso una referencia expresa la supresión de los datos no cedidos como garantía de seguridad jurídica, máxime dada la ausencia de una previsión de este tipo en el artículo 4.5 LOPD, que sólo alude a la cancelación, que no es equivalente a la supresión, sino al "bloqueo". Ello no obstante, debe entenderse que tal deberá ser el destino de los datos no cedidos.

LVIII. Si bien el plazo anual es plenamente predicable de todos los elementos *dinámicos* de las comunicaciones, obviamente no podrá suceder lo mismo respecto de ciertos elementos *estáticos* —en concreto, los datos de identificación de abonados o usuarios, a los que hemos denominado "datos de suscripción" o "datos de abonado"— durante todo el tiempo que se mantenga la relación contractual del abonado con su operador. Esto hace que se solapen a la vez dos obligaciones de conservación: una para dar respuesta al mandato de la LCD y otra para poder prestar el servicio a aquéllos.

LIX. Las normas de protección y seguridad de los datos en la LCD (art. 8) se configuran como auténticas normas de remisión a la compleja normativa sobre protección de datos que, hasta la fecha, han de entenderse referidas al Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, cuya vigencia provisional ha sido ratificada por la Disposición Transitoria Tercera de la LOPD, y se sobreentiende en el art. 8.3 LCD. Sin embargo, la remisión en bloque a tal normativa olvida que los datos de carácter personal de conservación obligatoria encuentran un difícil acomodo en la determinación de los niveles de seguridad exigibles a los responsables de los ficheros. La existencia de datos que pueden considerarse encuadrados tanto en niveles de seguridad bajo, medio y alto habrían hecho conveniente que el legislador hubiera determinado claramente el nivel de seguridad exigible, estableciendo acaso un catálogo de normas específicas sobre los criterios y exigencias de protección y seguridad de los ficheros donde se almacene tan ingente y valiosa información.

LX. Particularmente criticable es la regulación por el art. 6.2 LCD de cuáles son las concretas autoridades públicas que tienen la consideración de "agentes

facultados", y por tanto, son competentes para recabar los datos conservados. De lo previsto en la LCD parece desprenderse una concepción del proceso penal en que las labores de investigación se atribuyen con carácter general a la Policía, limitándose el Juez a habilitar a ésta para proceder a la injerencia. El legislador ignora que la investigación penal corresponde en nuestro actual modelo procesal penal a los Jueces instructores y, en su caso, al Ministerio Fiscal, en tanto la Policía Judicial dispone de competencias investigadoras por propia autoridad sólo en supuestos de actuación "a prevención". Sin embargo, el art. art. 6.2 LCD identifica como exclusivos destinatarios de la cesión a los agentes facultados —la Policía o Vigilancia Aduanera—, sin mención a los Jueces y Fiscales, que deberían ser los destinatarios de la información comunicada, previo control judicial en todo caso, disponiendo la Policía Judicial de la información únicamente en la medida en que actúen como auxiliares de estos órganos, que son los competentes para dirigir la investigación penal.

LXI. Habiéndose establecido la exigencia de resolución judicial habilitante, lo coherente con dicho presupuesto es que los datos sean cedidos al órgano judicial a fin de que efectúe el control de la medida realizada y que, una vez efectuado éste, sea él el que facilite los datos recabados a los agentes facultados. Los únicos supuestos en que la Policía, por razón de sus competencias, debería ser en rigor considerada destinataria de la cesión son los de prevención de delitos, es decir, justamente cuando desempeña las labores que no corresponden a las de Policía Judicial y que, por tanto, a tenor de la Ley, no legitiman la cesión de datos de las comunicaciones.

LXII. La LCD deja primeramente a la discrecionalidad del Juez el plazo "razonable" para que el cumplimiento de la obligación de cesión se lleve a cabo, según la necesidad del caso concreto, así como a la proporcionalidad del beneficio de la medida en relación a la injerencia infligida. La exigencia de que el plazo de ejecución de la orden de cesión se fije en la autorización judicial "atendiendo a la naturaleza y complejidad técnica de la operación" no resulta el más prudente criterio, pues no parece que el titular de un órgano judicial sea el más indicado para calibrar las susodichas "naturaleza y complejidad técnica", en tanto que las tales podrían ser distintas para cada operador en función de la configuración de sus equipos y de sus propios medios tecnológicos. Por contra, no cabe sino reconocer mayor peso a otros elementos no

menos relevantes para la fijación del plazo, como pueden ser la mayor o menor urgencia de la cesión —a la que se refiere también el art. 7.3 LCD—, a efectos de la investigación o enjuiciamiento de que se trate en cada caso.

LXIII. En lo tocante a la resolución judicial habilitante —que, en cuanto debe ser motivada, deberá adoptar la forma de auto—, no se acierta a entender la alusión que se hace en el art. 7.2 LCD a la LECrim como referencia normativa para establecer los datos que han de ser cedidos a los agentes facultados. Esta mención podría interpretarse como una alusión a la incardinación de la medida en el marco de la investigación penal y, de este modo, a los fines del proceso penal, de manera que los datos recabados se restrinjan a aquellos precisos para averiguar el delito e identificar el delincuente.

LXIV. Respecto de la exceptuación del deber de recabar el consentimiento del afectado que plantea el art. 9.1 LCD, hemos de señalar que, si bien el art. 6.1 LOPD establece que el tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado, el mismo precepto advierte *in fine* que este principio despliega su eficacia "salvo que la ley disponga otra cosa". De este modo, si la LCD es la fuente misma de la regulación de unos ficheros que son completamente ajenos a la voluntad o consentimiento de los ciudadanos, se echa de ver claramente que la cesión de estos datos a los agentes facultados, bajo la salvaguardia de la autoridad judicial, se excepciona del principio del consentimiento con completa legitimidad.

LXV. Dado que la cesión debe ser acordada por el órgano judicial, resulta lógico —aunque nada dice la LCD al respecto— que sea éste el que deba compatibilizar las necesidades de la investigación, que pueden comportar la de asegurar la clandestinidad de la cesión, a fin de que el titular de los datos, prevenido por la adopción y práctica de la cesión, no oculte o destruya informaciones u otros elementos de interés para el esclarecimiento de los hechos investigados, o altere su conducta posterior, con el derecho de defensa del imputado y, en todo caso, el derecho a la protección de los datos de carácter personal del titular de los datos.

LXVI. Pese a la carga económica que supone la nueva normativa de conservación, ni la DCD ni la LCD han optado por prever ningún tipo de compensación

económica a favor de los proveedores de servicios de comunicaciones electrónicas. En el caso español, el problema de los costes y la repercusión de esta reforma en el mercado de las telecomunicaciones apenas fue considerada por nuestro legislador. En la memoria económica del Proyecto de Ley se incluyó un tercer epígrafe sobre la incidencia económica sobre el sector, pero su contenido se redujo prácticamente a distinguir entre los costes de adaptaciones técnicas y los de actividades administrativas —sin cuantificar unos ni otros—. El Gobierno español no prestó atención a las alegaciones u observaciones a las alegaciones y propuestas de los interesados o afectados a este respecto por la normativa.

LXVII. En todo caso, a la vista de las actuales vicisitudes económicas por las que atraviesa tanto nuestro país como otros tantos Estados miembros de la Unión, parece que la posibilidad de establecer una compensación económica en favor de los operadores a cargo de los presupuestos nacionales ha quedado completamente postergada frente a la necesidad urgente y prioritaria de reducir el gasto público.

Conclusiones de la Cuarta Parte. Constitucionalidad de la Ley 25/2007, de 18 de octubre.

LXVIII. Resulta patente que las medidas previstas en la LCD suponen una notable afectación de derechos fundamentales, principalmente los reconocidos por el art. 18 CE: intimidad personal y domiciliataria y el secreto de las comunicaciones. La mera perspectiva de que todos los datos externos de nuestras comunicaciones por teléfono e internet hayan de ser conservados durante un plazo de doce meses se antoja por sí misma notablemente invasiva de la esfera íntima.

LXIX. Para que la norma en presencia pueda adquirir carta de naturaleza en el ordenamiento español, debe quedar acreditado que sus medidas, aun comportando una injerencia en los derechos fundamentales afectados respetan de todo punto los parámetros de legitimidad constitucional establecidos por nuestro texto fundamental y la jurisprudencia del TC. Conforme a estos, tanto la conservación generalizada de datos

como las demás medidas de la LCD habrán de respetar las exigencias clásicas de cualquier restricción de derechos fundamentales, a saber: previsión legal, reserva de decisión judicial motivada y estricta observancia del principio de proporcionalidad. Este último principio se concreta en tres requisitos o condiciones: idoneidad de la medida para alcanzar el fin constitucionalmente legítimo perseguido —lo que se denomina *juicio de idoneidad*—; que la misma resulte imprescindible o necesaria para ello, esto es, que no existan otras medidas menos gravosas que, sin imponer sacrificio alguno de derechos fundamentales o con un sacrificio menor, sean igualmente aptas para dicho fin —*juicio de necesidad—;* y, por último, que se deriven de su aplicación más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o intereses en conflicto, o dicho de otro modo, que el sacrificio impuesto al derecho fundamental no resulte desmedido en relación con la gravedad de los hechos y las sospechas existentes —*juicio de proporcionalidad en sentido estricto*—.

LXX. La norma en presencia supone la creación de una nueva obligación para los operadores que prestan servicios de comunicaciones electrónicas de captar y conservar por el plazo de doce meses una amplia y detallada cantidad de datos generados por cada uno de sus usuarios en el marco de los servicios de comunicaciones electrónicas, de manera que estén disponibles para su cesión a las autoridades policiales —previa autorización judicial— para la averiguación y represión de delitos graves.

LXXI. Varios aspectos separan claramente la clásica intervención del contenido o de los datos externos de las comunicaciones —regulados principalmente en la LECrim— de la medida que constituye el núcleo de la LCD, pese a lo que podría parecer *prima facie*. El principal elemento que distingue a la LCD es que impone la obligación para los operadores de guardar todos y cada uno de los datos relevantes de las comunicaciones electrónicas de sus abonados durante un período de doce meses. De este modo, la gravedad de la injerencia en los derechos fundamentales que lleva a cabo la LCD no radica en la cesión de ciertos datos de las comunicaciones electrónicas a los agentes facultados para la investigación y enjuiciamiento de delitos —pues tal cesión se lleva siempre a cabo previa resolución judicial y de acuerdo con los principios de necesidad y proporcionalidad, tal como determina taxativamente el art. 7.2 LCD—,

sino en esta obligación principal, cuyos rasgos separan la LCD de las demás medidas de interceptación hasta ahora conocidas.

LXXII. Ha de subrayarse igualmente que no estamos ante una medida *puramente procesal* sino, sobre todo, ante una norma *administrativa* que obliga a sujetos particulares —los operadores de servicios de comunicaciones electrónicas— a interceptar un ingente número de datos generados por los servicios que prestan a sus clientes.

LXXIII. En segundo lugar, no estamos ante un *acto de investigación en el marco de un procedimiento penal*. No se ha cometido ni se está investigando ningún delito en el momento en que tiene lugar la medida limitadora del derecho: la retención y archivo masivos de datos electrónicos. Los datos se interceptan pero, al contrario que en una intervención de las comunicaciones al uso, no se ponen en manos ni del Juez ni de la Policía Judicial; simplemente pasan a formar parte de un fichero de datos que el obligado debe mantener a su costa, y de acuerdo con unos mínimos de seguridad, durante el plazo de doce meses.

LXXIV. En tercer lugar, ninguna de estas acciones de interceptación y conservación se realiza *por orden o bajo control judicial*; es la LCD la que prescribe directa y genéricamente las acciones que debe llevar a cabo el obligado.

LXXV. En cuarto lugar, la medida no afecta a un concreto individuo en un concreto proceso, sino a cualquier persona que tome parte de una comunicación telefónica o por internet, lo que en la práctica comprende a la *generalidad de la ciudadanía* en un aspecto esencial de la vida cotidiana. Este rasgo —como se aprecia fácilmente— resulta relevante a la hora de valorar la proporcionalidad de tal regulación.

LXXVI. Otro rasgo fundamental de la LCD es el hecho de que no sea el poder público quien directamente se ocupe de interceptar todos los datos de tráfico y conservarlos en inmensas bases de datos. La injerencia en el derecho o derechos fundamentales se realiza *ex lege* por los particulares obligados. Todos los aspectos

externos de cada una de las comunicaciones telefónicas o de internet que hayamos mantenido durante los últimos doce meses —quién, desde dónde, a quién, cuándo, etc.— quedan en manos de compañías de telecomunicaciones privadas, que deben almacenarlos a su costa y bajo su responsabilidad. Es cierto que los datos no estarán disponibles para el uso de los operadores, y que su custodia deberá rodearse de estrictas medidas de seguridad pero, en cualquier caso, la creación y mantenimiento por mandato legal de tan ingente masa de información personal supone, a todas luces, el surgimiento de una esfera de especial vulnerabilidad —artificialmente creada por expresa voluntad del legislador— y una potencial amenaza para la privacidad de cada ciudadano, así como una formidable injerencia en el espacio de libertades del que el Estado de derecho se supone protector, no agresor, por más que la conservación de los datos se haga y mantenga a través de particulares sometidos a un régimen de responsabilidad y a estrictas garantías de seguridad.

LXXVII. La concreción de los derechos fundamentales que se ven afectados por la medida central de la LCD —el mandato legal por el cual se establece la conservación masiva por parte de los operadores de los datos externos de las comunicaciones electrónicas— resulta polémica. Una posición mantiene que la acción por la que el operador debe captar la lista de datos del art. 5 LCD y conservarlos en una base de datos donde han de permanecer a disposición de las autoridades facultadas debe ser considerada como una interceptación de las comunicaciones sobre los datos externos. Esta interceptación presentaría sobre todo dos peculiaridades respecto de las tradicionales: se realiza por mandato legal, no judicial, y, en segundo término, los datos no se transmiten directamente a las autoridades públicas sino que pasan a formar parte de un fichero, a la espera de una eventual entrega a las mismas. Por tanto, la acción de captar todos estos datos afectaría al derecho al secreto de las comunicaciones y la de su prolongado archivo, al derecho a la protección de datos —abstracción hecha de los *datos de suscripción*, en los que es claro que únicamente éste último el que queda afectado—.

LXXVIII. De acuerdo con una segunda tesis, no puede decirse que exista captación de los datos y, en consecuencia, no habría injerencia en el derecho al secreto de las comunicaciones. En la práctica, los operadores ya retienen esos datos para la prestación

del servicio y su relación con los mismos es *per se* un tratamiento de los regulados en la LOPD. De este modo, sucedería con los datos de tráfico lo mismo que con los de suscripción; simplemente, la LCD los haría indisponibles para el titular. En consecuencia, el único derecho que resulta afectado por las medidas de la LCD es el de la protección de datos personales, no el secreto.

LXXIX. En todo caso, del conjunto general de la regulación parece colegirse que —para el legislador español— la captación y cesión de los datos por parte de los operadores vendría a ser una restricción del derecho al secreto de las comunicaciones, en tanto que la conservación *per se* lo sería del derecho a la protección de datos de carácter personal.

LXXX. Sea cuales fueren los concretos datos de tráfico que deben quedar excluidos de la protección del secreto de las comunicaciones, lo cierto es que una amplia mayoría de los que la LCD obliga captar y conservar caen sin duda dentro de su ámbito de protección, suponiendo su retención generalizada una clara afectación del derecho —baste pernsar en números de teléfono marcados, la hora y la duración de la llamada—. En relación con estos novedosos medios de investigación, nuestro TC ha declarado que ciertos aspectos formales de la comunicación, como la entrega de los listados por las compañías telefónicas a la Policía sin consentimiento del titular del teléfono, requería también la correspondiente resolución judicial, pues suponía una injerencia en el proceso de comunicación que está comprendida en el ámbito de protección del derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE. Tal doctrina es plenamente aplicable al acceso a los datos conservados por mandato de la LCD, que como ya sabemos, requiere asimismo la autorización judicial de los listados y cualquiera otra de las informaciones retenidas.

LXXXI. Los denominados datos de abonado no ofrecen duda alguna sobre su protección conforme al derecho fundamental a la protección de datos. Mucho más compleja es la protección de los datos de localización y los datos de trafico *stricto sensu*, que también quedan retenidos por mandato de la LCD. Lo cierto es que, si bien los datos de tráfico siguen siendo conceptualmente datos de tráfico con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso, bien de

la lícita facturación del servicio prestado, bien de su ilícita difusión, los tales experimentan un importante cambio cuando pasan a estar protegidos por el derecho a la protección de datos. Desde el momento en que se trata de datos relacionados con comunicaciones perfeccionadas, su protección bajo un ámbito distinto al del secreto de las comunicaciones se convierte en un factor a tener en cuenta a la hora de establecer el juicio de proporcionalidad de la medida invasiva del derecho de las personas concernidas.

LXXXII. La entrada de la LCD en el marco regulatorio de las telecomunicaciones en España supuso la irrupción de una amplísima excepción a todas las previsiones que concretaban el principio general de libre disposición de los datos por parte de los abonados. Respecto de los *datos de suscripción*, los proveedores tienen el deber de conservarlos por doce meses, estableciéndose así por imperativo legal una incisiva excepción a la regulación general del derecho a la protección de datos. Estos datos, que fueron proporcionados voluntariamente por el usuario, ahora se conservarán tanto al margen de su voluntad como de lo dispuesto en la LGT. Respecto de todos *los demás datos externos* —los generados por la tecnología comunicativa—, la acción del operador por mandato legal sobre estos datos ha dado lugar a los dos tipos de interpretaciones acerca de cuál es el derecho fundamental afectado, en los términos que expusimos anteriormente.

LXXXIII. El principio de legalidad constituye un presupuesto común para todo acto del poder público limitativo de cualquier derecho fundamental. Por mandato expreso de la CE, toda injerencia estatal en el ámbito de los derechos fundamentales y de las libertades públicas que incida directamente sobre su desarrollo o limite o condicione su ejercicio precisa de una habilitación legal. En el supuesto de la LCD, el requisito de la previsión legal de la norma habilitante según las exigencias de la doctrina del TEDH, entendida como la previsión normativa que permita a cualquier persona conocer cuándo y bajo qué circunstancias puede verse afectado su derecho fundamental, queda claramente perfilado en dos niveles de regulación: uno primero de captación, almacenamiento y conservación sin posibilidad alguna de tratamiento, desarrollado en los arts. 1.2, 2 a 5, 8, 9, y Disposición Adicional Única —en sus aparts. 1, 3, 7 y 8— LCD; y un segundo nivel, de mayor intensidad y trascendencia en la

afectación de concretos derechos de las personas afectadas, de cesión y utilización de la información así facilitada, desarrollado en los arts. 1.1 y 3, 6, 7 y Disposición Adicional Única —aparts. 2 y 4— LCD.

LXXXIV. Más dudosa es la observancia por la LCD del segundo requisito que ha de concurrir en relación con la necesidad de previsión legal de la medida, que es el que norma goce de un determinado rango legal. El art. 81.1 CE exige que las normas relativas al desarrollo de los derechos fundamentales y de las libertades públicas tengan carácter de ley orgánica. Aplicado al objeto de nuestro estudio, el hecho de que el rango normativo de la LCD sea el de una ley ordinaria, ha dado lugar a que una mayoría de voces, tanto desde la doctrina como desde la jurisprudencia del TS, hayan sostenido la insuficiencia de este rango y, en consecuencia, la propia inconstitucionalidad de la norma. De los argumentos adelantados se deduce que la aprobación mediante ley orgánica de la LCD habría sido más conveniente en tanto que al menos despejaría las dudas de constitucionalidad que pesan sobre ella.

LXXXV. Por otra parte, la jurisprudencia constitucional exige no sólo que la injerencia estatal en el ámbito del derecho esté presidida por el principio de legalidad; el respeto a dicho principio requiere también para tales casos que se trate de una ley de singular precisión, en el sentido de que use términos suficientemente claros para indicar en qué circunstancias y bajo qué condiciones se habilita a los poderes públicos para autorizar una medida consistente —en el caso de la LCD— en conservar y ceder los datos de tráfico con fines penales. En referencia a las escuchas telefónicas —materia cercana a la de la LCD—, los requisitos son los siguientes: la definición de las categorías de personas susceptibles de ser sometidas a escucha judicial; la naturaleza de las infracciones susceptibles de poder dar lugar a ella; la fijación de un límite a la duración de la ejecución de la medida; el procedimiento de trascripción de las conversaciones interceptadas; las precauciones a observar, para comunicar, intactas y completas, las grabaciones realizadas a los fines de control eventual por el Juez y por la defensa; las circunstancias en las cuales puede o debe procederse a borrar o destruir las cintas, especialmente en caso de sobreseimiento o puesta en libertad.

Si aplicamos estos criterios a la LCD, se comprueba que la norma no cumple con algunos de ellos. Para regular la cesión de los datos a los agentes

facultados, se remite a una resolución judicial conforme a lo previsto en la LECrim y de acuerdo con los principios de necesidad y proporcionalidad —art. 7.2 LCD— de un modo tan vago y genérico que resulta claramente insuficiente, por su falta de detalle, con la jurisprudencia del TEDH respecto a la calidad y la claridad de aquella ley que se ocupe de regular una restricción a un derecho fundamental.

LXXXVI. La falta de una regulación completa de la intervención de las comunicaciones electrónicas incide en la eficacia de la actuación de las Fuerzas y Cuerpos de Seguridad del Estado, que, en ocasiones, ven anuladas sus investigaciones o incluso se ve incursa en responsabilidad por vulneración del derecho al secreto de las comunicaciones y por la obtención ilícita de pruebas. Por todo ello, resulta sumamente aconsejable que las imprecisiones de la LCD sean subsanadas lo más pronto posible por el legislador.

LXXXVII. El segundo requisito para que la restricción de derechos fundamentales de la LCD sea compatible con nuestro orden constitucional es la reserva de decisión judicial motivada**.** Tal reserva en el acceso y cesión de la información contenida en los ficheros de datos relativos a las comunicaciones electrónicas se muestra como algo incuestionable en la LCD. Corresponde al Juez decidir *en toda ocasión* sobre el hecho de la cesión y el contenido de lo que ha de cederse, siempre en función de los principios de necesidad y proporcionalidad y de modo semejante a como se exige para la intervención de las comunicaciones telefónicas. Sólo cuando se observen todas estas condiciones la utilización de estos datos podrá tener la debida eficacia probatoria en el proceso penal.

LXXXVIII. No basta que la medida esté prevista en la Ley y sea adoptada por un Juez, sino que resulta imprescindible que objetivamente se justifique para obtener el cumplimiento de los fines constitucionales que la legitiman, debiéndose adoptar, en cualquier otro caso, la alternativa menos gravosa para el derecho fundamental. La regulación de la LCD de estar sometida al más estricto cumplimiento de los principios de idoneidad, necesidad y proporcionalidad *stricto sensu*. Entre los requisitos que debe cumplir la norma en aplicación del principio de proporcionalidad se cuentan la idoneidad y la necesidad de la medida, lo que implica, de un lado, que sea apta para conseguir el fin perseguido —la investigación del hecho punible y la determinación de

su autor—; y, de otro, imprescindible para alcanzarlo, sin que puedan determinarse tales extremos a través de otro mecanismo.

LXXXIX. La creación *ex lege* de un deber general de conservación de datos constituye la cuestión central de la LCD en lo que a la proporcionalidad de la injerencia en los derechos fundamentales se refiere. La Ley establece un mandato legal dirigido a los proveedores en virtud del cual se erige un deber de retención de forma generalizada, con independencia del supuesto de hecho concreto que en el futuro pueda fundamentar la obligación de cesión de dichos datos a instancia de la autoridad judicial.

XC. El deber de retención persigue así conservar unos datos que eventualmente pueden ser útiles en la investigación de una concreta infracción penal de carácter grave. Se trata de conservar de forma generalizada sin individualizar ni los sujetos ni las comunicaciones concretas que pueden verse afectadas por la medida. El deber de conservación generalizada de datos no cumple con el principio de intervención indiciaria que nuestro sistema constitucional exige a las medidas restrictivas de los derechos fundamentales orientadas a la prevención o persecución de los delitos. Esto es, estamos ante una medida que se apoya en el riesgo —completamente genérico— de que cualquier ciudadano pueda cometer delitos graves para cuyo esclarecimiento y castigo puedan resultar útiles los datos de tráfico de sus comunicaciones, lo que hace que se determine *ex lege* la conservación masiva de los mismos.

XCI. Aunque en nuestro sistema existen ya supuestos de intervención inindiciaria, tales como los registros en los aeropuertos o las videocámaras de seguridad de los bancos, en tales supuestos concurren circunstancias especiales de potencial peligro que concurren en esos lugares y que justifican la intervención o el control. El uso habitual de las redes de comunicaciones no es en sí mismo un peligro y, por añadidura, no se trata de una situación concreta, sino un aspecto intrínsecamente ligado a la vida cotidiana de todos los ciudadanos. Un riesgo tan genérico no justifica la legitimidad del deber de conservación generalizada impuesto por el legislador.

XCII. El hecho de que la conservación de los datos no está destinada a la investigación criminal de modo directo sino indirecto, ya que se lleva a cabo antes de la comisión del hecho delictivo e incluso antes de la sospecha de que pueda cometerse en un período determinado sitúa el deber de conservación en el ámbito de las *medidas prospectivas* —o de prevención desligadas de la realización de un hecho delictivo— cuya legitimidad, como es bien sabido, ha sido excluida por el TC. Para que una intervención de este tipo sea válida en nuestro sistema, hemos de hallarnos en todo caso ante una medida *post delictum*, dictada una vez que ha llegado al Juez la *notitia criminis* y, normalmente tras haber recaído el auto de incoación del sumario, supuestos que no concurren en la LCD.

XCIII. La interpretación literal del art. 1.1 LCD, en lo que se refiere a la correcta delimitación de la noción que de "delito grave" maneja la LCD, conduce a resultados y conclusiones notablemente insatisfactorias. En conclusión, la interpretación del concepto de delito grave usado por el legislador de la LCD debe estar abierto a todos estos matices y criterios y no al meramente literal de nuestro código criminal. Es la autoridad judicial quien, en última instancia ha de valorar, en función de los intereses en conflicto, si para avanzar en la investigación de cualquier delito puede o no tenerse acceso, y en qué medida, a los ficheros de datos relacionados con las comunicaciones electrónicas conservados por las operadoras de telecomunicaciones, y si, por tanto, estamos o no ante un delito grave a efectos del art. 1.1 LCD. Teniendo en cuenta la doctrina ya asentada del Tribunal Constitucional sobre la caracterización del concepto de delito grave como aquel que sea susceptible de superar el juicio de proporcionalidad en las injerencias en el derecho al secreto de las comunicaciones, la expansión de tal doctrina en la posible utilización procesal de la información almacenada sobre datos relativos a las comunicaciones es incuestionable, y habrá de permitir sin duda su aplicación a importantes campos de la investigación criminal que quedarían si no fuera de los límites fijados por los arts. 13.1 y 33.2 CP. Todo ello, sin perder de vista que sigue resultando constitucionalmente necesaria la determinación por el legislador de los concretos tipos penales que pueden dar lugar al empleo de las medidas de la LCD. Estas conclusiones quedan reforzadas si analizamos la cuestión tanto desde la perspectiva estricta de nuestro sistema constitucional de derechos como desde el punto de vista del Derecho europeo.

XCIV. El régimen de conservación de datos para aquellos delitos que no puedan calificarse como graves a efectos de la aplicación de la LCD ha de consistir en la aplicación ordinaria de la LECrim. Queda absolutamente vedada la posibilidad de aplicar las medidas de la LCD a los hechos que desde un primer momento sean calificadas como simples faltas. Los datos electrónicos de meras comunicaciones contractuales mercantiles o civiles no pueden ser puestas a disposición de la autoridad competente en tanto su ámbito cae fuera de la obligación impuesta por los arts. 6 y 7 LCD. El legislador no tiene obligación alguna, derivada del art. 24 CE, de proporcionar o facilitar medios de prueba al litigante en un proceso civil imponiendo a los operadores de telecomunicaciones deberes de retención y conservación de los datos generados en la prestación de sus servicios. Si efectivamente los establece, le resulta constitucionalmente lícito —y ajustado al Derecho de la Unión Europea— restringir su uso al ámbito del proceso penal y, en concreto, al proceso penal por delito grave.

XCV. El plazo de conservación de los datos plantea la necesidad de ponderación entre la finalidad perseguida —el aseguramiento de la eventual puesta a disposición de los datos conservados, cediéndolos a los agentes facultados— y el gravamen que para el derecho a la protección de los datos de carácter personal supone la prolongación en el tiempo del tratamiento de los datos. La cuestión de la proporcionalidad de los plazos no es, sin embargo, tan sencilla pues al ser inindiciaria, la justificación de la medida en atención a la finalidad perseguida no se manifiesta en el momento de llevar a cabo la conservación, sino cuando se presenta la conveniencia de ceder los datos. Ello supone que, aunque la cesión de datos sólo tenga lugar cuando se vincule a la represión de delitos graves, la conservación se efectuará igualmente respecto de la totalidad de datos —ya que todos deberán estar disponibles—, sin que se produzca ninguna matización en la afectación que implica el plazo de conservación de los datos, que será igual para todos los datos, con independencia de que sólo se revelen durante el segundo período aquellos cuya cesión se justifique por la particular gravedad del delito investigado. En definitiva, la duración de la conservación sólo admite su ponderación atendiendo a la gravedad del perjuicio que comporta la extensión temporal de la conservación, por un lado, y la finalidad inmediata como un "todo", esto es,

contemplada como el aseguramiento de la puesta a disposición con vistas al fin de la cesión.

XCVI. Se constata una tendencia a considerar —por parte de los organismos implicados y dela doctrina— los actuales plazos permitidos por la LCD y la DCD como excesivos. Así las cosas —y con la perspectiva de una anunciada reforma de la DCD en éste y otros puntos— parece que una mejor ponderación de los plazos, efectuada sobre datos empíricos, puede dar lugar a una revisión a la baja de los plazos de conservación permisibles.

Conclusiones de la Quinta Parte. Régimen de los servicios de telefonía mediante tarjetas prepago.

XCVII. Sin base en previsión alguna de la DCD, la DAU de la LCD introduce en nuestro ordenamiento a través sus ocho apartados una regulación especial para los servicios de telefonía mediante tarjetas de prepago. La finalidad de la DAU ha sido la de romper con la puerta abierta al anonimato en las comunicaciones telefónicas que brindaban estas populares y económicas tarjetas.

XCVIII. El primer epígrafe de la DAU establece por vez primera en la historia del Derecho español de las telecomunicaciones el deber para los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago de llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

XCIX. En cuanto a los *sujetos obligados* a cumplir con el deber, estos son los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago. El ámbito subjetivo coincide así en buena medida con el trazado por el art. 1 LCD para la conservación de datos, lo que resulta ciertamente criticable, pues el legislador parece no haber reparado en que —en la práctica cotidiana— la recepción de tales datos recaerá en su mayor parte en

personas que nada tienen que ver con los operadores concernidos, y a quienes indirectamente se hace poseedores y responsables de la conservación de datos sensibles sobre la identificación de los clientes.

C. La norma somete la información almacenada a los mismos principios de calidad, conservación, no manipulación y acceso limitado a los mismos que los demás datos de la LCD. En la práctica, la aplicación de la DAU comporta diferir la entrega de los datos al operador concernido, dado que los vendedores directos han de proceder a la obtención de los datos y a su inmediata cesión a la empresa de telecomunicaciones, que es el verdadero destinatario de la norma. Como no existe una compartición de ficheros —al no existir una relación de dependencia—, el dato captado por el expendedor ha de ser cedido, irremisiblemente y *ministerio lege*, al sujeto obligado a la llevanza del libro-registro, con aplicación por tanto de lo establecido en el art. 11.2.a) LOPD. Así pues, la solución pasa necesariamente, bien por la respuesta práctica empleada por las operadoras —que recaban del expendedor los datos en soporte de papel, que los remite a éstas sin quedarse copia—, bien por establecer sistemas de almacenamiento temporal a los solos efectos de su pronta remisión al destinatario real de la norma de conservación y ulterior cancelación.

CI. Los operadores deben ceder los datos identificativos que acabamos de describir cuando les sean requeridos para el cumplimiento de sus fines por los agentes facultados —los mismos a que se refiere el art. 6.2 LCD— así como a "los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública en el curso de las investigaciones de seguridad sobre personas o entidades". A pesar de que el tenor de la disposición da la impresión de que nos encontramos ante un círculo de agentes facultados más amplio que el señalado en el art. 6.2 LCD, lo cierto es que esta actuación de investigación del delito previa a la actuación judicial entraña igualmente una actuación propia del concepto de Policía Judicial, por lo que en realidad se trata del mismo conjunto de sujetos que están autorizados en virtud de la LCD para acceder a los datos conservados ex art. 5 LCD.

CII. Otra diferencia crucial de la DAU frente a la regulación contenida en la LCD radica en el tipo de infracciones penales que habilitan el acceso a los datos conservados, pues frente a la necesidad de investigación de *delitos graves* en el primer caso, en el segundo se reduce la exigencia a *cualquier delito del Código Penal o de las leyes penales especiales*. Obviamente, tal ampliación de la finalidad justificativa del acceso abre el abanico ya no sólo a los delitos graves o muy graves, sino también a los leves, dado que, al emplear el término genérico de "delito", caen bajo el amparo de la Disposición todos los tipos y subtipos penales codificados —excepto las faltas—.

CIII. A diferencia de lo que sucede en el caso de la cesión de datos de las comunicaciones en el articulado de la LCD, la DAU habilita soterradamente la cesión con fines preventivos, superando el ámbito exclusivamente procesal penal que presenta la cesión en el caso del art. 1 LCD. En concreto, el apartado segundo de la DAU es susceptible de una lectura aún más extensiva por lo que respecta a las finalidades de la cesión en tanto que, allí donde el apartado cuarto señala como finalidades de la cesión "la investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales", el apartado segundo se limita a establecer el deber de cesión "para el cumplimiento de sus fines" de las autoridades indicadas. La amplitud con que están formuladas las finalidades de la cesión permite que ésta no sólo se restrinja a la finalidad de identificar a los titulares de los datos conservados, sino que haga posible su comunicación para cualquier otra investigación o actividad de detección de delitos.

CIV. La interpretación del apartado cuarto de la DAU no puede llevarnos a concluir que no se precisa la autorización judicial para el acceso y cesión de los datos conservados en el libro-registro, pese a que el articulado omita cualquier mención a tal requisito. Visto desde la perspectiva de la proporcionalidad de la medida, se echa de ver que la cesión de estos datos identificativos resulta más gravosa que los generales del art. 5 LCD, por ser los primeros susceptibles de identificar claramente a su titular. Así pues, lo que realmente lleva a cabo la DAU es la creación de un fichero de datos de carácter personal con un contenido concreto que se integra en el art. 3 LCD, es decir: impone a los operadores el deber de identificar al adquirente de tarjetas de prepago; y

esa información que ha de recabarse *ministerio lege* se integra plenamente en las normas comunes relacionadas con los deberes impuestos a los operadores concernidos.

La solución a tan grave problema de legalidad constitucional ha de encontrarse a nuestro modo de ver en la extensión natural de la reserva de autorización judicial contenida en el art. 6.1 LCD a los datos conservados en el libro-registro de clientes de tarjetas de prepago.

CV. La principal objeción que cabe realizar a las medidas introducidas por la DAU es que constituye una agravación de la inindiciariedad que comporta la LCD. A fin de obtener la supuesta eficacia de la conservación generalizada de datos, en que se ha pretendido sustentar su necesidad, se incrementa la limitación indiscriminada de un derecho fundamental (al extender la conservación inindiciaria a nuevas categorías de datos de carácter personal) con carácter secundario y, por ende, aún más alejada de la finalidad perseguida (la prevención e investigación de delitos).

CVI. La finalidad perseguida por la DAU ha sido lograda parcialmente, pues resuelve un segmento muy concreto del espectro de posibilidades de navegación anónima a través de las redes de telecomunicaciones. La capacidad innovadora de las tecnologías de las comunicaciones y el interés de los operadores para hacerse con un tipo de clientes que buscan el anonimato posiblemente conviertan a la norma en una rémora que sólo afecte los derechos de personas de escaso nivel económico o conocimiento de las posibilidades que ofrecen las tecnologías de la comunicación.

SUMMARY

The Legality of the EU Legislation on Data Retention in Electronic communications and its Implementation in Spain

This dissertation introduces for the first time into the Spanish legal academia a thorough study of the EU and Spanish legislation on data retention in electronic communications and their compatibility with the EU and Spanish declarations of rights.

For the last six year, the external data of the electronic communications—i.e. almost every data but for the content—of more than 500 million European citizens have been routinely stored in the databases of the telecom companies for a period ranging from six months up to twenty-four, in case law enforcement agents need these data for the investigation, detection or prosecution of serious crime. Under the current legislation, any authorized public agent can access any of this information, namely: who called whom, when, between which cellphone models, for how long, and from which place to which place. Similar information concerning internet-based communications gets stored as well.

This dissertation covers every aspect of the Spanish and EU regulation on this matter, and additionally examines its compatibility with the EU and Spanish declarations of rights. The work is divided into five blocks, plus a list of conclusions, a bibliography and several annexes.

The dissertation's first contribution lies on Parts One and Three, which offer a structured, comprehensive, and contextualized analysis of the EU and Spanish legislation on data retention. The political, legal, and historical circumstances surrounding the drafting of the rules are addressed in great detail from different perspective, mainly criminal procedure, administrative law, and constitutional law. To our knowledge, such analysis is the most extended one to this day in the legal literature, and provides detailed reasons to understand the shortcomings of the legislation.

Parts Two and Three cover the impact of the directive and the transposing national act on the fundamental rights. Data retention measures limit everyday-exercised rights such as data protection, secrecy of communications, and privacy. The compatibiliy of the current legislation with the EU's and Spanish constitution's bill of right is questioned at lenght.

Part Five explores the constitutionality problems of pre-paid cards phone services. The Spanish transposing act creates a special regime to stop anonymity of these cards' users. However, the regime presents many serious flaws regarding both its legality and its constitutionality.

Finally, the body of the dissertation ends with more than a hundred conclusions, explaining the major findings of this research.

CONCLUSIONS

Conclusions from Part One: Data Retention in European Union Law

(1) The political and legislative circumstances surrounding the drafting of the Data Retention Directive (DRD) in the European Union are particularly relevant to evaluate the necessity and proportionality of the measure. The approval of the DRD is the result of a long process in which the European Union became aware—largely driven by the events— of how relevant data retention was a tool for dealing with crimes concerning international terrorism. Moreover, it can be argued that the DRD came to life within the legislative antiterrorism policy that many Western states launched as a result of the terrorist attacks in New York, Madrid, and London during the first decade of the century. After these events, some developed countries began to show great concern about the threat of international terrorism posed to national security, particularly regarding the internet and electronic communications, which were regarded as suitable channels for an attack. The result of this alarm was an increase in EU police, judicial and criminal cooperation. In a short time, intercepting telecommunications data went from being considered a secondary matter—catching the attention of a small circle of security experts—to be one of the key elements of the EU security policy.

(2) The legislative proceedings for the DRD presents a great interest for an in-depth study. Many of the legal and political controversies surrounding the Directive—its flaws and shortcomings— arose during this period, giving rise to an intense debate that continues to this day.

(3) As to the observance of the principle of subsidiarity and the reasons why the European Commission chose the directive as the legal instrument governing data retention, it should be noted that no instrument from the first pillar but this one was been suitable. Moreover, a directive provided the necessary level of harmonization in the EU internal market. The directive also left enough room for member states to meet the particular national requirements.

(4) The numerous enquiries and reports issued during the passing of the DRD showed, first, a great interest in the act on the side of the security and police forces, for communications data retention was considered an essential tool for fighting crime (particularly, terrorism). On the other hand, the European telecommunications sector did not object strongly to the proposed legislation, but advocated for retention periods not exceeding six months. Finally, the data protection authorities and civil rights associations argued that data retention was an interference with the citizens' privacy and, therefore, the purpose and objectives of conservation should be defined with great precision.
The proposal drafted by the Commission would be presented as a "balanced approach" among these three positions.

(5) The opinions expressed about the bill by the Working Group of Article 29 (WGA29), the European Data Protection Supervisor (EDPS), the European Parliament and the European Economic and Social Committee (EESC) can be described as strong rebuke to the bill, the main and common objection being that it did not protect sufficiently the fundamental rights affected by the measure. In fact, some of this criticism found its way into the amendments to the draft, and that helped to improve the final version. Another portion got ignored, and remains as compelling arguments against the current legislation. In this sense, the difficult negotiation of the DRD failed to satisfy all sides' expectations.

(6) The Directive requires member states to take measures to ensure that a given set of external data from electronic communications be preserved and remain available for a period between six to twenty-four months for the purpose of investigation, detection and prosecution of serious crime, as defined by each member state in its national law. The need for harmonization of the matter through a directive was based on the existence of a plethora of national rules and the absence of regulation in some countries. The big differences among the laws, regulations, and techniques on traffic data retention in each member state posed obstacles to the internal market for electronic communications. Service providers had to meet very different sets of requirements as to

which type of data must be retained. This lack of harmonization was an obstacle for the exchange of information among law enforcement authorities of the member states.

(7) Time has now passed, and the transposition of the DRD has revealed how the meaning of *serious crime* varies widely from one EU country to another. The intended harmonization has revealed itself a notable failure in this important area. At the present time, each country allows transfers of data for completely divergent criminal purposes. Naturally, such contrasts have harmed the volume and frequency of transfers of data between member states, which was also another goal pursued by the Commission. This obstacle has additionally increased the costs that telecommunications companies have to incur for compliance with the DRD.

(8) The failure of harmonization affects the personal scope of the Directive. Article 1.1 DRD defines which operators must comply with the obligation to retain data, describing them as "providers of publicly available electronic communications services or of public communications
networks." When transposing the Directive into the national laws, different definitions of which providers fall within have once again led to undesirable disparity. The differences between national laws are additionally a clear cause of discrimination in the single market.

(9) The obligation to keep external data in electronic communications is at the heart of the legislation, and stands as a huge exception to the general principles on the matter set by arts. 5, 6, and 9 of the EU directive on privacy and electronic communications, which created strong privacy safeguards in favor of electronic communications users. The result is the reversal in the legislative situation: the exception has now become the rule.

(10) Article 5.1 DRD classified the data to be retained into six categories. These categories set out by the Directive must be interpreted as *numerus clausus*; additional obligations to retain cannot be imposed onto the operators. The comprehensive list contained in Art. 5 DRD has been one of the few points of the regulation in which a high level of harmonization has been reached.

(11) The data retention period is still one of the most discussed topics in the DRD, insofar as it is directly related to the proportionality of the retention measures and, consequently, to its legality. Discussions on the suitability of the retention period revolve around two competing interests. On the one hand, there is the claim of law enforcement authorities to ensure a sufficiently long period of time to carry out the investigation—the longer, the better—. On the other, the telecommunications businesses and the citizens, both parties seeking to keep the periods as short as possible in order to reduce storage costs and interference with the right to privacy. The transposition of the Directive in the national laws has shown that such broad margins, ranging from to six months up to twenty-four, are clearly unsuitable to achieve the harmonization sought by the rule. Once the DRD has been transposed, it is clear that member states apply retention periods that vary considerably, even within the limits of Art. 6 DRD.

(12) Art. 12 DRD provides that member states "facing particular circumstances that warrant an extension for a limited period of the maximum retention period . . . may take the necessary measures." By virtue of Art. 12 DRD, states are given prerogatives that open the door to expand further the retention powers originally granted. This is indeed one of the most objectionable provisions of the DRD, because of its problems of interpretation and its questionable legality. Expecting a ruling by the ECJ that may eventually strike down this section, we also believe that the fact that it has never been applied has kept this provision off the controversy.

(13) The safety and security measures for the retained data in Arts. 7 and 8 DRD are another most objectionable provision. Our analysis shows how efficiency in the data transfers, and not privacy, was the actual driver in the drafting of the DRD by the European Commission. The transposition and implementation of the DRD has shown the result of a regulation marked by neglect and a flawed legislative technique concerning data protection: only fifteen countries have implemented the data protection principles in the transposing legislation.

(14) Under the title *Access to Data*, Art. 4 DRD provides that member states take

measures to ensure that those data retained under the Directive are accessed only according to three concurrent conditions: (1) the data are provided only to the competent national; (2) in specific cases, and (3) in accordance with national law.

(15) In regard to the competent national authorities, the main criticism lies on the vagueness of the term. The serious omissions in Art. 4 DRD on access conditions have caused that member states incorporate these provisions into their domestic legislation in disparate ways. Access regimes goes from those countries that rely only on judicial proceedings and strong safeguards to those ones that authorize a panoply of law enforcement agencies to access the retained data based on purely procedural requirements. Given this disparity, it stands to reason that DRD has failed once again in its attempt to harmonize national regulations.
Considering a future reform, we suggest that it should be expressly stated that the retained data may only be accessed by those authorities which guarantee a well-defined level of quality, confidentiality and security of data. Access to data ought to be authorized on a case-by-case basis by a judicial—or at least independent—authority in any event.

(16) Article 10 DRD creates the obligation for member states to annually provide the European Commission with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. It is paradoxical that the failure to harmonize national legislations has reached this assessment task as well. In compliance with this provision, the European Commission called on member states to provide detailed information on individual applications for data. As the institution itself admitted, the statistics provided differed so widely in scope and detail that no conclusions could be hardly drawn from them.

(17) DRD regulation has caused a profound impact on the EU legislation on data protection in electronic communications, to the extent that the DRD itself included a provision aiming to restore the original harmony: Art. 11DRD amends the Directive on privacy and electronic communications, adding a section 1.bis to Art. 15 thereof. This “patch” by Art. 11 DRD is clearly insufficient. Since DRD has deprived Directive

2002/58/EC of much of its content and effectiveness, the relationship between the two set of rules should have been clarified in further detail. The references in Article 15.1 to Article 6 and 9 of that Directive would have better been eliminated, or at least modified, to clearly state that member states have no longer authority to adopt legislation in relation to criminal offenses. In short, it would have been desirable to clarify any ambiguity regarding their remaining powers, for instance, with regards to the retention of data for the purpose of non-serious criminal offenses. This is therefore another major pitfall in the DRD, the consequences of which extend its effects to the entire field data privacy in telecommunications.

(18) Regarding the provision under which the DRD must be implemented by member states no later than September 15, 2007, we have to emphasize that such a period was too short, especially when you consider the complexity of the matter in presence. There is no better proof of this as the fact that sixteen out of twenty-five member states submitted, at the time of adopting the Directive, exceptions under art. 15.3 DRD to delay transposition for eighteen months, with regard to the conservation of data communications, internet access, internet telephony and email.

(19) Compliance with the requirements of the Directive entails significant economic burden for providers of electronic communications services, with no benefit for these companies. Although the DRD does not provide any financial compensation for operators, put the whole burden on the operators has negative consequences in term of services cost. First, it can be assumed that the safety measures are not being as appropriate as necessary, in order to save in costs. Second, the increase in costs will be eventually charged to the European users.

(20) The transposition of the DRD has been problematic and unsatisfactory. The problematic aspect of the process is apparent from the fact that, as of June 2011, the transposing legislation was only in force in twenty out of the twenty-seven member states. Sweden still has to implement it, and other three have seen their transposing legislation overturned by its constitutional courts—namely, Germany, Czech Republic, and Romania. Apart from these decisions, other constitutional courts have heard cases regarding the transposition of the DRD, with no serious consequences. Such is the case

of Bulgaria, whose transposing law had to be revised; Cyprus, where it was considered that judicial decisions under the national law were unconstitutional; and Hungary, where it is pending a case concerning the failure by the legislative to specify for which purposes the data can be treated.

Given the high volume of litigation that the DRD has caused, it is not surprising that the European Commission expressed in its 2011 Assessment Report its willingness to reconsider all the issues raised by constitutional courts in its future proposal for revision of the data retention framework. In any event, the unceasing judicial activity around the DRD on both EU and national levels is probably the best evidence of the existence of many defects in the current statute.

(21) The transposition can be described as unsatisfactory because, as the European Commission admitted itself, the DRD has not fully harmonized the data retention legislation, nor has created a levelled playing field for operators. Significant differences in relevant aspects still remain in national legislations, such as the limitation and purpose of the retention, data access, data security, storage period, or the reliability of the statistics collected.

(22) While it is true that all EU countries have now data retention legislation in force thanks to the DRD, the fact remains that many of these regulations present serious flaws that put in jeopardy—when they do not clearly violate—fundamental rights. The European Commission itself has admitted that the Directive does not guarantee that the concerned data can be stored, retrieved and used with full respect for the rights to privacy and data protection. However, the institution has tried to pass the buck for these results by holding that the responsibility for ensuring these rights lies with the member states and that the Directive seeks only partial harmonization on data retention legislation.

In any case, the shortcomings that we have shown throughout this analysis of the body of the Directive explains why, at the time of transposition, there was no common approach in implementing the provisions of the Directive—e. g., when it comes to the retention periods or the reimbursement of data retention cost—. Beyond the amount of flexibility expressly sought by the DRD, differences in the national implementation of

data retention have posed risks for European citizens' rights, as well as unnecessary hardships for operators.

Conclusions from Part Two: Fundamental Rights in Directive 2006/24/EC of 15 March 2006 on Data Retention

(1) Since the first hour, whether or not the regulation at stake violates fundamental rights has been the object of heated debate, particularly from those actors promoting data protection, privacy and secrecy of communications rights. In fact, the legality of the DRD depends on the compatibility of its provisions with the ones in the Charter of Fundamental Rights of the European Union (CFR) which under Art. 6 Treaty of the European Union (TEU) has become now primary law of the European Union. Any rule or act falling within secondary law—including directives—must comply with the Charter under penalty of being declared void.

(2) There is a general agreement that the content of the DRD limits certain freedoms that individuals enjoy in a democratic system. The European Commission itself admitted this when presenting the draft of the Directive, but contended that such limitations were proportionate and necessary to reach the goal of fighting crime, in particular, terrorist threats. Some of the institutions—namely, the EESC, the WGA29, and the EDPS— issued opinions during the legislative proceedings for the DRD which were very critical about fundamental rights treatment and, in particular, personal data protection (art. 8 CFR) and right to privacy (art. 7 CFR). The analysis of all these reports shows the general agreement on how the measures contained in the DRD do involve a significant limitation of certain fundamental rights.

(3) In particular, the fact that the data retention measures imposed by the Directive is a limitation on the right to privacy and confidentiality of communications (Articles 7 and 8 CFD) has been acknowledged by the European Commission in both the preamble of the DRD and in the evaluation report. The reports elaborated by independent agencies stressed this aspect as well. The DRD has a direct impact on privacy rights where

examined under the European Court of Human Rights (ECtHR) caselaw, which considers the storing information about an individual as an interference with private life, even though it contains no sensitive data.

(4) With regard to the secrecy of communications, ECtHR caselaw expressly recognizes the possibility that the right may be violated by the use of a technical device that records which phone numbers have been dialed on a particular device, but not the content communication itself.

(5) Besides the right to privacy, the DRD also affects the fundamental right to personal data protection, a group of guarantees on privacy proclaimed by both Art. 8 CFR and Art. 16 Treaty of Lisbon.

(6) The provisions of the DRD were intended to fit in the legal framework of rules and guarantees that has traditionally surrounded data protection. As it happens, the Directive ended up having a huge negative impact on those principles recognized by the European law. Data are retained for a period much longer than the one applied by providers of publicly available electronic communications or by a public communications network, running up to twenty-four months. Unlike the Directive 2002/58/EC, which attempts to protect confidentiality, the introduction by the DRD of the obligation to retain data creates substantial risks for owners of these data. The creation of databases may also encourage the so-called "fishing expeditions," i.e. completely random police investigations in which investigators revise documents and personal items without having any clear idea of what kind of crime or evidence is pursued.

(7) Once we have demonstrated above the way the data retention obligation impacts the rights to privacy and personal data protection, its legality under European law remains to be examined at length.

(8) The ECtHR and the EU Court of Justice caselaw have specified in which cases and on what conditions it is permissible for a public authority to interfere with the exercise of fundamental rights. Namely, any limitation must first be established by law with

enough precision to prevent arbitrary government action—and inform the citizens about the potential interference—. Second, the purpose of the interference must be legitimate: it must be necessary to achieve an objective of general interest, to protect the rights and freedoms of others, and to relate to any of the categories recognized by Art. 8 ECHR: "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." Third, the interference with the rights must be proportionate to the aim pursued and respect the essential content of the concerned fundamental rights. Proportionality unfolds into two elements: (a) the search for a less aggressive alternative to achieve the intended purpose; and (b) a weighting of the relevance of the right in question against the public purpose to be achieved. If the law is sufficiently important and there are alternative means to achieve the public purpose, the law will not be upheld.

(9) The requirement of legal provision presents two levels. On one hand, the issue of whether the legal basis of the Directive was valid. On the other, the so-called quality of the act. Viewed from both sides, we can only conclude that the right-limiting measures introduced by the DRD do meet the requirement of legal provision as demanded by the European Union legal framework.

(10) As for the so-called quality of the law, the requisite imposed by Art. 52.1 CFD and Art. 8 ECHR is met as long as any European or national law is predictable and accessible to the public. Applied these parameters to the DRD, the Directive regulates with enough detail the main aspects of the data retention policy, namely: objective and scope (Art. 1 DRD), definitions of the major elements of the regulation (Art. 2 DRD), obligation to retain data (Art. 3 DRD), access to data (Art. 4 DRD), categories of data to be retained (Art. 5 DRD), retention period (Art. 6 DRD), basic data security measures (Art. 7 DRD), storage requirements for retained data (Art. 8 DRD), and other aspects of the retention measure in sufficient abundance to exceed the quality requirement of the CFR and ECtHR case law.

(11) As to the question of the legal basis, it must be said that the content of the DRD replace conflicting national standards on the matter, specifying the circumstances under

which providers are required to keep the data for criminal investigations. Any interference, like the retention and use of traffic data to help criminal investigations, had to be authorized by law: it has so occurred.

(12) Turning to the next requirements of Art. 8 ECHR, the measure must necessarily pursue a legitimate goal. In this regard, Art. 1.1 DRD sets the obligation to retain data to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. Art. 82 Treaty of Lisbon *et seq.* vest the Union with authority on judicial cooperation in criminal matters, including the investigation, detection and prosecution of serious crime. The obligation created by Art. 1 DRD thus falls within the objectives of general interest recognized by the Union (art. 52.1 CFR) and, consequently, satisfies this aspect of the proportionality test.

(13) Before addressing the proportionality test *stricto sensu*, we have to make a brief reference to two other parameters that, in the case of DRD, are not relevant because they are readily determinable; namely, the criteria of necessity and adequacy.

The adequacy requirement only demands that the measure is not manifestly inappropriate to its goals, such as the ECtHR caselaw holds. Applied to our case, the retention of data as regulated by the DRD is adequate to achieve the goal expressed in art. 1.1 DRD.

Regarding the requirement of necessity of the measure, data retention may be considered necessary only if it is the least invasive measurement available among those which could achieve the goal expressed by Art. 1.1 DRD: the "investigation, detection and prosecution of serious crime." Of the three purposes, it is "detection" the one which enable the DRD to pass the necessity test. While interception of a suspect's telecommunications or quick-freeze procedures might be sufficient for the investigation and prosecution of serious crime, they are not suitable alternatives for the detection of these crimes since both require that the crime—or at least one potential perpetrator—has already been detected. Thus, the detection of serious crime makes the DRD retention measures be classified as "necessary" for purposes of the test of legality.

(14) It is a general principle of EU law that any limitation of a fundamental right must be proportionate to the general interest, necessary, and respectful of a minimum set of guarantees. When the matter involved is data protection, such judgment is guided by the more specific guarantees provided by Convention 108. In any case, the implications of the principle of proportionality can only be assessed in light of its concrete manifestations. Applied to the DRD, the three relevant areas to examine are as follows: the proportionality of the data retention blanket measure, the retention periods, and the substantive nature of the information to be retained.

(15) The reasons supporting which is or which is not proportional in the DRD are subject to constant variation, since the measure is designed to prosecute crimes in the technology arena, an area in constant evolution. The introduction of general surveillance may start a spiral of potential violations of the fundamental rights of citizens difficult to stop. Hence the need for proportionality considerations should at least be evaluated periodically and the results be published.

(16) Two of the most controversial aspects of the debate on the proportionality of the DRD are the retention periods and the amount and nature of the data to be retained. As to the first, the duration of data retention demands to weigh the pursued aim (securing the provision of data retained to the authorities) against the right to personal data protection. The longer the data processing runs, the more harmed the right gets. Different periods depending on the crime investigated could have been a good solution in this regard. However, this has not been the case with the DRD. According to the arguments put forward during the proceedings, the best parameter of the proportionality in order to set maximum periods would have come from getting precise practical data, supported by evidence, about the use of the data for the authorities.

(17) As for the proportionality of the DRD regarding the categories of data to be retained, the selection of them is not a neutral decision. Information such as the identity of the senders and receivers of communications, their physical location, or the duration and frequency of the communications are elements that invade the users' privacy and, in some cases, other rights such as professional secrecy. The legislative and later the judge must carefully weigh the different interests at stake, applying a reasoned

proportionality test in which the general and specific circumstances concurrent must be taken into account.

(18) With respect to the selection made in the abstract by the European legislative power, it should be criticized that the list of data to be retained is an exhaustive one, binding on each of its points, instead of a maximum from which the states could exception whichever they may want.

Conclusions from Part Three. Law 25/2007, on October 18, on Data Retention

(1) The general duty of preserving electronic data traffic is not entirely novel in our national law. A previous internet-regulatory act contained a similar regime which did not enter into force because of lack of the necessary regulatory development by the government.

(2) The RDA places itself in the middle between telecommunications law—insofar as it establishes a number of administrative obligations on the telecom operators—and criminal procedure—insofar as such obligations are meant to facilitate the prosecution of serious crime. The result is a set of public law rules which could lead to a severe limitation of fundamental rights of growing importance today.

(3) The RDA stands as a broad exception to many general principles of telecom law. The severity made the legislative add a final provision in the act, introducing a new paragraph to Article 38.5 of the Telecommunications General Act, providing that all the traditional principles are established without prejudice of the obligations of the RDA.

(4) From the perspective of criminal procedure, we must emphasize that the Spanish legislative has traditionally been reluctant to establish a detailed regulation concerning the contents of communications interception, even before the digital age. Spain has kept falling behind the meticulous regulation of the telecommunications sector carried out by European Union law. At least, though, the Spanish legislative has implemented all the reforms coming from Brussels, most of them focusing on the risks of anonymity in

telecommunication networks and its potential to become a suitable tool for conducting criminal activities through the network.

(5) The drafting of the transposition of the DRD was carried out by the Spanish executive without the care and accuracy required. For example, the file for the first draft of the law did not include all requests and opinions submitted by the telecom sector. Neither did the record give explanations about the reasons why the executive accepted or not the proposals, suggestions, and comments made by the agencies and entities which issued opinions on the draft. The explanatory report limited itself to make a short, general reference to the need and opportunity of the legislation, based on its mandatory implementation of the DRD, without explaining why to adopt a particular solution over others.

(6) Another flaw in the bill sent by the executive to the parliament was the absence of data on the economic effects that the measures were to have on the market. Although the financial report included a third section about economic impact on the industry, its content simply distinguished between the costs of technical adaptations and administrative activities—without quantifying any of them. It also stated that a balance between the objectives and costs incurred it would also be taken into account. The information in the file was clearly insufficient for the parliament to make an informed decision on the possible impact of the draft in the telecom market.

(7) The central measure of the RDA is what has been called a blanket measure on data retention. The measure operates when the crime has not even happened, is purely hypothetical and there is no initial suspicion or indication. It just freezes data in huge databases so that they can be used as evidence on the infinitesimal percentage of occasions in which a crime takes place. This type of tool also involves the outsourcing of the government's essential task of preventing and prosecuting crime, burdening a private actor with it.

(8) In the Spanish case, the particular legal instrument—the RDA—had two main purposes, one immediate and another mediate. The first is the duty for operators to retain data categories set out in the act, a premise for the immediate purpose which is

stated in Article 1.1 RDA: the eventual transfer of the data to the authorized agents for the detection, investigation and prosecution of serious crimes under the penal code or special criminal laws.

(9) The concept of felony handled by Art. 1.1 RDA cannot be interpreted in the literal sense defined by Arts. 13.1 and 33.2 of the Spanish penal code. First, such an interpretation would be insufficient as it would lead us to use the RDA measures only to prosecute those offenses punishable with more than five years of imprisonment while excluding areas of criminal investigation certainly appropriate, such as possession and distribution of child pornography, some types of drug trafficking, bank robberies, and the like.

Second, the strict application of the provisions of Arts. 13.1 and 33.2 would be an arbitrary criterion for determining where the retained data can be used. As a matter of fact, the actual reason why the penal code qualified as serious criminal those offenses punished with more than five years of imprisonment does not lie on the type of crime. As the explanatory memorandum to the Law 15/2003 of 25 November makes clear, the will of the legislative was to differentiate the crimes to be heard by the *audiencias provinciales* from those to be heard by the *juzgados de los penal*. The Spanish legislative was lazy and sloppy to choose a direct translation of the term "serious crime" by the Directive 2006/20/EC. There is no logical, direct relationship between the tools provided by the RDA and the criminal cases heard by the *audiencias*.

(10) The list of data to be retained, as specified in Art. 3 LDC, is a faithful transcription of Art. 5 DRD. All the small differences of the Spanish version obey to didactic purposes or to an intended redundancy.

(11) The RDA transcends the classic concept of data traffic in two ways. First, the idea of abandoning the traffic data as a dynamic element: the law does not distinguish between the data captured when it is being generated and the data stored as personal data in a file. Second, the RDA uses a broad concept of data, including not only the essential components of traffic data (connected terminals, user identification and

communication) but also the location of the user. Both kinds of data are retained for potential use later.

(12) Another important aspect regarding the list of Art. 3 RDA is that the Spanish legislative has ignored the constitutional caselaw on the distinction between the formal and the substantial dimension of each communication. The lack of this distinction in the law may cause difficulties when it comes to geographical location data. The need to minimize these potential is one more reason to consider the list of Art. 3 RDA exhaustive, leaving no room for flexible application or analog.

(13) The general duty for operators to retain data from electronic communications (Art. 4 RDA) is a broad exception to the general principles of telecommunications law that until now meant to protect the rights to privacy, personal data protection and confidentiality of communications by preventing providers from using these data at will. Data treatment is generally subject to a number of principles for the benefit of the users, who must give their informed consent for the treatment. Otherwise, the companies have to make the data anonymous or cancel them once they are no longer needed for the purpose of the transmission of a communication.

(14) The legislative has strongly involved the telecom operators in the duty to cooperate with the criminal investigation, imposing on them the complex and expensive task of facilitating the technological and storage resources to retain data. Here lies precisely the essence of the act.

(15) In fact, the RDA has listed a number of data sources which were already supported by the jurisprudence of both the Supreme Court and the Constitutional Court. After its entry into force, the tools available to the authorized law enforcement agents now cover the entire spectrum of possibilities in data retention.

(16) The irruption of the RDA into the general regulation of telecommunications has led to the coexistence of two different regimes. On the one hand, a public-purpose file has been created by the RDA; the telecom companies have to store all the information requested by the law and make it available at the authorities' request. On the other

hand, the general principles on telecommunications law are still in force. The companies can use traffic data only for maintenance and billing purposes. This situation is likely to create complex areas of coexistence, at the expense of the users' privacy rights.

(17) Article 5 RDA provides that retained data will be eliminated twelve months after the communication took place. That period falls within the parameters established by the DRD and is the same amount of time established by Art. 12 LSSI. In any case, an explicit reference to the suppression of data is missing, although such should be the final destination of the retained data.

(18) However, while the one-year-long retention can be applicable to the dynamic elements of communications, it cannot be the case for certain static elements—for instance, the identity information of the users—as they are needed to maintain the contractual relationship with the operator.

(19) Article 8 rules on security of the data refer to the complex general rules on data protection provided Royal Decree 994/1999, of June 11, on security measures for automated files containing personal data. However, the referral in bloc to such legislation forgets that the decree establishes three different levels of security in storing personal data—low, medium and high—. It would have been very advisable that the law specified which level is required for the retained telecom data.

(20) Particularly objectionable is Art. 6.2 RDA, specifying what public authorities are considered "authorized agents" to collect the retained data. The RDA seems to use a notion of criminal procedure in which the investigation is generally attributed to the police and the judge limits himself to grant warrants. The legislative ignored that in our criminal procedure the investigation corresponds to the *jueces instructores* and, where necessary, to the public prosecutor. The judicial police acts under their supervision. However, Art. 6.2 RDA identifies as recipients of the transfer of the retained data the authorized agents, with no mention to judges or prosecutors, who should be the recipients of the information. The judicial police access that information only to the extent that they act as auxiliaries to them.

(21) Since a judicial warrant is always required, the logical step is that the data be transferred to the court, which decides whether or not to forward them to the law enforcement agents. The only cases in which the police, based on their own powers, should be considered a direct addressee of the retained data is for prevention of crime—a task that does not correspond to the judicial police and therefore, under the RDA, does not legitimize the transfer of data.

(22) RDA leaves to the discretion of the judge to decide what is proportional and reasonable when granting a warrant for the transfer of the retained data. However, the requirement that the execution time of the warrant is set by the judge based on the nature and technical complexity of the operation" is not the most prudent approach. The judicial authority may not be the most competent to determine the technical complexity of the operation, which will depend on each operator and its technology.

(23) With regard to the judicial decision authorizing the data transfer, this should adopt the form of *auto*. The reference in Art. 7.2 RDA to the Criminal Procedure Act should be interpreted as an allusion to the need to restrict the transfer to those data strictly necessary.

(24) Regarding the duty by Art. 9.1 RDA to seek the consent of the concerned person, we note that, although Art. 6.1 Data Protection Act establishes that the treatment of personal data requires the consent of the concerned person, the same article ends up adding "unless the law provides otherwise." The transfer of the retained data under the warrant is excepted from the principle of consent with full legitimacy.

(25) Since the data transfer must be approved by the court, it makes sense that the court is the one which balances the different interests at stake—by weighing the needs of the investigation against the fundamental rights—. The owner of the data has his rights protected and, at the same time, is prevented from hiding information or altering his behavior.

(26) Despite the financial burden placed on the providers of electronic communications

services, neither DRD nor RDA have provided for their economic compensation. Actually, in the Spanish case the question of the costs and the impact of this reform in the telecommunications market was hardly considered by the legislative. In the financial report attached to the bill, a third section assessed he economic impact of the legislation on the industry, but its content was limited to a few irrelevant comments about the distinction between the costs of technical adaptations and the cost of administrative activities. The Spanish government paid no attention to the observations and proposals from the subjects affected by the regulation.

(27) In view of current economic hardships Spain and many other EU member states are going through, the possibility of financial compensation for operators at the expenses of national budgets has become most unlikely, particularly considering the urgent need to reduce public spending.

Conclusions from Part Four: Constitutionality of the Law 25 /2007 of October 18.

(1) The measures introduced by the RDA are a clear limitation to fundamental rights, particularly those recognized by Art. 18 of the Spanish Constitution (SC): privacy and secrecy of communications. The mere prospect that all external data from our phone and internet communications are to be preserved for a period of twelve months seems itself remarkably invasive.

(2) For the norm in presence to be legitimate, its compatibility with the Constitution must be established. In particular, the RDA needs to respect the classic requirements of any restriction of fundamental rights, namely: legal provision, judicial control, and strict observance of the principle of proportionality. This last principle requires three specific conditions: suitability of the measure to achieve a constitutionally legitimate goal, necessity—i.e. no other less onerous measures are equally suitable—, and the sacrifice imposed on the fundamental right not be excessive—test of strict proportionality—.

(4) Various aspects separate classic telecom wiretapping (regulated in detail by the Criminal Procedure Act) from external data communications. The main distinction is that RDA imposes the obligation for operators to keep each and every data of an electronic communication—except the contents—for a period of twelve months. Thus, the real threat for the fundamental rights does not lie on the data transfer—which falls under prior judicial scrutiny—, but on the fact that huge amounts of private information is stored for potential investigation purposes.

(5) It must also be stressed that we are not before a purely procedural rule but, above all, before an administrative rule requiring operators to intercept the data generated by the services they provide to their customers.

(6) Secondly, this is not an investigation measure to be used within the framework of criminal proceedings. No crime has been committed or is being investigated at the time that the fundamental rights are limited. A massive electronic data retention takes place; the data are not put in the hands of the judge or judicial police but remain stored for twelve months.

(7) Third, none of these data retention actions are done under judicial control. The RDA directly and generically prescribes the actions to be carried out.

(8) Fourth, the measure does not affect a particular individual in a particular investigation, but to anyone who uses the phone or the internet, which in practice involves all citizens in their the daily life interactions. This aspect has to be taken into account to assess the proportionality of such regulation.

(9) Another key feature of the RDA is that is not the government, but private entities, which carry out the interference. All external aspects of each telephone or internet communications over the last twelve months are kept by private telecommunications companies and under their responsibility. The creation and maintenance of such huge mass of personal information rise a critical area of vulnerability and a potential threat to the privacy of every citizen, even though the companies are subject to a strict liability regime and have to comply with safety obligations.

(10) Which fundamental rights are affected by the central measure of the RDA is a controversial question. Some hold that the action by which the operator must retain the data listed in Art. 5 RDA and store them in databases at the disposal of the authorities affects the right to secrecy of communications and the right to data protection.

(11) According to a second theory, the data are not really retained *ex lege*, since they are already legitimately in the companies' possession. Consequently, there would not be interference with the right to secrecy of communications: the only right affected by the measures of the RDA would be the personal data protection rights.

(12) For the reasons explained, we believe that in the Spanish system of rights, the capture and transfer of data by the operators would be deemed a restriction of the right to secrecy of communications, while retention per se would limit the right to personal data protection.

(13) Whatever theory is preferred, the fact is that the vast majority of the data falling within the RDA scope involves the right to secrecy of communications. The Constitutional Court has made clear several times that these external data of communications are formal aspects whose transfer requires a judicial warrant since the mentioned right is being affected. This doctrine is fully applicable to RDA retained data access.

(14) The subscribers' data undoubtedly fall under the fundamental right to data protection. As to the location and traffic data, strictly speaking, they turn to be protected by this right once they got stored in the telecom's databases, and therefore, their protection must be consider under different parameters when determining applying the proportionality test.

(15) The RDA introduces a severe exception in the regulatory framework of telecommunications data protection. Regarding the subscribers' data, the general rule is that they must be eliminated when become unnecessary for billing purposes. With the

RDA, now the providers will have to keep this kind of personal information twelve months after the contractual relationship has ended, regardless the subscriber's desire.

(16) The principle of legality is a common requirement for any governmental action intending to limit a fundamental right. By express mandate of the Constitution, any government interference with fundamental rights and public freedoms requires a legal provision. The standard to be met here is that the rules are clear and foreseeable enough. A detailed analysis of the RDA shows that the act meets this requirement.

(17) More questionable is the observance by the RDA of the second requirement. Art. 81.1 of the Constitution requires that legislation regulating fundamental rights and civil liberties must take the form of *ley orgánica*. The fact that the RDA is a *ley ordinaria* led to a majority of voices, including the Supreme Court, to question its constitutionality. Passing the RDA as a *ley orgánica* would have cleared up this serious problem.

(18) Moreover, the constitutional caselaw requires not only that government interference is governed by the principle of legality, but also that the act is detailed enough (accuracy), in the sense that it uses terms that are sufficiently clear to indicate—in RDA case—under what circumstances and under what conditions both operators and public authorities can retain and transfer the data traffic. For wiretapping rules—a matter close to the RDA—the requirements are as follows: definition of the categories of persons to be subjected to wiretapping: nature of the offenses investigated; the duration of the measure, precautions to be observed, control by the judge, destruction of the recordings, etc.
If we apply these criteria to the RDA, we find that the act does not meet some of them. The transfer standards in Art. 7.2 RDA are regulated in a manner so vague that is clearly insufficient to meet requirements of the caselaw regarding quality and clarity of the act.

(19) The lack of full regulation of electronic communications retention and transfer harms the effectiveness of the law enforcement agent, who may find their investigation

void as unlawful evidence. Therefore, it is highly desirable that the inaccuracies of the RDA are remedied as soon as possible by the legislative.

(20) The second requirement for the restriction of fundamental rights by the law is judicial control through a warrant. Fortunately, this is as unquestionable condition in the RDA for the transfer of data. The court will decide on all occasions according to the principles of necessity and proportionality. In fact, only when all the conditions are observed the evidence will be admitted in criminal proceedings.

(21) It is not enough that the measure is provided by the RDA and "administered" through judicial warrant and supervision. The regulation of the RDA has to be subjected to the strictest observance of the principles of adequacy, necessity and proportionality *stricto sensu*.

(22) The creation *ex lege* of a general data retention duty is the central issue of the RDA, when it comes to the proportionality of the interference with fundamental rights. The act establishes a legal mandate directed to the suppliers, regardless of any particular factual circumstances.

(23) The duty to retain data that might eventually be useful in the investigation of a specific serious crime is a blanket measure. Such a broad duty does not meet the principle of circumstantial-evidence intervention that our constitutional system requires where it comes to restricting fundamental rights. The measure is based on the assumption that any citizen might commit a serious crime and, consequently, all communications data traffic is massively retained to facilitate prosecution.

(24) There are some uncircumstantial-evidence measures, such as security measures in airports and banks which are justified by the special circumstances and the potential danger present at those places. However, our contention is that the regular use of communication networks is not in itself a danger, all the more when one considers that phone calls and the internet are now part of our daily lives. A generic risk does not constitutionally justify the legitimacy of the blanket measure set by RDA.

(25) Data retention is not intended to criminal investigation directly but indirectly; it takes place before the commission of the offense, and even before the suspicion that may be committed. Therefore, we are before prospective measures of prevention, whose legitimacy has been excluded by the Constitutional Court. For an intervention of this type to be valid in our system, at least the summons must have been opened. All these requirements are not present in the RDA.

(26) The literal interpretation of the notion of "serious crime" in Art. 1.1 RDA leads to unsatisfactory results. It is the judicial authority who ultimately has to assess to what extent felony falls within a serious crime for the RDA purposes. Given the doctrine of the Constitutional Court on the characterization of the concept of a felony, there is no doubt its application to important areas of research beyond the limits set by Arts. 13.1 and 33.2 of the Penal Code. All this regardless of the fact that the legislative should have been more specific in determining which criminal offences justify the use of the retained data.
These conclusions are reinforced if we look at the issue strictly from the perspective of our constitutional system of rights and from the point of view of European law.

(27) The RDA measures cannot be used for the investigation of nonserious crimes, but the ordinary rules of the Criminal Procedure Act. It is strictly prohibited to apply the RDA measures to misdemeanors. The retained data are not available for civil matters either. Furthermore, the legislative has no obligation, deriving from Art. 24 SC, to provide or facilitate evidence in civil proceedings.

(29) For the reasons explained above, there is a general agreement on the part of jurists, independent agencies, and other analysts on considering that the impact of the RDA and DRD on the citizens' fundamental rights is excessive and disproportionate. Therefore, in light of a future reform of these two pieces of legislation, we expect that the legislative do a better job in balancing the different interests at stake, this time based on accurate empirical data, so that the retention periods and the categories of data can be reduced to match the real needs of the law enforcement actors in a way more respectful with the fundamental rights proclaimed by the Spanish Constitution.

Conclusions from Part Five: Special Regime on Telephony Services through Prepaid Cards

(1) With no basis on any provision of the DRD, a final additional disposition (FAD) of the RDA introduces a special regulation for telephony services through prepaid cards. The purpose of the FAD was to close the door to the anonymity provided by these popular and economical cards.

(2) The first section of the FAD provides for the first time in Spanish law a duty for operators of mobile telephony services to keep a log-book stating the identity of customers who purchase prepaid smart cards.

(3) The actors required to comply with the duty are the operators of mobile telephony services of prepaid cards with activation system mode. The personal scope largely overlaps with the one of art. 1 RDA for data retention, which is certainly questionable, since in practice the recipients of such data are mostly people who have nothing to do with the operators concerned. Those holders are now indirectly responsible for the conservation of customers' sensitive data.

(4) The information stored is subject to the same principles of quality, conservation, not manipulation, and limited access as the other data retained under the RDA. In practice, retailers have to immediately transfer the data to the telecommunications company, which is the real subject to the rule. As there is no file sharing—and no agency relationship between the parties—the data collected has to be transfer without delay to the operators, which have to keep the log-book pursuant to Art. 11.2.a) of the Data Protection Act. In practice, what happens is that the operators get a hardcopy of the log-book from the retailer, who sends the data without keeping a copy. Others operators have temporary storage systems that send the information automatically to their databases.

(5) Operators must transfer the data where they are so required by agents authorized pursuant to Art. 6.2 RDA: members of the national police forces and security forces of

the autonomous communities with responsibility for the protection of persons and property and for the maintenance of public security in the course of the safety investigations persons or entities. Although the wording of the provision gives the impression that the authorized agents are more than those in Art. 6.2 RDA, the fact is that this crime investigation prior to court action entails duties proper of the judicial police so, actually, it is the same set of agents that are authorized under the RDA to access the retained data pursuant to Art. 5 RDA.

(6) A crucial difference between the FAD regime and the RDA regime is the type of crimes that enable access to stored data. While in the later is only serious crimes, in the former may be any offense in the penal code or in special criminal laws. Obviously, the definition makes possible to use the data for any crime different from misdemeanors.

(7) Unlike what happens in the case of the transfer of data communications under the RDA, the FAD applies beyond crime investigation, and extends its scope to crime prevention as well. Section 2 FAD can be read to extend the purposes of data transfer not only for the investigation, detection and prosecution of any offense under the penal code or special criminal laws, but for any other purpose of the authorized agents. Any investigation or crime detection activity can be covered by this section.

(8) The interpretation of section four of the FAD cannot lead us to conclude that no court permission is required for access and transfer of data stored in the log-book, although the text has not clarified this point. Viewed from the perspective of the proportionality of the measure, the transfer of the identification data is even more burdensome for the right to privacy than the general measure set by Art. 5 RDA, since it clearly identifies the persons. Therefore, what the FAD actually carries out is to make create a file of personal data with specific content which falls under Art. 3 RDA. The operators have now a duty to identify the purchaser of prepaid cards, and the information collected gets fully integrated into the common rules imposed onto operators.

The solution to the underlying constitutional issue is to be found in the natural extension of the need for judicial authorization contained in Art . 6.1 RDA to the customers data kept in the log-book.

(9) The main objection against the measures introduced by the FAD is that it is an aggravation of the indiscriminating blanket measure established by the RDA. For the sake of efficiency, the data retention extends to new categories of personal data and for new purposes, such as the prevention and investigation of any crime, serious or not.

(10) The intended purpose of the FAD has been achieved only partly, for it covers a very specific segment of the spectrum of possibilities of anonymous surfing on the telecommunications networks.

BIBLIOGRAFÍA

Documentación oficial citada

Conclusiones de la Presidencia con motivo del Consejo Europeo de Bruselas, de 16 y 17 de junio de 2005[1195]

Decisión de la Comisión, de 25 de marzo de 2008 , por la que se crea el grupo de expertos Plataforma para la conservación de datos electrónicos con fines de investigación, detección y enjuiciamiento de los delitos graves *Diario Oficial n° L 111 de 23/04/2008 p. 0011 - 0014* [1196]

Declaración del Consejo Europeo sobre la lucha contra el terrorismo, de 25 de marzo de 2004[1197]

Declaración del Consejo Europeo sobre la Respuesta de la UE a los Atentados de Londres de 13 de julio de 2005, en sesión extraordinaria[1198]

Dictamen 4/2005 del Grupo del Artículo 29, adoptado el 21 de octubre de 2005 (1868/05/ES. WP 113), sobre la Propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005)438 final de 21.09.2005][1199].

[1195] http://ue.eu.int/ueDocs/cms_Data/docs/pressData/es/ec/85347.pdf

[1196] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:111:0011:0014:ES:PDF

[1197] http://www.realinstitutoelcano.org/especiales/atentados/docs/declaracterrorUE25304.pdf [buscar link oficial}

[1198] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/es/jha/85826.pdf

[1199] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp113_es.pdf

Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE» COM(2005) 438 final — 2005/0182 (COD) (2006/C 69/04) Diario Oficial de la Unión Europea de 21 de marzo de 2006 (C 69/16 - C 69/21)[1200]

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final] (2005/C 298/01), publicado en el Diario Oficial de la Union Europea el 29 de noviembre de 2005, C 298/1 a C 298/12)[1201]

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105 de 13.4.2006, p. 54/63)[1202]

Informe de Evaluación de la Comision al Consejo y al Parlamento Europeo sobre la Directiva de conservación de datos (Directiva 2006/24/CE) (COM(2011) 225 final), de 18 de abril de 2011[1203].

Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE (presentada por la

---

[1200] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:069:0016:0021:ES:PDF

[1201] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_ES.pdf

[1202] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:ES:HTML

[1203] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:ES:PDF

Comisión) {SEC(2005) 1131}, Bruselas, 21.9.2005 ;COM(2005) 438 final; 2005/0182 (COD)[1204]

Dictamen del Consejo de Estado, de 22 de febrero de 2007, sobre el Anteproyecto de Ley de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (n. expediente 32/2007)[1205]

Bibliografía

Abril, R., "De Guantánamo a Bagdad. Estatuto jurídico y trato a los detenidos en la lucha contra el terrorismo", en *REEI*, n. 9, 2005, pp. 1 y ss.

Ackerman, B., "Don"t Panic", en *London Review of Books, n.* 24(3), 2002. Disponible en http://www.lrb.co.uk/v24/n03/acke01_.html. — "The Emergency Constitution", en 113 *Yale Law Journal*, 2004, pp. 1029 y ss. —*La costituzione di emergenza. Come salvaguardare libertá e diritti civili di fronte al pericolo del terrorismo*, tr. it., Meltemi, Roma, 2005. Hay traducción al español: *Antes de que nos ataquen de nuevo. La defensa de las libertades en tiempos de terrorismo*, Ediciones Península, Barcelona, 2007.

Adams, J, *Risk*, University College London Press, London, 1995. —"The World's Biggest Ideas: Risk", en *New Scientist*, 187: 2517, 2005.

Aguado, C., "Sentencias de control de Leyes", en *Actas de las IX Jornadas de la Asociación de Letrados del Tribunal Constitucional. Extranjería e inmigración*, Colección Cuadernos y debates por el Tribunal Constitucional y el Centro de Estudios Políticos y Constitucionales, pp. 115 y ss.

Ahmed, n. M., *Guerra alla libertá. Il ruolo dell´amministrazione Bush nell´attacco dell´11 settembre*, Fazi, Roma, 2002.

Aláez Corral, B., "Defensa de la Constitución, libertad de expresión e información y principio de proporcionalidad (a propósito de la STC 136/1999, de 20 de julio de 1999)", en *Repertorio Aranzadi del Tribunal Constitucional*, T. III, 1999, pp. 2567 y ss.

Álvarez García, F. J., "La legislación antiterrorista: una huida hacia el derecho penal", en *RFDUC*, n. 68, 1983, pp. 161 y ss. —"Principio de proporcionalidad. Comentario a la Sentencia del Tribunal Constitucional de 20 de julio de 1999, recaída en el recurso de

[1204] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:ES:PDF

[1205] http://www.boe.es/aeboe/consultas/bases_datos_ce/doc.php?coleccion=ce&id=2007-32

amparo interpuesto por los componentes de la Mesa Nacional de Herri Batasuna", en *La Ley*, n. 4913, 26 de octubre de 1999, pp. 1 y ss.

Álvarez Rodríguez, M. C., "El Derecho en la regulación de las telecomunicaciones y la cuestión de la privacidad", en Abaco: Revista de cultura y ciencias sociales, n. 14-15, 1997, pp. 85-94.

Alvaro, A., *Report on the Initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the Retention of Data*, Committee on Civil Liberties, Justice and Home Affairs, European Parliament; A6–0174/2005, 31 de mayo de 2005.

Amnesty International EU Office *Human Rights Dissolving at the Borders? Counter-Terrorism and EU Criminal Law*, 31 de mayo de 2005.

Amoore, L. y Goede, M. de, *Risk and the War on Terror*, Routledge, London, 2008. — "Governance, Risk and Dataveillance in the War on Terror", en *Crime, Law and Social Change* 43(2), 2005, pp. 149–173.

Amoore, L., "Biometric Borders: Governing Mobilities in the War on Terror", en *Political Geography*, 25, 2006, pp. 336–351.

Anderson, R., Brown, I. *et al*., *Data Base State: A report Commissioned by Joseph Rowntree Reform Trust Ltd.*, Joseph Rowntree Reform Trust Ltd (ed.), Garden House Water End, York, 2009.

Andreas, P. "The Rise of the American Crimefare State", en *World Policy Journal*, 14(3), pp. 37–45, 1997. —"Smuggling Wars: Law Enforcement and Law Evasion in a Changing World", en *Transnational Crime in the Americas (*T. Farer, ed.), Routledge, New York, 1999, pp. 85–98.

Ansell, C. K., y G. Di Palma, *Restructuring territoriality: Europe and the United States compared*, Cambridge University Press, Cambridge, 2008.

Aradau, C., y Munster, R. van, "Governing Terrorism through Risk: Taking Precautions, (Un)knowing the Future", en *European Journal of International Relations* 13(1), pp. 89–115. (2007)

Araujo Boyd, M., "El Derecho de la competencia y las telecomunicaciones", en *Derecho de las telecomunicaciones* (coord. por Javier Cremades García), 1997, pp. 777-794.

Article par Article des Nouveaux Traitées Européens (TUE-TFUE)", La Documentation Française, Paris 2008.

Ash, T. G., "The Peril of Too Much Power", en *New York Times*, online edition, 9 April. (2002)

Ashby Wilson, R., *Human rights in the war on terror*, Cambridge University Press, Cambridge, 2005.

Asís Roig, A. de, "Protección de datos y derecho de las telecomunicaciones", en *Régimen jurídico de internet* (coord. por Miguel Angel Fernández Ordóñez, Javier Cremades García, Rafael Illescas Ortiz), 2001, pp. 201-228.

Avril, P. y Gicquel, J., "Le triomphe de l'entonnoir", en *Les petites affiches*, 15 de febrero de 2006, n. 33, pp. 6 y ss.

Badham, R. T., "Police in India to Monitor Cybercafes", 2005, disponible en: http://www.boston.com/business/technology/articles/2004/01/18/police_in_india_to_monitor_cybercafes/

Bainbridge, D. I., *EC Data Protection Directive*, Butterworths, London, 1996. — *Introduction to Computer Law*, 4th Edition, Harlow, Longman, 2000.

Baker, T., y Simon, J., *Embracing Risk: The Changing Culture of Insurance and Responsibility*, University of Chicago Press, Chicago, 2002.

Baldini, V., *Sicurezza e libertà nello Stato di diritto in trasformazione*, Torino, 2005.

Balibar, É., *We the People of Europe?,* Princeton University Press, Princeton, 2005.

Balzacq, T. "The three faces of securitisation: Political agency, audience and context", en *European Journal of International Relations* 11 (2), pp. 171–201. 2005.

Balzacq, T., Bigo, D., Carrera, S., y Guild, E., "Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats", en CEPS – Working Document,

Banks, C. P. (2004) "Protecting (or Destroying) Freedom through Law: The USA Patriot Act"s Constitutional Implications", in David B. Cohen and John W. Wells (eds) *American National Security and Civil Liberties in an Era of Terrorism*. New York: Palgrave MacMillan.

Barak, A., "Democrazia, terrorismo e Corti di giustizia", en *Giurisprudenza constituzionale*, 2002, pp. 3384 y ss.

Barak-Erez, D., "An International Community of Legislatures?", en *The least examined branch. The role of legislaturas in the Constitutional State* (eds. Bauman y Kahana) University Press, Cambridge, 2006, pp. 542 y ss.

Barbera, A., y Fusaro, C., *Il Goberno delle democrazie*, Il Molino, Bolonia, 1997.

Barbosa Delgado, F. R., "El servicio y acceso universal en el derecho de las telecomunicaciones y su aplicación en la libertad de expresión", en *Derecho Comparado de la Información*, n. 19, 2012, pp. 3-28.

Barnes Vázquez, J., "La internet y el derecho: Una nota acerca de la libertad de expresión e información en el espacio cibernético", en *Cuadernos de derecho judicial*, n. 6, 1997, pp. 233-272.

Bassu, C., "Libertá personale e lotta al terrorismo: i casi di Canada e Stati Uniti", en *Democrazia e Terrorismo* (coord. Groppi, Tania), Lezioni Volterrane, volumen I, Editoriale Scientifica, Napoli, 2005, pp. 425 y ss.

Baxter, W. P. 2003. "Has spam been canned? Consumers, marketers, and the making of the CAN-SPAM act of 2003", en *NYU Journal of Legislation and Public Policy*, 8 (1), pp. 163–177.

Beck, U., "The Terrorist Threat: World Risk Society Revisited", en *Theory, Culture & Society* 19(4), 2002, pp. 39–55.

Belda Pérez-Pedrero, E., "El derecho al secreto de las comunicaciones: algunos apuntes sobre su protección en las relaciones por correo electrónico", en *JIS 2000: III Jornadas sobre informática y sociedad* (coord. por Miguel Ángel Davara Rodríguez), 2001, pp. 73-86

Bellazzi, M., "I 'Patriot Acts' e la limitazione dei diritti costituzionali negli Stati Uniti", en *Politica del Diritto*, a. XXXIV, n. 4, 2003, pp. 681 y ss.

Beltrán de Felipe, M. y González García, J. V., *Las sentencias básicas del Tribunal Supremo de los Estados Unidos de América*, Centro de Estudios Políticos y Constitucionales, BOE, Madrid, 2005. —"Terrorismo y garantías individuales: la experiencia de los Estados Unidos", en *La seguridad integral europea*, Lex Nova, Valladolid, 2005, pp. 351 y ss.

Bemelmans-Videc, M., Rist, R. C., y Vedung, E., *Carrots, sticks & sermons: Policy instruments and their evaluation*, Transaction Publishers, New Brunswick, 1998.

Benazzo, A., "Corte Suprema e Inmigration cases: la dottrina del plenary power federale e l´astensione del controllo giudiziario en materia di immigrazione", en *Corte Suprema e assetti sociali negli Stati Uniti d´America* (1874-1910) (S. Volterra, dir.). —"Convenzione eruropea, misure d´emergenza e garanzie giurisdizionalei dei diritti dell"uomo", en *Rivista trimestrale di diritto e procedura civile*, 1993, pp. 1141 y ss. — *L´emergenza nel conflitto fra libertá e sicurezza*, G. Giappichelli editore, Torino, 2004.

Bennett, C. 1988. "Regulating the computer: comparing policy instruments in Europe and the United States", en *European Journal of Political Research*, 16 (5), pp. 437–466. —*Regulating privacy: Data protection and public policy in Europe and the United States*, Cornell University Press, Ithaca, NY, 1992. —"Understanding ripple effects: The cross-national adoption of policy instruments for bureaucratic accountability", en Governance, 10 (3), 1997, pp. 213–233.

Bennett, C., y Raab, C., *The governance of privacy: Policy instruments in global perspective*, MIT Press, Second ed., Cambridge, 2006.

Benvenisti, E., "National Courts and the War on Terrorism", *Enforcing International Law Norms Against Terrorism* (dir. Bianchi, A.), Oxford, Hart Publishing, 2004, pp. 307 y ss. —"United we stand: national courts reviewing Counterterrorism measures", en *Counterterrorism: Democracy's Challenge* (Bianchi & Keller, ed.), Hart Publishing, Oxford, 2008, pp. 250 y ss.

Bertram, E., Blachman, M., Sharpe, K., y Andreas, P., *Drug War Politics: The Price of Denial*, University of California Press, Berkeley, 1996.

Biersteker, T. J., "Counter-Terrorism Measures Undertaken under UN Security Council Auspices", en *Business and Security: Public–Private Relationships in a New Security Environment* (dir. Alyson J.K. Bailes e I. Frommelt), Oxford University Press, Oxford, 2004, pp. 59–75.

Bignami, F., "Protecting privacy against the police in the European Union: The data retention directive", 2006. —"The case for Tolerant Constitutional Patriotism: The right to Privacy before the European Courts", en *Duke Law School,* Vol. 41, pp. 212-249. Disponible en http://ssrn.com/abstract=1309823.

Bigo, D., "To Reassure, and Protect, After September 11", en *Social Science Research Council After September 11, 2001*. Disponible en http://www.ssrc.org/sept11/ essays/bigo.htm — "Security and Immigration: Toward a Critique of the Governmentality of Unease", en *Millennium*, 27, 2002, pp. 63–92.

Bigo, D., y Guild, E. (eds.), *Controlling frontiers: Free movement into and within Europe*, Aldershot, Ashgate, 2005.

Bird, J., "Terrorist Use of the Internet", en *The Second International Scientific Conference on Security and Countering Terrorism Issues*, Moscow State University Institute for Information Security Issues, 25–28 de octubre de 2006.

Birkland, T. A., "The world changed today: Agenda-setting and policy change in the wake of the September 11 terrorist attacks", en *Review of Policy Research*, 21 (2), 2004, pp. 179–200.

Birnhack, M. D., "Soft Legal Globalization: The Role of the EU Data Protection Directive in the Emerging Global Data Protection Regime", en *Tel Aviv University Law School, Law Faculty Papers*, Draft-Paper, Febrero de 2008. —"The EU Data Protection Directive: An Engine of a Global Regime", en *Tel Aviv University Law School, Law Faculty Papers*, Paper 95, 2008, Disponible en : http://law.bepress.com/taulwps/fp/art95

Bobillo, F. J., "Constitución y legislación antiterrorista", en *Revista de Estudios Políticos*, n. 48, 1985, pp. 47 y ss.

Bollo Arocena, M. D., "Hamdan v. Rumsfeld. Comentario a la Sentencia dictada por el Tribunal Ssupremo de Estados Unidos el 29 de junio de 2006", en *Revista Electrónica de Estudios Internacionales*, 12, 2006.

Bonetti, P., *Terrorismo, emergenza e costituzioni democratiche,* Il Mulino, Bolonia, 2006. —"Terrorismo, emergenza e principi fondamentali", en *Giurisprudenza costituzionale e principi fondamentali: alla ricerca del nucleo duro delle costituzioni: atti del Convegno annuale del Gruppo di Pisa*, Capri, 2005.

Bonner, D., *Executive measures, terrorism and national security: have the rules of the game changed*, Aldershot, Ashgate, 2007.

Bonnini, C., *Guantánamo, USA, viaggio nella prigione del terrore*, Einaudi, Torino, 2004.

Borzel, T., y Hosli, A., "Brussels between Bern and Berlin: Comparative federalism meets the European Union", en Governance, 16 (2), 2003, pp. 179–202.

Bowring, W., *The Human Rights Implications of International Listing Mechanisms for "Terrorist" Organisations*. OSCE/ODIHR – UN HCHR Expert Workshop on Human Rights and International Co-operation in Counter-terrorism, ODIHR.GAL/14/07. Disponible en http://www.statewatch.org/terrorlists/OSCE-UN-feb-2007.pdf

Brondel, S., "Le Conseil constitutionnel durcit sa jurisprudente sur le droit d"amendement", en *Act. Jur. Dr. Adm.*, 2006, pp. 172 y ss.

Brouwer, E., "Towards a European PNR System? Questions on the Added Value and the Protection of Fundamental Rights", en *Study for CEPS on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, 2009.

Brown, I., "The Law and Economics of Cybersecurity", en *Law Quarterly Review 123*, 2007, pp. 172–175.

Brown, I., y Korff, D., *Striking the Right Balance: Respecting the Privacy of Individuals and Protecting the Public from Crime*, Information Commissioner"s Office, Wilmslow, 2004.

Buergenthal, T., "To Respect and to Ensure: State obligations and Permissible Derogations", en *The International Bill of Rights. The Covenant on Civil and Political Rights*, Nueva York, 1981, pp. 74 y ss.

Bugnion, F., "El derecho de Ginebra y el derecho de la Haya", en *Revista Internacional de la Cruz Roja*, n. 844, diciembre 2001.

Bullard, A., *Human rights in crisis*, Aldershot, Ashgate, 2008.

Bunyan, T., "The Shape of Things to Come – EU Future Group", en *Statewatch*, 2008. Disponible en: http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf — *The War on Freedom and Democracy*, Statewatch Analysis 13, Septiembre 2002. Disponible en www.statewatch.org/news/2002/sep/analysis13.htm

Buzan, B., "Will the "Global War on Terrorism" be the New Cold War?", en *International Affairs*, 82(6), 2006, pp. 1101–1118.

C.A.S.E., Collective. "Critical approaches to security in Europe: A networked manifesto". En Security and Dialogue, 37 (4), 2007, pp. 443–487.

Cabañas García, J. C., "Crónica sobre la jurisprudencia del Tribunal Constitucional respecto del derecho fundamental a la tutela judicial efectiva (art. 24.1 CE)", en *La reforma constitucional: ¿hacia un nuevo pacto constituyente?. Actas de las XIV Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales – Tribunal Constitucional, Madrid, 2009, pp. 287 y ss.

Cabezudo Rodríguez, N., "La Administración de Justicia ante las nuevas tecnologías. Del entusiasmo a la desconfianza, pasando por el olvido", en *Revista Jurídica de Castilla y León*, n. 7, octubre 2005, p.188 y ss.

Cáceres Brun, J., *Manual básico de derechos humanos y derecho internacional humanitario*, Cruz Roja Española, Madrid, 2003.

Calamo Specchia, M., "Al vaglio del Conseil constitutionnel la loi anti-terroriste: il fine giustifica i mezzi?", en *Diritto pubblico comparato ed europeo*, 2006-II, G. Giappichelli Editore, Torino, pp. 722 y ss.

Cameron, I., "UN Targeted Sanctions, Legal Safeguards and the European Convention on Human Rights", en *Nordic Journal of International Law*, 72, 2003, pp. 159–214. — *The European Convention on Human Rights, Due Process and United Nations Security Council Counter-Terrorism Sanctions*, en Report for the Council of Europe, 6 de febrero de 2006.

Cancio Meliá, F., "Derecho penal del enemigo y delitos de terrorismo. Algunas consideraciones sobre la regulación de las infracciones en materia de terrorismo en el Código Penal Español después de la LO 7/2000", en *Jueces para la democracia*, número 44, 2002, pp. 19 y ss.

Cano Paños, M. A., "Respuestas legales al terrorismo yihadista. El ejemplo de Alemania", en *Athena Intelligence Journal*, vol. 3, n. 1, art. 5, 12 de marzo de 2008, disponible en www.athenaintelligence.org.

Carlile (Lord) of Berriew, *The Definition of Terrorism*, The Stationery Office, Cm. 7052, London, 2007.

Carlos Bertrán, L. de, y Cortina Navarro, S., "Telecomunicaciones y derecho comunitario", en *Noticias de la Unión Europea*, n. 84, 1992, pp. 19-28.

Cassel, E., *The war on civil liberties: how Bush and Ashcroft have dismantled the Bill of Rights*, Lawrence Hill Books, Chicago, 2004.

Cate, F. H., "The EU Data Protection Directive, Information Privacy, and the Public Interest", en *Iowa L. Rev.*, 80, 1994, pp. 431 y ss.

Cate, F., y Litan, R., "Constitutional issues in information privacy", en *Michigan Telecommunications and Technology Law Review*, 9 (1), 2002, pp. 35–63.

Cauley, L., "NSA has Massive Database of Americans" Phonecalls", en *USA Today*, 11 de mayo de 2006.

Ceccanti, S., *Le democrazie protette e semi-protette da eccezione a regola.prima e dopo le Twin Towers*, Giappichelli, Torino, 2004.

Cerri, A., "Legislazione dell"emergenza, cultura del sospetto, democrazia autoritaria", en *Intolleranza e società tra cultura e diritto*, Sapere, Roma, 2000, pp. 145 y ss.

Charlesworth, A., "Clash of the data titans: US and EU data privacy regulation", en *European Public Law*, 6 (2), 2000, pp. 253–274.

Chertoff, M., "The Tool We Need to Stop the Next Airliner Plot", en *Washington Post*, 29 de agosto de 2006 (edición online).

Chinchilla Marín, M. C., "El derecho a la ocupación del dominio público y de la propiedad privada necesarios para el establecimiento de redes públicas de telecomunicaciones", en *Telecomunicaciones: estudios sobre dominio público y propiedad privada* (coord. por M. Carmen Chinchilla Marín), 2000, pp. 93-148.

Coker, C., *Globalisation and Insecurity in the Twenty-first Century*, Oxford University Press, Oxford, 2002.

Cole, David, "Enemy Alliens", en *Stanford Law Review*, 54, 2002, pp. 954 y ss. —"Judging the Next Emergency: Judicial Review and Individual Rights in Times of Crisis", en *Michigan Law Review*, 2004, pp. 2565 y ss. —y DINH V., "Guantánamo: democrazia e non persone", en *Micromega*, n. 4, 2004, pp. 237 y ss. —*Enemy aliens: double standards and constitutional freedoms in the war on terrorism*, The New Press, New York, 2005, pp. 316 y ss. —"Rights over Borders, Transnational Constitutionalism and Guantanamo Bay", en *Cato Supreme Court Review*, 2007-2008, pp. 51 y ss. —Cole, D., y Dempsey, J. X., *Terrorism and the Constitution*, The New Press, New York, 2002.

Condorelli, L. y Sena, P. de, "Les droits de l"homme à Guantanamo: en attendant la Cour Suprême des Estats-Units", en *Libertés, Justice, Tolérance. Mélange en hommage au Doyen Gérard Cohen-Jonathan*, Vol. I, Bruylant, Bruselas, 2004, pp. 445 y ss.

Connolly, W. E., "The Complexity of Sovereignty", en *Sovereign Lives: Power in Global Politics* (eds. Jenny Edkins, Véronique Pin-Fat y Michael J. Shapiro), Routledge, London, 2004, pp. 23–40.

Consejo de Europa, *La lutte contre le terrorisme: les normes du Conseil de l"Europe*, Strasbourg, Edit. du Conseil de l"Europe, 2004. —*La LUTTE contre le terrorisme: les normes du Conseil de l"Europe*, Strasbourg, Edit. du Conseil de l"Europe, 2005. —*La lutte contre le terrorisme: les normes du Conseil de l"Europe*, Strasbourg, Edit. du Conseil de l"Europe, 2007.

Constantine, T. A., Testimony Before the Senate Judiciary Committee, Subcomittee on Technology, Terrorism, and Government Information, 3 de septiembre de 2007. Disponible en http://www.dea.gov/pubs/cngrtest/ct970903.htm.

Corte Heredero, N., "Crónica de de jurisprudencia constitucional en materia de derechos fundamentales", en *Actas de las X Jornadas de la Asociación de Letrados del Tribunal Constitucional. La Constitución europea*, publicadas en la Colección Cuadernos y debates por el Tribunal Constitucional y el Centro de Estudios Políticos y Constitucionales, Madrid, 2005, pp. 179 y ss.

Cortés López, A. M., "Aproximación al Derecho Comunitario en materia de telecomunicaciones", en *Telecomunicaciones por cable* (coord. por Enrique Arnaldo Alcubilla, Salvador Montejo Velilla), 2000, pp. 111-148.

Cotino Hueso, L., "Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías" (coord. por Lorenzo Cotino Hueso), 2011, pp. 386-401.— "Datos personales y libertades informativas : medios de comunicación social como fuente accesibles al público: Título I. Disposiciones Generales. artículo 3", en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (dir. Antonio Troncoso Reigada), 2010, pp. 295-321. —"Tratamiento jurídico y normativo de la democracia, participación y transparencia electrónicas: presente y perspectivas", en *Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías* (coord. por Jordi Barrat i Esteve, Rosa María Fernández Riveira), 2011, pp. 221-260. —"Propuestas para una eficaz campaña del bicentenario de la Constitución de 1812, especialmente en Internet", en *El legado de las Cortes de Cádiz* (coord. por Pilar García Trobat y Remedio Sánchez Ferriz), 2011, pp. 889-903. —*Libertades, democracia y gobierno electrónicos* (coord. por Lorenzo Cotino Hueso), Comares, 2006. —*Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (Lorenzo Cotino Hueso, coord.), Universidad de Valencia, 2011.

Cox, M., "Empire, Imperialism and the Bush Doctrine", en *Review of International Studies*, 30(4), 2004, pp. 585–608. — "Beyond the West: Terrors in Transatlantia", en *European Journal of International Relations*, 11(2), 2005, pp. 203–33.

Cremades Garcia, J., "El derecho de las telecomunicaciones en Europa y en España", en *Derecho de las telecomunicaciones* (coord. por Javier Cremades García), 1997, pp. 7-94

Crump, C., "Data retention: privacy, anonymity, and accountability online", en *Stanford Law Review*, 2003, pp. 191-229.

Cruz Villalón, P., *El Estado de sitio y la Constitución: la constitucionalización de la protección extraordinaria del Estado*, 1789-1878, CEC, 1980. —"La protección extraordinaria del Estado", en *La Constitución Española de 1978* (dir. A. Predieri y E. García de Enterría), Civitas, Madrid, 1981. —"El nuevo derecho de excepción (Ley Orgánica 4/1981, de 1 de junio)", en *REDC*, n. 2, 1981, pp. 93 y ss. —*Estados excepcionales y suspensión de garantías*, Madrid, Tecnos, 1984. —"Tres sentencias sobre el Decreto-Ley", en *El Gobierno en la Constitución Española y en los Estatutos*

de Autonomía, Diputación de Barcelona, 1985. —"Suspensión individual de derechos", en *Temas básicos de Derecho constitucional. Tomo III. Tribunal Constitucional y Derechos fundamentales* (Aragón Reyes, Manuel, coord.), Civitas, Madrid, 2001. —"Normalidad y excepción", en *REDC*, n. 71, 2004, pp. 232 y ss.

Cuerda Arnau, M. L., "Terrorismo y libertades políticas", en *Teoría & Derecho*, n. 3, 2008.

Cuerda Riezu, A., "Jurisprudencia constitucional en los procesos de amparo", en *Actas de las V Jornadas de la Asociación de Letrados del Tribunal Constitucional. El principio de legalidad*, Colección «Cuadernos y Debates», Tribunal Constitucional y el Centro de Estudios Políticos y Constitucionales, pp. 251 y ss.

Cueva Aleu, I., "Crónica de jurisprudencia constitucional en materia de derechos fundamentales sustantivos", en *Actas de las X Jornadas de la Asociación de Letrados del Tribunal Constitucional. La Constitución europea*, Colección Cuadernos y debates por el Tribunal Constitucional y el Centro de Estudios Políticos y Constitucionales, Madrid, 2005, pp. 225 y ss.

Cuijpers, C., "A Private Law Approach to Privacy: Mandatory Law Obliged", en *SCRIPT-ed*, Vol. 4, Issue 4, Sept. 2007, pp. 305-318.

Daleau, J., "Validation de la loi contre le terrorisme et précisions sur le droit d'amendement", en *Dalloz*, 2006, pp. 247 y ss.

Daviter, F., "Policy framing in the European Union", en *Journal of European Public Policy*, 14 (4), 2007, pp. 654–666.

De Goede, M., "Hawala Discourses and the War on Terrorist Finance", en *Environment and Planning D: Society and Space*, 21(5), 2003, pp. 513–32. —"Financial Regulation in the War on Terror", en *After Deregulation: Global Finance in the New Century* (eds. Libby Assassi, Duncan Wigan y Anastasia Nesvetailova), Palgrave, Londres, 2003, pp. 193–206.

De Hert, P., "Balancing security and liberty within the European human rights framework. A critical regarding of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", en *Utrecht Law Review*, Vol. 1, 2005, pp. 68-96.

De Hert, P., Papakonstantinou, V. and Riehle, C., "Data protection in the Third Pillar: cautious pessimism" en *Crime Rights and the EU: The Future of the Police and Judicial Cooperation* (Martin, M., ed.), Justice, London, 2008, pp. 121-181.

De Hert, P., y De Shutter, B., "International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and SWIFT", en *Justice, Liberty and Security: New Challenges for EU External Relations* (eds. Martenczuk, B. y van Thiel, S.), VUB Press, Bruselas, 2008.

De Hert, P., y Gutwirth, S., "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", en *Privacy and the criminal law* (eds. E. Claes, A. Duff y S. Gutwirth), Intersentia, Antwerp/Oxford, 2006. —"Regulating Profiling in a Democratic Constitutional State", en *Profiling the European Citizen* (eds. Hildebrandt, M. y Gutwirth, S.), Dordrecht, Springer, 2008.

De la Quadra-Salcedo y Fernández del Castillo, T., "El derecho europeo de las telecomunicaciones", en *Cuadernos de derecho judicial*, n. 6, 1997, pp. 45-86. — "Telecomunicaciones y Derecho público", en *Derecho de las telecomunicaciones* (coord. por Javier Cremades García), 1997, pp. 131-150.

Dempsey, J., "Civil liberties in a time of crisis", en *Human Rights*, 29 (1), 2002, pp. 8–10.

Den Boer, M., y Monar, J., "11 September and the Challenge of Global Terrorism to the EU as a Security Actor", en *Journal of Common Market Studies*, 40, 2002, pp. 11–28.

Department of Homeland Security – Chief Privacy Officer, *2008 Report to Congress. Data Mining: Technology and Policy*, Washington, Diciembre 2008.

Derrida, J., "Force of Law: The Mystical Foundation of Authority", en *Deconstruction and the Possibility of Justice* (Drucilla Cornell, Michael Rosenfeld y David Gray Carlson, eds.), Routledge, New York, 1992, pp. 3–67.

Dershowitz, A. M., *Preemption: A Knife that Cuts Both Ways*, WW Norton, New York, 2006.

DeSimmone, C., "Pitting Karlsruhe against Luxembourg-German Data Protection and the Contested Implementation of the EU Data Retention Directive", en *German LJ*, 11, 2010, pp. 291 y ss.

Díaz Cappa, J., "Confidencialidad, secreto de las comunicaciones e intimidad en el ámbito de los delitos informáticos", en *Diario La Ley*, n. 7666, 2011.

Dicey, A., Introduction to the Study of the Law of the Constitution, Macmillan, London, 1915.

Diffie, W. y Landau, S., *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, Cambridge, 1998.

Dimitriu, E., "The EU"s Definition of Terrorism", en *German Law Journal*, 5(5), 2004, pp. 435–617.

Doménech Pascual, G., "¿Puede el Estado abatir un avión con inocentes a bordo para prevenir un atentado kamikaze?: comentario a la sentencia del Tribunal Constitucional Federal alemán sobre la Ley de seguridad aérea", en *Revista de Administración Pública*, n. 170, 2006.

Domke, D., Graham, E. S., Coe, K., John, S. L., y Coopman, T., "Going public as political strategy: The Bush administration, an echoing press, and passage of the patriot act", en *Political Communication*, 23 (3), 2006, pp. 291–312.

Donahue, J. D., y Pollack, M. A., "Centralization and its discontents: The rhythms of federalism in the United States and the European Union", en *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union* (K. Nicolaidis, y R. Howse, ed.), Oxford University Press, Oxford, 2001, pp. 73–117.

Doyle, C., *National security letters in foreign intelligence investigations: A glimpse of the legal background and recent amendments*, CRS Report RS22406, 2008.

Drumbl, M. A., "Judging the 11 September terrorist attack", en *Human Rights Quarterly*, n. 2, 2002, pp. 329 y ss.

Dumorttier, J., y Goermans, C., "Data Privacy and Standardization", en *Discussion Paper prepared for the CEN/ISSS Open Seminar on Data Protection*, ICRI, Bruselas, 23/24 de marzo de 2000, disponible en http://www.law.kuleuven.ac.be/icri 135

Dutton, W. H., y Helsper, E., *Oxford Internet Survey 2007 Report: The Internet in Britain*, Oxford Internet Institute, Oxford, 2007.

Dworkin, R., "What the Court Really Said", en *The New York Review of Books*, vol. 51, n. 13 (12 de agosto 2004) —*La democracia posible: principios para un nuevo debate político*, Paidós, Barcelona, 2008.

Dyzenhaus, D., "The Permanence of the Temporary: Can Emergency Power be Normalized?", en *The Security of Freedom. Essays on Canada"s Anti-terrorism Bill* (eds. Daniels, Macklem y Roach), University of Toronto Press, Toronto, 2001, pp. 21 y ss.

Edkins, J. y Pin-Fat, V., "Introduction: Life, Power, Resistance", en *Sovereign Lives: Power in Global Politics* (Jenny Edkins, Véronique Pin-Fat y Michael J. Shapiro, eds.), Routledge, Londres, 2004, pp. 1–21.

Electronic Privacy Information Center (EPIC) and Privacy International. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*. EPIC, Washington, DC, 2004.

Ericson, R. V., *Crime in an Insecure World*, Polity Press, Cambridge, 2007. —y Doyle, A., "Catastrophe Risk, Insurance and Terrorism", en *Economy & Society*, 33(2), pp. 135–73. —Haggerty, K. D., The Policing of Risk", en *Embracing Risk: The Changing Culture of Insurance and Responsibility* (Tom Baker and Jonathan Simon, eds.), University of Chicago Press, Chicago, 2004, pp. 238–272.

Escobar Hernández, C., "La protección internacional de los derechos humanos (I y II)", en *Instituciones de Derecho internacional público* (dir. Díez de Velasco, M.), Tecnos, 12º edición, Madrid, 1999, pp. 535 y ss.

Esquirol Zuloaga, I., "El derecho fundamental al secreto de las comunicaciones: postales y telegráficas. Marco legal del derecho", en *La prueba en el proceso penal* (coord. por Pedro Martín García), 2000, pp. 437-504

Etzioni, A., *How patriotic is the Patriot Act?: freedom versus security in the age of terrorism*, New York, Routledge, 2004.

Ewald, F., "Two Infinities of Risk", en *The Politics of Everyday Fear* (Brian Massumi, ed.), University of Minnesota Press, Minneapolis, 1994, pp. 221–8. —"The Return of Descartes: Malicious Demon: An Outline of a Philosophy of Precaution", en *Embracing Risk: The Changing Culture of Insurance and Responsibility* (ed. Tom Baker y Jonathan Simon), University of Chicago Press, Chicago, 2002, pp. 273–302.

Fabbrini, S., "Transatlantic constitutionalism: Comparing the United States and the European Union", en *European Journal of Political Research*, 43 (4), 2004, pp. 547–569.

Fabiano, L., "Garante dei diritti e giudice dei poteri: il doppio volto della Corte Suprema nelle sentenze "Guantanamo"", en *Diritto Pubblico Comparato ed Europeo*, n.1, 2005, pp. 104 y ss.

Fallon, R. H., "Habeas corpus jurisdiction, substantive rights, and the war on Terror", en *Harvard Law Review*, n. 8, 2007, pp. 2031 y ss.

Fanchiotti, V., "Il dopo 11 setembre e lUSA Patriot Act: lotta al terrorismo e «effetti collaterali»", en *Questione Giustizia*, 2004, pp. 283 y ss.

Farrell, H., "Constructing the international foundations of e-commerce – the EU-US Safe Harbor Arrangement", en *International Organization*, 57 (2), pp. 277–306, 2003.

Featherstone, K., y Radaelli, C. (eds.), *The politics of Europeanization*, Oxford University Press, Oxford, 2004.

Feiler, L, "The legality of the data retention directive in light of the fundamental rights to privacy and data protection", en *European Journal of Law & Technology*, 1, 2010.

Fernández Segado, F., "El Estado de excepción en el Derecho constitucional español", en *Revista de Derecho Privado*, 1977. —"La Ley Orgánica de los Estados de alarma, excepción y sitio", en *Revista de Derecho Político*, n. 11, 1981, pp. 83 y ss. — "Naturaleza y régimen legal de la suspensión general de los derechos fundamentales", en *Revista de Derecho Político*, 18-19, 1983, pp. 31 y ss. — "La suspensión individual del ejercicio de derechos constitucionales", en *Revista de Estudios Políticos*, n. 35, 1983. —*El sistema constitucional español*, Dykinson, 1992. —"Artículo 55. La suspensión de derechos", en *Comentarios a la Constitución española de 1978* (dir. Alzaga Villamil, O.), Cortes Generales-Editoriales de Derecho Reunidas, Madrid, 1996, pp. 597 y ss.

Fernández-Miranda Campoamor, A. y Fernández-Miranda Campoamor, C., *Sistema electoral, partidos políticos y Parlamento*, 1ª ed., Madrid, Colex, 2003.

Fernando Pablo, M. M., *Derecho general de las telecomunicaciones*, Editorial Constitución y Leyes, Colex, 1998.

Ferrajoli, L., "El Derecho penal del enemigo y la disolución del Derecho", en *Jueces para la Democracia*, n. 57, 2006, pp. 3 y ss.

Fitzpatrick, J., "Speaking Law to Power: The War Against Terrorism and Human Rights", en *European Journal of International Law*, 14(2), 2003, pp. 241–264.

Fix-Zamudio, H., "Los estados de excepción y la defensa de la constitución", en *Boletín Mexicano de Derecho Comparado*, n. 111, 2004.

Ford, R., Beware Rise of Big Brother State, Warns Data Watchdog. *The Times*, 16 de agosto de 2004.

Foucault, M., *Society Must Be Defended*, Picador, New York, 2003.

Franciscis, M. E. de., "In margine alle sentenze sul caso dei detenutti di Guantanamo: la ragione di Stato e le garanzie processuali negli USA", en *Rassegna Parlamentare*, n. 2, 2005, pp. 427 y ss.

Franziska, B., "Confusing fundamental rights protection in Europe: Loopholes in Europe"s fundamental rights protection exemplified on European data protection rules", *Law Working Paper Series*, 2009-01, 24 de febrero de 2009, University of Luxembourg. Disponible en http://ssrn.com/abstract=1348472

Frigols i Brines, E., "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", en *La protección jurídica de la intimidad* (coord. por Angeles Jareño Leal; Francisco Javier Boix Reig), 2010, pp. 37-90.

Frowein, J. A., "The Relationship between Human Rights Regimes and Regimes of Belligerent Occupation", en *Israel Year Book on Human Rights*, 28, 1998, pp. 453 y ss.

García Llovet, E., "Derecho sancionador de las telecomunicaciones", en *Telecomunicaciones, infraestructuras y libre competencia* (coord. por Enrique Gómez-Reino y Carnota), 2004, pp. 329-354

García Mexía, P., y Corona Herrero, J. U., "Internet y el derecho de las telecomunicaciones: el régimen jurídico del acceso a la red", en *Principios de derecho de internet* (coord. por Pablo García Mexía), 2005, pp. 132-188.

Garuti, G., "Le intercettazioni preventive nella lotta al terrorismo internazionale", en *Diritto penal e processo*, 2005, pp. 1457 y ss.

Geradin, D., Reysen, M., y Henry, D, "Extraterritoriality, Comity and Cooperation in EC Competition Law", Julio de 2008, SSRN, Paper Series, disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1175003

Gest, J., "House Wants to Inhibit Offshore Internet Gambling", en *Los Angeles Times*, 38, 11 de junio de 2003.

Gimbernat Ordeig, E., "El TC y el principio de proporcionalidad", en *El Mundo, 22 de julio de 1999*.

Gimeno Sendra, V., "Nuevas perspectivas de la legislación procesal penal Antiterrorista", en *Documentación Jurídica*, n. 37-40, 1983, pp. 1243 y ss. —"Repercusiones de la lucha contra el terrorismo en la tutela de los derechos humanos", en *La Ley*, T. 2, 2002. —*Derecho procesal penal*, primera edición, 2004. —"Repercusiones de la lucha norteamericana contra el terrorismo en la tutela de los derechos humanos", en *Derechos, justicia y estado constitucional: un tributo a Miguel C. Miravet*, Tirant lo Blanch, Valencia, 2005.

Giovine, A. di, *La protezione della democrazia tra libertà e sicurezza*, en www.dpce.it., 2005.

Gómez Sánchez, Y., "La sociedad de la información en Europa (I)", en *Libertades informativas* (coord.. Antonio Torres del Moral), 2009, pp. 1215-1250. —"Las organizaciones internacionales y la defensa de los derechos", en *Los derechos en Europa* (coord. por Yolanda Gómez Sánchez), 1997, pp. 105-126. —"Constitucionalismo multinivel y relaciones entre Parlamentos.: Parlamento europeo, Parlamentos nacionales y Parlamentos regionales con competencias legislativas", Centro de Estudios Políticos y Constitucionales, Madrid. —y Rebollo Delgado, L., *Biomedicina y protección de datos*, Dykinson, Madrid, 2008. —*Derechos y libertades*, Sanz y Torres, Madrid, 2003.

Gomez, J., "Dumbing Down Democracy: Trends in Internet Regulation, Surveillance, and Control in Asia", Paper Presented at the Centre for Southeast Asian Studies Seminar Series, Monash Asia Institute, 2004.

Gómez-Ferrer Rincón, R., "Cambios de modelo y derecho. El derecho transitorio en la evolución de la ordenación de las telecomunicaciones", en *Derecho de la regulación económica* (dir. Santiago Muñoz Machado), Vol. 4, 2010, pp. 759-810.

González de la Garza, L. M., "La sociedad de la información en Europa (II)", en *Libertades informativas*, 2009, pp. 1251-1304. —"La sociedad de la información en Europa (III)", en *Libertades informativas*, 2009, pp. 1305-1359.

González Fuster, G., y Paepe, P., "Reflexive Governance ad the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects", en *Security versus Justice?* (eds. Guild, E. y Geyer, F.), Aldershot, Ashgate, 2008.

González González, J., y Sanz Fernández-Vega, B., *Nuevo marco regulatorio europeo en el sector de las telecomunicaciones: una regulación sectorial que introduce conceptos y principios del derecho de la competencia*, Universidad San Pablo-CEU, Madrid, 2002.

González Muñoz, A., y Cortés López, A. M., "Las telecomunicaciones por cable en el Derecho Comparado", en *Telecomunicaciones por cable* (coord. por Enrique Arnaldo Alcubilla, Salvador Montejo Velilla), 2000, pp. 75-110.

González Pascual, M. I., "Cuestiones constitucionales planteadas por la legislación antiterrorista: el ejemplo alemán", en *Revista Vasca de Administración Pública*, n. 77, 2007, pp. 209 y ss. —"Seguridad y libertad en la legislación alemana del tratamiento policial de la información: la posición del Tribunal Constitucional Federal", en *Cuadernos de Derecho público*, n. 33 (enero-abril 2008), pp. 167 y ss.

González Soler, O. E., "Aspectos constitucionales de algunas diligencias sumariales que afectan a los derechos a la intimidad y al secreto de las comunicaciones: entradas domiciliarias. Comunicaciones postales y telefónicas", en *Cuadernos de derecho judicial*, n. 15, 2003, pp. 91-164

Götz, V., "La costituzione dell"emergenza nella Legge Fondamentale tudesca", en *Diritto e societá*, n. 4, 1991, pp. 545 y ss.

Gow, G., "Prepaid Phone Cards: The Anonymity Question", paper presented at Simon Fraser University, 24 de marzo de 2005. Disponible en http://www.sfu.ca/cprost/prepaid/downloads.htm#Mar%2024%202005.

Gragl, P., The Accession of the European Union to the European Convention on Human Rights, Hart Publishing, Londres, 2013.

Graham, S., "Cities and the War on Terror", en *International Journal of Urban and Regional Research*, 30(2), 2006, pp. 255–276.

Grewe, C., "Constitution et secret de la vie privée", en *AIJC XVI*, 2000, pp. 135 y ss.

Grewe, C., y Koering-Joulin, R., "De la légalité de l"infraction terroriste à la proportionnalité des mesures antiterroristes", en *Libertés, justice, tolérance. Mélanges en hommage au Doyen Gérard Cohen-Jonathan*, Vol. II, Bruylant, Bruselas, 2004, pp. 891 y ss.

Grewe, C., y Sommermann, K.-P., "Lutte contre le terrorisme et protection des droits fondamentaux. Allemagne", en *Annuaire International de Justice Constitutionnelle*, XVIII, *Economica-Presses Universitaires D"Aix-Marseille*, 2002, pp. 72 y ss.

Groppi, T., "La garantie des droits et des libertés au niveau fédéral et provincial au Canada", en *The protection of Fundamental Rights in Europe: Lessons from Canada*, Trento, Università degli Studi di Trento, 2004, p. 75 y ss. —"Il Canada dopo l"11 settembe 2001: la ricerca di una "via canadese" per conciliare sigurezza e diritti", en *Quaderni costituzionali*, 2005, pp. 573 y ss.

Gudín Rodríguez-Magariños, F., "El Derecho Penal del enemigo y la Military Commissions Act de 2006: ¿Requiem por las garantías de los presuntos terroristas?", en *Revista de Derecho y Proceso Penal*, n. 17, Thomson-Aranzadi, 2007, pp. 13 y ss.

Guild, E., "The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the 'Terrorist Lists", en *Journal of Common Market Studies*, 46(1), 2008, pp. 173–93.

Gutiérrez Gil, A. J., "La participación por colaboración en el delito de terrorismo", en *La criminalidad organizada. Aspectos sustantivos, procesales y orgánicos*, *Cuadernos de Derecho Judicial II-2001*, Escuela Judicial-Consejo General del Poder Judicial, Madrid, 2001, pp. 13 y ss. —"Crónica de jurisprudencia constitucional en materia de derechos fundamentales sustantivos", en *Estado y religión en la Europa del siglo XXI. Actas de las XIII Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Colección Cuadernos y debates por el Tribunal Constitucional y el Centro de Estudios Políticos y Constitucionales, Madrid, 2008, pp. 245 y ss.

Guttry, A. de (coord.), *Oltre la reazione. Complessitá e limiti nella guerra al terrorismo internazionale dopo l"11 settembre*, ETS, Pisa, 2003.

Haggerty, K. D., y Ericson, R. V. (eds.), *Risk and Morality*, University of Toronto Press, Toronto, 2003.

Halberstam, D., "Comparative federalism and the issue of commandeering", en *The federal vision: Legitimacy and levels of governance in the United States and the European Union* (ed. K. Nicolaidis, y R. Howse), Oxford University Press, Oxford, 2001, pp. 213–251.

Hansell, S., y Lichtblau, E., "US Wants Companies to Keep Web Usage Records", en *New York Times*, online edition, 2 de junio de 2006.

Heisenberg, D., *Negotiating Privacy: The European Union, the United States and the Personal Data Protection*, Lynne Rienner Publishers, 2005, pp. 51-73.

Helleiner, E., "State Power and the Regulation of Illicit Activity in Global Finance", en *The Illicit Global Economy and State Power* (H.R. Friman y P. Andreas, eds.), Rowman and Littlefield, Lanham, 1999, pp. 53–90.

Herman, S., "The USA Patriot Act and the Submajoritarian Fourth Amendment", en *Harvard Civil Liberties Law Review*, 41 (1), 2006, pp. 67–132.

Herrera González, F., "La aplicación de principios de derecho de competencia a la regulación sectorial de telecomunicaciones", en *Información Comercial Española*, ICE: Revista de economía, n. 832, 2006, pp. 45-57

Herrmann, C., "Mush Ado about Pluto? The Unity of the Legal order of the European Union Revisited", en *EU Foreign Relations Law: Constitutional Fundamentals, Essays in European Law* (Cremona, M., y De Witte, ed.), Volume 13, Hart Publishing, Oxford y Portland, 2008, pp.19-51.

Hetcher, S., "The FTC as internet privacy norm entrepreneur", en *Vanderbilt Law Review*, 53 (6), 2000, pp. 2041–2062.

Heymann, P. B., *Protecting liberty in an age of terror*, The MIT Press, Cambridge, 2005.

Hijmans, H., "The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority", en *Common Market Law Review*, Vol. 43, 2006, pp. 1313-1342.

Hildebrandt, M,. y Gutwirth, S. (eds.), *Profiling the European Citizen*, Dordrecht, Springer, 2008.

Hinojosa Segovia, R., "Otras especialidades procesales", en *Derecho procesal penal* (Andrés de la Oliva Santos y otros), séptima edición, Editorial Universitaria Ramón Areces, Madrid, 2004, pp. 801 y ss.

Hix, S., "Elections, parties and institutional design: A comparative perspective on European Union Democracy", en *West European Politics*, 21 (3), 1998, pp. 19–52.

Hol, A. M., y Vervaele, J. (eds.), *Security and civil liberties: the case of terrorism*, Intersentia, Antwerpen, 2005.

Hornung, G., y Schnabel, C., "Data protection in Germany I: The population census decision and the right to informational self-determination", en *Computer Law & Security Review*, 25, n. 1, 2009, pp. 84-88.

Hosein, I., "The Collision of Regulatory Convergence and Divergence: Updating the Policies of Surveillance and Information Technology", en *South African Journal of Information and Communication*, 2(1), 2002, pp. 18–33. —"The Sources of Laws: Policy Dynamics in a Digital and Terrorized World", en *Information Society*, Vol. 20, 2004, p. 187-199.

Hueglin, T., y Fenna, A., *Comparative federalism: A systematic inquiry*, Broadview Press, Toronto, 2006.

Huerta Tocildo, S., "Principio de legalidad y normas sancionadoras", en *Actas de las V Jornadas de la Asociación de Letrados del Tribunal Constitucional. El principio de legalidad*, Colección Cuadernos y Debates, Tribunal Constitucional y Centro de Estudios Políticos y Constitucionales, pp. 11 y ss.

Husabo, E., y Bruce, I., *Fighting Terrorism through Multilevel Criminal Legislation, Security Council Resolution 1371, the EU Framework Decision on Combating Terrorism and their Implementation in Nordic, Ducht and German Criminal Law*, M. Nijhoff Publishers, Leiden, 2009.

Huysmans, J., *The Politics of Insecurity: Fear, Migration and Asylum in the EU*, Routledge, London, 2006.

Jakobs, G., *Sociedad, norma y persona en una teoría de un derecho penal funcional*, Cívitas, Madrid, 1996. —*Derecho penal del enemigo*, Civitas, Madrid, 2003. —*La pena estatal: significado y finalidad*, Civitas, Madrid, 2006.

John, S. L., Domke, D., y Coe, K. M., "Going public, crisis after crisis: The Bush administration and the press from September 11 to Saddam", en *Rhetoric & Public Affairs*, 10 (2), 2007, pp. 195–220.

Johnson, C., *Blowback: The Cost and Consequence of American Empire*, Henry Holt, New York, 2000. —*The Sorrows of Empire: Militarism, Secrecy, and the End of the Republic*, Metropolitan Books, New York, 2003.

Jones, E., "The Politics of Europe 2003", en *Industrial Relations Journal*, 35(6), 2004, pp. 483–499.

Jóri, A., *Data Protection Law – An Introduction*, 2006-2007. Disponible en http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy

Kant, I., *La paz perpetua*, Tecnos, Madrid, 1985.

Kelemen, D., "Regulatory federalism: EU environmental regulation in comparative perspective", en *Journal of Public Policy*, 20 (3), 2002, pp. 133–167.

Kerr, O. S., "Internet surveillance law after the USA Patriot Act: The big brother that isn't", en *Northwestern University Law Review*, 97 (2), 2003, pp. 607–673.

Kincaid, J., "From cooperative to coercive federalism", en *The Annals of the American Academy of Political and Social Science*, 509(1), 1990, pp. 139–152.

Kindt, E., "Biometric Application and the data protection Legislation: The legal review and the Proportionality Test", en *DuD-Datenschuts und Datensicherheit*, 31, 2007.

Köpsell, S., Wendolsky, R., y Federrath, H., "Revocable anonymity", en *Emerging Trends in Information and Communication Security*, Springer Berlin Heidelberg, 2006, pp. 206-220.

Korff, D., "EC Study on the Implementation of Data protection Directive", en *Report on the Findings of the Study*, Julio-septiembre, 2002. Disponible en: http://ssrn.com/abstract=1287667

Kosta, E., Coudert, F., y Dumortier, J., "Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive", en *International Review of Law Computers and Technology*, 21(3), 2007, pp. 347-362.

Koushede, S., "Regulation and Information Technology: A case study of the EU-US negotiations on the Data Protection Directive", en *College of Europe*, Department of Political Administrative Studies, Master Thesis, Academic Year 1999-2000.

Krane, D., "The middle tier in American federalism: State government policy activism during the Bush presidency", en *Publius: The Journal of Federalism*, 37 (3), 2007, pp. 453–477.

Kuner, C, *European Data Protection Law: Corporate Compliance and Regulation*, 2nd ed., Oxford University Press, Oxford, 2007.

Lafuente Balle, J. M., "Los estados de alarma, excepción y sitio", en *RDPUNED*, n. 30, Madrid, 1990, pp. 23 y ss.

Lanchester, F., "Gli Stati Uniti e l"11 settembre", 2001, en: www.associazionedeicostituzio nalisti.it/dibatitti/vicendeinternazionali. — "L"11 settembre: gli USA e i doveri dell"Europa", en *I perscorsi del federalismo* (B. Caravita, coord.), Giuffré, Milano, 2004, pp. 59 y ss.

Langheinrich, M., "Privacy in ubiquitous computing", en *Ubiqutious Computing Fundamentals*, 2009, pp. 96-156.

Lascuraín Sánchez, J. A., "¿Que les corten la cabeza?", en *Claves de Razón práctica*, n. 145, septiembre 2004, pp. 37 y ss.

Lenaerts, K., y Van Nuffel, P., *Constitutional Law of the European Union*, Second ed., Sweet and Maxwell, London, 2005.

Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

Levin, A, y Nicholson, M. J., "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground", 2005.

Lewis, M., *When Worlds collide: Suggested Best practices For Navigating European Data Protection Laws in the U.S. Litigation*, white paper, Communicate, Julio de 2009, disponible en www.morganlewis.com

Linder, S. H., y Peters, G. B., "Instruments of government: Perceptions and contexts", en *Journal of Public Policy*, 9 (1), 1989, pp. 35–58.

Llaneza González, P., *Nuevo marco regulatorio de las telecomunicaciones*, Editorial Bosch, Barcelona, 2002.

Loewenstein, K., "Militant Democracy and Fundamental Rights", en *American Politics Scienst Review*, 1937, pp. 418 y ss.

López Garrido, D., *Terrorismo, política y derecho: la legislación antiterrorista en España, Reino Unido, República Federal de Alemania, Italia y Francia*, Alianza D.L., Madrid, 1987.

López Pina, A., "Internet: un pretexto para discurrir sobre los límites y las potencialidades del derecho", en *Sistema: Revista de ciencias sociales*, n. 231, 2013, pp. 105-122.

Lorenzo, R., "Vigencia del principio de legalidad en el derecho de las telecomunicaciones", en *El derecho público a comienzos del siglo XXI: estudios en*

homenaje al profesor Allan R. Brewer Carías (coord. Alfredo Arismendi A., Jesús Caballero Ortiz), Vol. 2, 2003, pp. 2025-2034.

Lu, S., "Cellco Partnership v. FCC & Vonage Holdings Corp. v. Minnesota Public Utilities Commission: VoIP's shifting legal and political landscape", en *Berkeley Journal of Law and Technology*, 20, 2005, pp. 859 y ss.

Lyon, D., *Surveillance after September 11*, Polity, Londres, 2003.

MacCoun, R. J., y Reuter, O., *Drug War Heresies: Learning from Other Vices, Times and Places*, Cambridge University Press, Cambridge, 2001.

Majone, G., "What Price Safety? The Precautionary Principle and its Policy Implications", en *Journal of Common Market Studies*, 40(1), 2002, pp. 89–109.

Marazzita, G., *L"emergenza costitutionale. Definizioni e modelli*, Giuffré, Milán, 2000.

Marks, G., Hooghe, L., y Blank, K., "European integration from the 1980s: State-centric v. multilevel governance", en *Journal of Common Market Studies,* 34 (3), pp. 343–378. 1996.

Marshall, J., "European Commission Disbands Privacy Group", en *ClickZ*, 17 de febrero de 2009, disponible en http://www.clickz.com/3632816.

Martín Morales, R., *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid, 1995.

Martínez Cuevas, R., "La suspensión de derechos y libertades por terrorismo en el Reino Unido, Italia, Alemania, Francia y España: su incorporación a la legislación ordinaria con carácter permanente", en *Libro homenaje a Luis Portero*, Granada, 2001, pp. 515 y ss.

Martínez Vicente, E. L., y Sánchez Pérez, M. C., "Estudio jurisprudencial del derecho fundamental al secreto de las comunicaciones", en *La Constitución y la práctica del derecho* (coord. por Julián Martínez-Simancas Sánchez, Manuel Aragón Reyes), Vol. 2, 1998, pp. 1015-1026.

Marx, G., "Ironies of Social Control: Authorities as Contributors to Deviance through Escalation, Nonenforcement and Covert Facilitation", en *Social Problems*, 28(3), 1980, pp. 221–44.

Matia Portilla, F. J., y Ripoll Carulla, S., "Crónica de de jurisprudencia constitucional 2004-2005 relacionada con los derechos sustantivos de la Constitución", en *Actas de las XI Jornadas de la Asociación de Letrados del Tribunal Constitucional. El Estado autonómico*, Colección Cuadernos y debates por el Tribunal Constitucional y el Centro de Estudios Políticos y Constitucionales, Madrid, 2006, pp. 223 y ss.

Maxeiner, J. R., "Freedom of Information and the EU Data protection Directive", en *Federal Communications Law Journal*, Vol. 48, No. 1, 1995, disponible en: http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=825054

Mazaud, P., "La lutte contre le terrorisme dans la jurisprudente du Conseil constitutionnel", en www.conseil-constitutionnel.fr, 2006.

McKay, D., *Federalism and European Union: a political economy perspective*, Oxford University Press, Oxford, 1999. —*Designing Europe: Comparative lessons from the federal experience*, Oxford University Press, Oxford, 2001. —"William Riker on federalism: sometimes wrong but more right than anyone else?", en *Regional and Federal Studies*, 14 (2), 2004, pp. 167–186. —"Economic logic or political logic? Economic theory, federal theory, and the EMU", en *Journal of European Public Policy*, 12 (3), 2005, pp. 528–544.

Mendes, E., "Between Crime and War: Terrorism, Democracy and the Constitution", en *National Journal of Constitutional Law*, 2003, pp. 95 y ss.

Mendez, F., "The European Union and cybercrime: insights from comparative federalism", en *Journal of European Public Policy*, 12 (3), 2005, pp. 509–527.

Mendez, M., "Passenger name record agreement", en *European Constitutional Law Review*, 3 (1), 2007, pp. 127–147.

Merino Merchán, J. F., "Derecho de los usuarios en materia de telecomunicaciones", en *Curso de derecho de las telecomunicaciones* (coord. por María Pérez-Ugena Coromina, José Fernando Merino Merchán), 2000, pp. 39-69.

Meron, T., *Human Rights in Internal Strife: Their International Protection*, Cambridge University Press, Cambridge, 1987.

Miraglia, M., "Paura e libertá (Legislazione antiterrorismo e diritti di difesa negli Stati Uniti)", en *Questione Giustizia*, n. 2-3, 2004, pp. 304 y ss.

Mitrou, L., "The impact of communications data retention on fundamental rights and democracy–the case of the EU Data Retention Directive", en *Haggerty, Kevin/Samatas, Minas*, 2010, pp. 127-147.

Mitsilegas, V., *EU Criminal Law*, Hart Publishing, Oxford, 2009.

Monar, J., "Justice and home affairs", en *Journal of Common Market Studies Annual Review*, 39, 2001, pp. 121–137.

Montedoro, G., "Diritto alla sicurezza e sicurezza dei diritti", en *Aspenia*, n. 24, 2004, pp. 57 y ss.

Montero Pascual, J. J., *Derecho de las telecomunicaciones*, Tirant lo Blanch, Valencia, 2007.

Moreillon, L., y Courten, F. de, "La lutte contre le terrorisme et les droits du suspect: le principe de sécurité à l"épreuve des droits fondamentaux", en *Schweizerische Zeitschrift für Strafrecht (ZStrR)*, n. 2, 2003, pp. 117 y ss.

Morley, D., y Robins, K., *Spaces of Identity: Global Media, Electronic Landscapes and Cultural Boundaries*, Routledge, Londres, 1995.

Muñoz Bellvehí, X., Nolla Puertas, J. M., y Herreros Margarit, I., *Manual de derecho de las telecomunicaciones*, Servidoc, Barcelona, 2006.

Murgia, C., "Meno libertá piú sicurezza?", en *Studi per Giovanni Motzo* (VV.AA.), Giuffré, Milano, 2003. pp. 297 y ss.

Navas Castillo, M. A., "El Tribunal Constitucional en la declaración-autorización de los estados de alarma, excepción y sitio", en *Parlamento y Justicia Constitucional* (coord. Pau y Vall), Navarra, 1997. ―"Los estados excepcionales y su posible control, por el Tribunal Constitucional", en *RFDUC*, n. 87, Madrid, 1997.

Naylor, R. T., *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*, Cornell University Press, Ithaca, 2002.

Nelson, L., "Privacy and technology: Reconsidering a crucial public policy debate in the post-September 11 era", en *Public Administration Review*, 64 (3), 2004, pp. 259–269.

Neppi Modona, G., "La giurisprudenza costituzionale italiana in tema di leggi di emergenza contro il terrorismo, la mafia e la criminalità organizzata", en *Democrazia e terrorismo*, Editoriale Scientifica, Nápoles, 2006, pp. 83 y ss.

Nettleton, E. y Watts, M., "The data retention directive", en *Journal of Database Marketing & Customer Strategy Management*, 14, 1, 2006, pp. 74-77.

Newman, A., "Building transnational civil liberties: Transgovernmental entrepreneurs and the European Data Privacy Directive", en *International Organization*, 62 (1), 2008, pp. 103–130.

Nicolaidis, K., y Howse, R. (eds.), *The federal vision: Legitimacy and levels of governance in the United States and the European Union*, Oxford University Press, Oxford, 2003.

Nye, D., *American Technological Sublime*, MIT Press, Cambridge, 1994.

O'Harrow, R., *No Place to Hide*. Free Press, New York, 2005.

O'Malley, P., *Risk, Uncertainty and Govern*ment, The GlassHouse Press, New York, 2004.

Obinger, H., Leibfried, S., y Castles, F. G., "Bypasses to a social Europe? Lessons from federal experience", en *Journal of European Public Policy*, 12 (3), 2005, pp. 545–571.

Olarieta Alberdi, J. M., "Ley antiterrorista, Audiencia Nacional y derecho de defensa", en *RFDUC*, n. 74 (1988-1989), pp. 477 y ss.

Ortega Díaz-Ambrona, J. A., "Ironías constitucionales", en *ABC, 28 de julio de 1999*.

Paye, J. C., "Lutte antiterroriste: la fin de l'état de droit", en *Revue Trimestrielle des Droits de l''Homme*, n. 57, 2004, pp. 61 y ss.

Pednekar-Magal, V. y Shields, P., "The State and Telecom Surveillance Policy: The Example of the Clipper Chip Initiative", en *Communication, Law & Policy*, 2003, 8(4), pp. 429–64.

Peers, S., *EU justice and home affairs law*, Oxford University Press, segunda ed., Oxford, 2006.

Peissl, W., "Surveillance and Security: A Dodgy Relationship", en *Journal of Contingencies and Crisis Management*, 11(1), 2003, pp. 19–24.

Pellizonne, I., "Le misure anti-terrorismo internacionales e la "normalizzazione dell"emergenza"", en *Giurisprudenza Costituzionale*, LI, marzo-abril de 2006, fasc. 2, pp. 1765 y ss.

Peris, J. M., y Cuesta Pastor, P. J., "Comentario a la Sentencia del Tribunal Constitucional 136/1999, de 20 de julio (proporcionalidad de los sacrificios en la aplicación de las penas)", en *La Ley*, n. 4970, 14 de enero de 2000, pp. 1 y ss.

Peters, G. B., y Nispen, F. K. M. van, *Public policy instruments: evaluating the tools of public administration*, Edward Elgar Publishers, Northampton, 1998.

Petrillo, P., "Forma di governo e legislazione antiterrorismo in Canada. Spunti di riflessione comparata sul ruolo dei Parlamenti al tempo dell´emergenza permanente", *Democrazia e Terrorismo* (ed. Groppi, T.), Editoriale Scientifica, Nápoles, 2006, pp. 381 y ss.

Pettiti, L.-E., Decaux, E., y Imbert, P.-H., *La CEDH, commentaire article par article*, 2ª edición, París, 1999.

Phillips, D., "Texas 9-1-1: Emergency Telecommunications and the Genesis of Surveillance Infrastructure", en *Telecommunications Policy*, 29(11), 2005, pp. 843–56.

Pictet, J., *Desarrollo y Principios del Derecho internacional humanitario*, Instituto Henry Dunant, Ginebra, 1986.

Portilla Contreras, G., "El Derecho penal y procesal-penal del 'enemigo'. Las viejas y nuevas políticas de seguridad frente a los peligros internos-externos", en *Libro homenaje a Bacigalupo* (López Barja de Quiroga, Jacobo y Zugaldía Espinar, José Miguel, coord.), Marcial Pons, Madrid, 2004, pp. 693 y ss.

Posner, E., y Vermeule, A., *Terror in the Balance: Security, Liberty and the Courts*, Oxford University Press, Oxford, 2007.

Prieto Sanchís, L., *Justicia constitucional y derechos fundamentales*, Trotta, Madrid, 2003.

Princen, S., "Trading up in the transatlantic relationship", en *Journal of Public Policy*, 24 (1), 2004, pp. 127–144.

Pulido Quecedo, M., "Los límites de la justicia (Reflexión sobre la STC 136/1999, de 20 de julio)", en *Repertorio Aranzadi del Tribunal Constitucional*, n. 12, septiembre 1999, pp. 9 y ss.

Quintero Olivares, G., "Colaboración con banda armada", en *La Vanguardia*, 23 de julio de 1999.

Radaelli, C., "Whither Europeanization? Concept stretching and substantive change", en *European Integration Online Papers*, 4 (8), 2000, pp. 1–31.

Rasmussen, M. V., "It Sounds Like a Riddle: Security Studies, the War on Terror and Risk", en *Millennium*, 33(2), 2004, pp. 381–95.

Rebollo Delgado, L., "Origen y fundamento de la protección de datos: datos especialmente protegidos, Título II. Principios de la Protección de Datos. artículo 7", en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (dir. Antonio Troncoso Reigada), 2010, pp. 578-597. —"El derecho a la intimidad", en *Libertades informativas* (dir. Antonio Torres del Moral), 2009, pp. 241-294. —"El secreto de las comunicaciones problemas actuales", en *Revista de derecho político*, n. 48-49, 2000, pp. 351-382. —"Veinticinco años de relación entre la informática y los derechos al honor y a la intimidad personal y familiar", en *Revista de derecho político*, n. 58-59, 2003-2004, pp. 215-240. —*Vida privada y protección de datos en la Unión Europea*, Dykinson, Madrid, 2008. —"Balance constitucional: artículo 18.4 CE", en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n. 6, 2003.

Rees, W. H., "Inside out: the external face of EU internal security policy", en *Journal of European Integration*, 30 (1), 2008, pp. 97–111.

Rees, W., *Transatlantic Counter Terrorism Cooperation: The New Imperative*, Routledge, Londres, 2006.

Rees, W., y Aldrich, R. J., "Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence?", en *International Affairs*, 81(5), 2005, pp. 905–23.

Rehnquist, W. H., *All the Laws but One: Civil Liberties in Wartime*, Knopf, New York, 1998.

Reid, P., "Regulating online data privacy", en *SCRIPT-ed*, Vol. 1, Issue 3, Sept. 2004.

Remotti Carbonell, J. C., *Constitución y medidas contra el terrorismo. La suspensión individual de derechos y garantías*, Colex, Madrid, 1999.

Renoux, T., "Juger le terrorisme?", en *Cahiers du Conseil constitutionnel*, n. 14, 2003, pp. 102 y ss.

Revenga Sánchez, M., *El imperio de la política. Seguridad nacional y secreto de Estado en el sistema constitucional norteamericano*, Ariel, Barcelona, 1995. —"Razonamiento judicial, seguridad nacional y secreto de Estado", en *REDC*, n. 53, 1998, pp. 66 y ss. —"Garantizando la libertad y la seguridad de los ciudadanos en Europa: nobles sueños y pesadillas en la lucha contra el terrorismo", en *Parlamento y Constitución*, Cortes de Castilla la Mancha y Universidad de Castilla la Mancha, n. 10, 2006-2007, pp. 3 y ss.

Riker, W. H., *Federalism: Origins, operation, significance*, Brown, Boston, 1964. — *The art of political manipulation*, Yale University Press, New Haven, 1986.

Ripoll Servent, A., "Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to co-decision", en *Journal of European Public Policy* 20, no. 7, 2013, pp. 972-987.

Roach, K., "The post 9/11 Migration of Britain"s Terrorism Act, 2000", en *The Migration of Constitutional Ideas* (ed. Choudhry, S.), Cambridge University Press, Cambridge, 2006, pp. 374 y ss. —"Sources and Trends in Post 9/11 Anti-Terrorism Laws", en *Human Rights and Security* (Lazurus y Goold, eds.), Hart Publishing, Oxford, 2007, p. 227 y ss.

Roberts, H., y Palfrey, J,. "The EU Data Retention Directive in an Era of Internet Surveillance", en *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*, 2010, pp. 36-54.

Rodríguez Montañés, T., "Terrorismo, enemigos y tortura", en *Teoría & Derecho*, n. 3, 2008, pp. 98 y ss.

Rosenfeld, M., "¿Es apropiada la ponderación judicial en la lucha contra el terrorismo? Contrastando tiempos normales, emergencias y tiempos de tensión", en *Real Instituto Elcano de Estudios Internacionales y Estratégicos*, ARI n. 109/2005, disponible en www.realinstitutoelcano.org.

Runciman, D., "The Precautionary Principle", en *London Review of Books*, 26(7), 2004. Disponible en http://www.lrb.co.uk/v26/n07/runc01_.html.

Ryan, J., *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web*, Institute of European Affairs, Dublín, 2007.

Salas Calero, L., "La Ley patriótica de USA", en *Terrorismo y proceso penal acusatorio*, Tirant lo Blanch, Valencia, 2006, pp. 255 y ss.

Salbu, S. R., "The European Union Data Privacy Directive and International Relations", en *Vand. J. Transnat"l L.,* 35, 2002, pp. 655.

Sánchez Agesta, L., *El sistema político de la Constitución española de 1978*, Editora Nacional, Madrid, 1980.

Sánchez Rodríguez, A. J., *Derecho de las telecomunicaciones, nuevo derecho y nuevo mercado*, Dykinson, Madrid, 2002.

Sandoz, Y., "Lutte contre le terrorisme et droit international, risques et opportunités", en *RSDIE*, 2002, pp. 253 y ss.

Santolaya Machetti, P., "El control de los secretos de Estado: la experiencia en Derecho comparado", en *Poder Judicial*, n. 40, 1997, p. 69 y ss.

Sartor, G., Privacy, Reputation and Trust: Some Implications for Data Protection, European University Institute (EUI), Department of Law, EUI Working Paper LAW, No. 2006/4, 2004.

Schepp, D., Money laundering in cyberspace, 2001, *BBC News*. Disponible en http://news.bbc.co.uk/1/hi/business/1149984.stm.

Schoetti, J. E., "La législation anti-terroriste à l"épreuve du contrôle de constitutionnalité", en *Gazette du Palais*, 5/7 de febrero de 2006, n. 36-38, pp. 20 y ss.

Schulhofer, S. J. *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11*, Century Foundation Press, New York, 2002.

Schutter, O. de, "La Convention européenne des droits de l"homme à l"épreuve de la lutte contre le terrorisme", en *Revue Universelle des Droits de l"Homme (RUDH)*, vol. 13, n. 5-8, 2001, pp. 185 y ss.

Schwartz, P., "*Preemption and privacy"*, en Yale Law Journal, 118, 2009, pp. 902–947.

Scirocco, A., "The Lisbon Treaty and the Protection of Personal Data in the European Union", en *Dataprotectionreview.eu*, 5, 2008.

Sciso, E., "La condizione dei detenuti di Guantamano fra diritto humanitario e garanzie dei diritti umani fondamentali", en *Rivista di Diritto Internazionale*, n. 1, 2003, pp. 111 y ss.

Scobbie, I., "The Last Refuge of Tyrant?" Judicial deference to Executive Actions in Time of "Terror"", en *Counterterrorism: Democracy"s Challenge* (Bianchi y Keller, eds.), Hart Publishing, Oxford, 2008, pp. 277 y ss.

Serrano Butragueño, I., "Proporcionalidad de las penas y legalidad penal", en *Otrosí. Publicación informativa del Colegio de Abogados de Madrid*, n. 8, octubre 1999, pp. 16-18.

Serrano-Piedecasas Fernández, J. R., y Demetrio Crespo, E., "Del Estado de derecho al Estado preventivo", en *El cronista del Estado social y democrático de derecho*, Iustel, n. 8, noviembre 2009, pp. 24 y ss.

Shaffer, G., "The power of EU collective action: The impact of EU Data privacy regulation on US business practice", en *European Law Journal*, 5(4), 1999, pp. 419–437.

Shahar, Y., *The Internet as a Tool for Counter-terrorism: Patrolling and Controlling Cyberspace*, en *NATO: Advanced Research Workshop*, Garmisch-Partenkirchen, Abril, 2007.

Shields, P., "Beyond "Loss-of-Control": Telecommunications, Surveillance, Drugs and Terrorism", en *The Journal of Policy, Regulation and Strategy for Telecommunications and Media*, 4(2), 2002, pp. 9–15. —"The "Information Revolution", Financial Globalization, State Power and Money Laundering", en *Journal of International Communication*, 11(1), 2005, pp. 15–39. —"When the 'Information Revolution' and US Security State Collide: Money Laundering and the Proliferation of Surveillance", en *New Media & Society*, 7(4), 2005, pp. 483–512.

Sitaropoulos, N., "The Role and Limits of the European Court of Human Rights in supervising State Security and anti-terrorism measures affecting alliens' rights", en *Terrorism and the Foreigner* (Elspeth Guild y Anneliesee Baldaccini, eds.), Amsterdam, 2007.

Snow, J., "Financial Intelligence", en *Washington Post*, online edition, 14 de abril de 2006.

Sofaer, A. D., "On the Necessity of Pre-emption", en *European Journal of International Law* 14(2), 2003, pp. 209–26.

Solove, D., Rotenberg, M., y Schwartz, P. M., *Information privacy law*, Aspen Publishers, Nueva York, 2006. —*Understanding Privacy*, Harvard University Press, Cambridge, 2008.

Sorel, J.-M., "Some Questions about the Definition of Terrorism and the Fight Against its Financing", en *European Journal of International Law* 14(2), 2003, pp. 365–378.

Sorkin, D., "Spam legislation in the United States", en *John Marshall Journal of Computer and Information Law*, 22 (1), 2003, pp. 3–12.

Sottiaux, S., *Terrorism and the limitations of rights: the ECHR and the US Constitution*, Hart Publishing, Oxford, 2008.

Sparke, M. B., "A Neoliberal Nexus: Economy, Security and the Biopolitics of Citizenship on the Border", en *Political Geography*, 25(2), 2006, pp. 151–180.

Spitz, P.-E., "À propos de la décision du Conseil constitutionnel n. 96-377 DC du 16 juillet 1996 sur la loi tendant à renfoncer la répression du terrorisme", en *Revue Française de Droit Administratif*, n. 3, 1997, pp. 538 y ss.

Stalder, F., "Opinion: Privacy is Not the Antidote to Surveillance", en *Surveillance & Society*, 1(1), 2002, pp. 120–124.

Standing, A., "The Concept of Organized Crime Reconsidered", Institute for Strategic Studies Monograph, 77, 2003, pp. 49–64. Disponible en http://www.iss.co.za/Pubs/Monographs/No77/Chap4.html.

Stenersen, A., "Chem-bio Cyber-class:Assessing Jihadist Chemical and Biological Weapons", en *Jane"s Intelligence Review*, 1 de septiembre de 2007, pp. 8–13.

Stevenson, B. A., "The politics of fear and death: successive problems in capital federal Habeas corpus cases", en *New York University Law Review*, n. 3, 2002, pp. 698 y ss.

Sunstein, C. R., "Beyond the Precautionary Principle", en *University of Pennsylvania Law Review*, 151(3), 2003, pp. 1003–1058.

Suskind, R., *The Price of Loyalty*, Simon & Schuster, New York, 2006. —*The One Percent Doctrine: Deep Inside America"s Pursuit of its Enemies Since 9/11*, Simon & Schuster, Nueva York, 2004.

Tappeiner, I., "The Fight Against Terrorism: The Lists and the Gaps", en *Utrecht Law Review* 1(1), 2005, pp. 97–125.

Tatelman, T. B., "The Real Id Act of 2005: Legal, regulatory, and implementation issues", en *CRS Report RL34430*, 2008.

Taylor, M., "The EU data retention directive", en *Computer Law & Security Review*, 22, n. 4, 2006, pp. 309-312. —"Data Protection: Too Personal to protect? ", en *Script-ed*, Vol. 3, Issue I, marzo de 2006.

Tena Piazuelo, V. M., y Gimeno Feliú, J. M., "El derecho comunitario de las telecomunicaciones", en *Informática y derecho: Revista iberoamericana de derecho informático*, n. 4, 1994, pp. 549-554.

Tenorio Sánchez, P. J., "Constitución y legislación antiterrorista", en *Revista d Derecho Político*, n. 71-72, Madrid, 2008, pp. 501 y ss.

Thachuk, K. L., "The Sinister Underbelly: Organized Crime and Terrorism", en *The Global Century: Globalization and National Security* (R.L. Kluger y E.L. Frost, eds.), National Defense University Press, Washington DC, 2001, pp. 743–759.

The White House, *A Framework for Global Electronic Commerce*, Office of the Press Secretary of the White House, Washington, D.C, 1997.

Tintó Gimbernat, M., "El secreto de las comunicaciones electrónicasen los ordenamientos jurídicos español y norteamericano", en *JIS-2000: III Jornadas sobre informática y sociedad* (coord. por Miguel Angel Davara Rodríguez), 2001, pp. 251-258.

Tomkins, A., "Readings of A. V. Secretary of State for the Home Departament", en *Public Law*, 2005, pp. 259 y ss.

Toniatti, R., "L'ordinamento costituzionale della difusa e degli stati di crisi in Gran Bretaña", en *Costituzione della difusa e stati di crisi* (coord.., G. de Vergottini), CeMISS, Roma, 1991, pp. 201 y ss.

Torralba Mendiola, E., y Roca Junyent, M., "Derecho a la intimidad: el secreto de las comunicaciones e Internet", en *Régimen jurídico de internet* (coord. por Miguel Angel Fernández Ordóñez, Javier Cremades García, Rafael Illescas Ortiz), 2001, pp. 181-200

Torre de Silva, J., *La doctrina del Consejo de Estado en materia de telecomunicaciones y de servicios de la sociedad de información: un estudio de derecho administrativo económico*, Boletín Oficial del Estado, Madrid, 2005.

Torres del Moral, A., "La libertad de comunicación pública", en *Derecho de las telecomunicaciones* (coord. por Javier Cremades García), 1997, pp. 989-1010. —"Ampliaciones y minoraciones de la libertad de comunicación pública", en *La democracia constitucional: estudios en homenaje al profesor Francisco Rubio Llorente*, Vol. 1, 2002, pp. 539-572. —"Naturaleza jurídica de los derechos constitucionales", en *Derecho constitucional y cultura: estudios en homenaje a Peter Häberle* (coord. por Francisco Balaguer Callejón), 2004, pp. 497-516. —"Valores y principios constitucionales: preámbulo, preceptos del Título Preliminar y artículo 10.1", en *Congreso 'La Reforma de la Constitución'*, La Rioja, 27-30 de abril de 1992, Vol. 2, 1992. —"Encuadramiento terminológico y evolución histórica de las libertades informativas", en *Libertades informativas*, 2009, pp. 15-70. —"Variaciones de la libertad de comunicación pública por razones laborales, profesionales, funcionariales y políticas", en *Libertades informativas*, 2009, pp. 485-510. —"Relaciones entre la Unión Europea y los Estados miembros según el Tratado Constitucional Europeo: principios que las rigen", en *Revista de derecho político*, n. 65, 2006, pp. 91-114. — *Principios de Derecho Constitucional español. Tomo I. Sistema de fuentes. Sistema de los derechos*, 5ª edición, Servicio de Publicaciones de la Facultad de Derecho-Universidad Complutense de Madrid, Madrid, 2004. ―*Estado de Derecho y democracia de partidos*, 2ª edición, Servicio de Publicaciones de la Facultad de Derecho-Universidad Complutense de Madrid, Madrid, 2004. —"La inconstitucionalidad de los partidos políticos. A propósito de la Ley 6/2002 de Partidos políticos", en *Revista de Derecho político, UNED*, n. 60, Madrid, 2004, pp. 39 y ss. — "Libertades públicas y fuerzas de seguridad", en *Constitución y seguridad pública: una reflexión a los veinticinco años*, Ministerio del Interior, Madrid, 2005, pp. 25 y ss.

Torreta, P., "Diritto alla sicurezza e (altri) diritti e libertà della persona: un complesso bilanciamento costituzionale", en *Diritti e Costituzione. Profili evolutivi e dimensione inedite* (dir. D'Aloia, A.), Giuffrè, Milán, 2003, p. 451 y ss.

Treacy, B., "Privacy and Security Law: Report: Report", en *Bureau and National Affairs* (BNA, INC), Vol. 7, n.12, 24 de diciembre de 2007, pp. 439-442, disponible en http://www.bna.com

Troncoso Reigada, A., "El principio de calidad de los datos: Título II. Principios de la protección de datos. artículo 4", en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (dir. Antonio Troncoso Reigada), 2010, pp. 340-394. —"La comunicación de datos personales: Título II. Principios de la Protección de los Datos. artículo 11", en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (Antonio Troncoso Reigada, dir.), 2010, pp. 950-1006. —"La Administración electrónica y la protección de datos personales", en *Revista jurídica de Castilla y León*, n. 16, 2008, pp. 31-112. —"El derecho al olvido en Internet a la luz de la propuesta de Reglamento General de Protección de Datos Personales", en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n. 59, 2012. — "Hacia un nuevo marco jurídico europeo de la protección de datos personales", en *Revista española de derecho europeo*, n. 43, Civitas, 2012, pp. 25-184. —Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas, Madrid, 2010.

Uría Meruendano, R., "El derecho y las telecomunicaciones", en *Derecho de las telecomunicaciones* (coord. por Javier Cremades García), 1997, pp. 95-110

US National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, National Academies Press, Washington, DC, 2008.

Van Buuren, J., *EU Wants Identification System for Users of Prepaid Telephone Cards*, disponible en http://www.heise.de/tp/r4/artikel/12/12574/1.html.

Van Munster, R., "The War on Terrorism: When the Exception Becomes the Rule", en *International Journal for the Semiotics of Law*, 17, 2004, pp. 141–53.

Vega Clemente, V., "La protección de datos en la sociedad de servicios de la información", en *Revista de estudios económicos y empresariales*, n. 22, 2010, pp. 205-244.

Vergottini, G. de, (coord.), *Costituzione della difesa e stati di crisi*, CeMISS, Roma, 1991. —"Necesitá, costituzione materiale e disciplina dell´emergenza", en *Diritto e societá*, 1994, pp. 245 y ss. —*Le transizioni costituzionali*, Il Mulino, Bolonia, 1998. —"Guerra e Costituzione", en *Quaderni costituzionali*, 2002, pp. 26 y ss. —"La difficile convivenza fra libertá e sicurezza. La riposta delle democrazie el terrorismo", en *Rassegna Parlamentare*, n. 2, 2004, pp. 427 y ss. —*Guerra e Costituzione. Nuovi conflitti e sfide alla democracia*, Il Mulino, Bologna, 2004. —"Il bilanciamento fra sicurezza e libertà civili nella stagione del terrorismo", en *CSGE, Sicurezza: nuove frontiere*, Franco Angeli, Milán, 2005, pp. 118 y ss.

Vervaele, J., "Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?", en *Utrecht Law Review*, 1(1), 2005, pp. 1–27.

Vidal Prado, C., "Nuevos (y viejos) recelos del Tribunal Constitucional Federal Alemán frente a la eficacia del Derecho comunitario", en *REDC*, n. 77, mayo-agosto 2006, pp. 273 y ss.

Vierucci, L., "Il caso Abbasi: la detencione arbitraira a Guantánamo davanti al giudice inglese", en *Rivista di diritto internazionale privato processuale*, 2003, pp. 911 y ss.

Villaverde Menéndez, I., *Estado democrático e información: el derecho a ser informado*, Junta General del Principado de Asturias, Oviedo, 1994.

Vírgala Foruria, E., "La suspensión de derechos por terrorismo en el ordenamiento español", en *REDC*, n. 40, 1994, pp. 64 y ss. —"La STS del 27 de marzo de marzo de 2003 de ilegalización de Batasuna: el Estado de derecho penetra en Euskadi", en *Teoría y Realidad Constitucional*, n. 12-13, 2003-2004, pp. 618 y ss.

Vité, S., *Les procédures internationales d"établissement des faits dans la mise en œuvre du droit international humanitaire*, Bruylant, Bruselas, 1999.

Vogel, D., *Trading up*, Harvard University Press, Cambridge, 1995

Von Beyme, K., "Asymmetric federalism between globalization and regionalization", en *Journal of European Public Policy*, 12 (3), 2005, pp. 432–447. —"La difesa dell"ordinamento costituzionale", en *Quaderni costituzionali*, 1984, pp. 387 y ss.

Vroom, C., "Lutte contre le terrorisme et protection des droits fondamentaux", en *Annuaire international de justice constitutionnelle*, XVIII, 2002, pp. 162 y ss.

Walker, C., y Akdeniz, Y., "Anti-terrorism Laws and Data Retention: War Is Over?", en *Northern Ireland Legal Quarterly*, 54(2), 2003, pp. 159–182.

Walker, N., "The pattern of transnational policing", en *A handbook of policing* (ed. Tim Newburn), Willan Publishing, Londres, 2003, pp. 11–35.

Walker, W. C., "Keeping Control of Terrorists Without Loosing Control of Constitutionalism", en *Stanford Law Review*, 2007, p. 1395 y ss.

Wallace, H., "An institutional anatomy and five policy modes", en *Policy-Making in the European Union* (ed. H. Wallace, W. Wallace, y M. Pollack), Oxford University Press, 5 ed., Oxford, 2005, pp. 49–90.

Walters, W., "The Political Rationality of European Integration", en *Global Governmentality: Governing International Spaces* (Wendy Larner y William Walters, eds.), Routledge, London, 2004, pp. 155–173.

Walters, W., y Haahr, J. H., *Governing Europe: Discourse, Governmentality and European Integration*, Routledge, Londres, 2005.

Warbrick, C., "The principles of the European Convention on Human Rights (ECHR) and the response of states to terrorism", en *European Human Rights Law Review*, n. 3, 2002. —"The European response to terrorism in an age of human rights", en *European Journal of International Law*, 15, 2004, pp. 989 y ss.

Warner, J., "The right to oblivion: data retention from Canada to Europe in three backward steps", en *University of Ottawa Law & Technology Journal*, 2, n. 1, 2005, pp. 75-104.

Warren, P., "The end of privacy?", en The Guardian, Thursday, 2 de abril de 2009.

Weckel, P., "Le statut incertain des detenus sur la base américaine de Guantanamo", en *Revue général de droit international publique*, 2002, pp. 357 y ss.

Welch, M., "Trampling Human Rights in the War on Terror: Implications to the Sociology of Denial", en *Critical Criminology*, 12, 2003, pp. 1–20.

White House, *The National Security Strategy of the United States of America*. Washington, Septiembre, 2002.

Whitley, E. A. y Hosein, I., "Policy Discourse and Data Retention: The Technology Politics of Surveillance in the United Kingdom", en *Telecommunications Policy*, 29, n. 11, 2005, pp. 857-874.

Winner, L., "Technology Today: Utopia or Dystopia?", en *Social Research*, 64(3), 1997, pp. 989–1018.

Wong, R., "The Shape of Things to Come: Swedish Developments on the Protection of Privacy", en *Script-Ed*, Vol. 2, No. 2, 2005, pp. 107-124.

Youngs, R., "Germany: shooting down aircraft and analyzing computer data", en *International Journal of Constitutional Law*, n. 2, 2008, pp. 331 y ss.

Zaffaroni, E. R., "¿Es posible un Derecho penal del enemigo no autoritario?", en *Homenaje al profesor Gonzalo Rodríguez Mourullo*, 1ª ed., Thomson-Aranzadi, Cizur Menor (Navarra), 2005.

Zarate, J. C., "Bankrupting Terrorists", en *E-Journal USA The Global War on Terrorist Finance*, Septiembre, 2004.

Ziller, J., *Les Nouveaux Traitées Européens: Lisbonne et Apres*, Clef Politiques, Montchrestien, Lextenso éditions, Paris, 2008.

Zimmerman, J., *Congressional preemption: Regulatory federalism*, State University of New York Press, Albany, 2005.

Zureik, E. y Salter, M. B. (eds.), *Global Surveillance and Policing: Borders, Security, Identity*, Willan Publishing, Devon, 2005.

ANEXO. Definiciones de términos de la normativa europea sobre privacidad y redes electrónicas

− «abonado»: cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público para la prestación de dichos servicios[1206];

− «autoridad nacional de reglamentación»: el organismo u organismos a los cuales ha encomendado un Estado miembro cualquiera de las misiones reguladoras asignadas en la presente Directiva y en las directivas específicas[1207];

− «comunicación»: cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información[1208];

− «consentimiento de un usuario o abonado»: el consentimiento del interesado, con arreglo a la definición de la Directiva 95/46/CE[1209];

− «consentimiento del interesado»: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan[1210];

− «consumidor»: cualquier persona física que utilice o solicite un servicio de comunicaciones electrónicas disponible para el público para fines no profesionales[1211];

[1206] Definición extraída del art. 2.k) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1207] Definición extraída del art. 2.g) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1208] Definición extraída del art. 2.d) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

[1209] Definición extraída del art. 2.f) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

[1210] Definición extraída del art. 2.h) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

− «correo electrónico»: todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo[1212];

− «datos de localización»: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público[1213];

− «datos de tráfico»: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma[1214];

− «datos personales»: toda información sobre una persona física idientificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social[1215];

− «datos»: los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario[1216];

− «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios[1217];

[1211] Definición extraída del art. 2.i) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1212] Definición extraída del art. 2.h) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

[1213] Definición extraída del art. 2.c) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

[1214] Definición extraída del art. 2.b) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

[1215] Definición extraída del art. 2.a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

[1216] Definición extraída del art. 2.a) de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

[1217] Definición extraída del art. 2.g) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

− «directivas específicas»: las siguientes Directivas: Directiva 2002/20/CE (Directiva autorización), Directiva 2002/19/CE (Directiva acceso), Directiva 2002/22/CE (Directiva servicio universal) y Directiva 97/66/CE[1218];

− «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento[1219];

− «equipo avanzado de televisión digital»: decodificadores para la conexión a televisores o televisores digitales integrados capaces de recibir servicios de televisión digital interactiva[1220];

− «fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica[1221];

− «identificador de celda»: la identidad de la celda desde la que se origina o termina una llamada de teléfono móvil[1222];

− «identificador de usuario»: un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a internet o a un servicio de comunicaciones por internet, o de su registro en uno de dichos servicios[1223];

− «interfaz de programa de aplicación (API)»: la interfaz de software entre las aplicaciones externas, puesta a disposición por los organismos de radiodifusión o

---

[1218] Definición extraída del art. 2.l) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1219] Definición extraída del art. 2.e) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

[1220] Definición extraída del art. 2.o) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1221] Definición extraída del art. 2.c) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

[1222] Definición extraída del art. 2.e) de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

[1223] Definición extraída del art. 2.d) de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

prestadores de servicios, y los recursos del equipo avanzado de televisión digital para los servicios de radio y televisión digital[1224];

− «llamada telefónica infructuosa»: una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación o en la que ha habido una intervención por parte del gestor de la red[1225];

− «llamada»: una conexión establecida por medio de un servicio telefónico disponible para el público que permita la comunicación bidireccional en tiempo real[1226];

− «mercados transnacionales»: los mercados definidos con arreglo al apartado 4 del artículo 15 que abarcan toda la Comunidad o una parte importante de la misma[1227];

− «recursos asociados»: aquellos recursos asociados con una red de comunicaciones electrónicas y/o con un servicio de comunicaciones electrónicas que permitan y/o apoyen el suministro de servicios a través de dicha red o servicio; incluyen los sistemas de acceso condicional y las guías electrónicas de programas[1228];

− «red de comunicaciones electrónicas»: los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluido internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada[1229];

[1224] Definición extraída del art. 2.p) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1225] Definición extraída del art. 2.f) de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

[1226] Definición extraída del art. 2.e) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

[1227] Definición extraída del art. 2.b) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1228] Definición extraída del art. 2.e) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1229] Definición extraída del art. 2.a) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

− «red pública de comunicaciones»: una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público[1230];

− «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario[1231];

− «servicio con valor añadido»: todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación[1232];

− «servicio de comunicaciones electrónicas»: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos asimismo los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas[1233];

− «servicio telefónico»: las llamadas (incluida la transmisión de voz, buzones vocales, conferencias y datos), los servicios suplementarios (incluido el reenvío o transferencia

---

[1230] Definición extraída del art. 2.d) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1231] Definición extraída del art. 2.d) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

[1232] Definición extraída del art. 2.g) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

[1233] Definición extraída del art. 2.c) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

de llamadas) y los servicios de mensajería y servicios multimedia (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia)[1234];

− «servicio universal»: un conjunto mínimo de servicios, definido en la Directiva 2002/22/CE (Directiva servicio universal), de una calidad determinada y que esté disponible para todo usuario con independencia de su localización geográfica y, a la vista de las condiciones nacionales específicas, a un precio asequible[1235];

− «sistema de acceso condicional»: toda medida técnica o mecanismo técnico que condicione el acceso en forma inteligible a un servicio protegido de radiodifusión sonora o televisiva al pago de una cuota u otra forma de autorización individual previa[1236];

− «suministro de una red de comunicación electrónica»: la creación, la explotación, el control o la puesta a disposición de dicha red[1237];

− «tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento[1238];

− «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión

---

[1234] Definición extraída del art. 2.c) de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

[1235] Definición extraída del art. 2.j) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1236] Definición extraída del art. 2.f) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1237] Definición extraída del art. 2.m) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1238] Definición extraída del art. 2.f) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción[1239];

− «usuario final»: el usuario que no suministra redes públicas de comunicaciones o servicios de comunicaciones electrónicas disponibles para el público[1240];

− «usuario»: toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público, con fines privados o comerciales, sin haberse necesariamente abonado a dicho servicio[1241];

− «usuario»: una persona física o jurídica que utiliza o solicita un servicio de comunicaciones electrónicas disponible para el público[1242];

− «usuario»: una persona física que utiliza con fines privados o comerciales un servicio de comunicaciones electrónicas disponible para el público, sin que necesariamente se haya abonado a dicho servicio[1243].

[1239] Definición extraída del art. 2.b) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

[1240] Definición extraída del art. 2.n) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1241] Definición extraída del art. 2.b) de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

[1242] Definición extraída del art. 2.h) de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002.

[1243] Definición extraída del art. 2.a) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

ANEXO. Declaraciones de los Estados miembros al amparo del art. 15.3 DCD

Declaración de los Países Bajos en virtud del artículo 15, apartado 3[1244], de la Directiva 2006/24/CE. Por lo que se refiere a la Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE, los Países Bajos harán uso de la opción de aplazar la aplicación de la Directiva a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet, durante un período no superior a 18 meses a partir de la fecha de entrada en vigor de la Directiva.

Declaración de Austria en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Austria declara que aplazará la aplicación de la presente Directiva a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet durante un período no superior a 18 meses a partir de la fecha especificada en el artículo 15, apartado 1.

Declaración de Estonia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. De acuerdo con el artículo 15, apartado 3, de la Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, Estonia declara su intención de hacer uso de ese párrafo y de aplazar la aplicación de la Directiva a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet hasta 36 meses después de la fecha de adopción de la Directiva.

[1244] Transcribimos aquí el precepto: "3. Cada Estado miembro podrá aplazar hasta el 15 de marzo de 2009 la aplicación de la presente Directiva en lo que se refiere a la conservación de los datos de comunicaciones en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet. Los Estados miembros que se propongan recurrir al presente apartado lo notificarán al Consejo y a la Comisión, mediante una declaración, en el momento de la adopción de la presente Directiva. Tal declaración se publicará en el Diario Oficial de la Unión Europea".

Declaración del Reino Unido en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. El Reino Unido declara, de acuerdo con el artículo 15, apartado 3, de la Directiva sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, que aplazará la aplicación de esa Directiva a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet.

Declaración de Chipre en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. La República de Chipre declara que aplazará la aplicación de la Directiva, respecto a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet, hasta la fecha fijada en el artículo 15, apartado 3.

Declaración de Grecia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Grecia declara que, de conformidad con el artículo 15, apartado 3, aplazará la aplicación de la presente Directiva, respecto a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet, hasta 18 meses después de la expiración del período fijado en el artículo 15, apartado 1.

Declaración de Luxemburgo en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Conforme a lo dispuesto en el apartado 15, apartado 3, de la Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, el Gobierno del Gran Ducado de Luxemburgo declara que tiene la intención de acogerse al artículo 15, apartado 3, de la Directiva en cuestión, a fin de poder aplazar su aplicación en lo que respecta a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet.

Declaración de Eslovenia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Eslovenia se une al grupo de Estados miembros que han hecho una

declaración en virtud del artículo 15, apartado 3, de la Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, relativa al aplazamiento de 18 meses de la Directiva a la conservación de datos de comunicación en relación con internet, la telefonía por internet y el correo electrónico por internet.

Declaración de Suecia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Suecia, en virtud del artículo 15, apartado 3, desea tener la opción de aplazar la aplicación de la presente Directiva a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet.

Declaración de Lituania en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. En virtud del artículo 15, apartado 3, del proyecto de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (en lo sucesivo, «la Directiva»), la República de Lituania declara que, una vez adoptada la Directiva, aplazará su aplicación a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet durante el período mencionado en el artículo 15, apartado 3.

Declaración de Letonia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. De acuerdo con el artículo 15, apartado 3, de la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, Letonia declara que aplazará la aplicación de la Directiva a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet hasta el 15 de marzo de 2009.

Declaración de la República Checa en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. En virtud del artículo 15, apartado 3, la República Checa declara que aplazará la aplicación de la presente Directiva a la conservación de datos de

comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet hasta 36 meses después de la fecha de su adopción.

Declaración de Bélgica en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Bélgica declara que, acogiéndose a la posibilidad prevista en el artículo 15, apartado 3, y durante un período de 36 meses tras la adopción de la presente Directiva, aplazará su aplicación respecto a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet.

Declaración de Polonia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Polonia declara que, en virtud de la posibilidad prevista en el artículo 15, apartado 3, de la Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE, la aplicación de la Directiva en lo relativo a la conservación de datos de comunicaciones en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet se aplazará hasta 18 meses después de la fecha a que se refiere el artículo 15, apartado 1.

Declaración de Finlandia en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Finlandia declara, de acuerdo con el artículo 15, apartado 3, de la Directiva sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, que aplazará la aplicación de esa Directiva a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet.

Declaración de Alemania en virtud del artículo 15, apartado 3, de la Directiva 2006/24/CE. Alemania se reserva el derecho a posponer la aplicación de la presente Directiva a la conservación de datos de comunicación en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet, por un período de 18 meses a partir de la fecha especificada en el artículo 15, apartado 1.

ANEXO. Disposiciones nacionales comunicadas por los Estados miembros acerca de las medidas de ejecución relativas a la Directiva

A continuación listamos, alfabetizadas, las disposiciones nacionales comunicadas por los Estados miembros acerca de las medidas de ejecución relativas a la Directiva[1245]:

Austria:

—Bundesgesetz, mit dem das Telekommunikations-gesetz 2003 – TKG 2003 geändert wird. Acto jurídico: Bundesgesetz, Número: I Nr. 27/2011; Diario Oficial: Bundesgesetzblatt für die Republik Österreich (BGBl.), Número: I Nr. 27/2011, Fecha de publicación: 18/05/2011, Entrada en vigor: 19/05/2011; Referencia: (MNE(2011)53999)

Alemania:

—Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG. Acto jurídico: Gesetz; Diario Oficial: Bundesgesetzblatt Teil 1 (BGB 1), Número: 70, Fecha de publicación: 31/12/2007, Página: 03198-03211, Entrada en vigor: 01/01/2008; Referencia: (MNE(2008)50149)

Bélgica:

—Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Acto jurídico: Loi; Diario Oficial: Moniteur Belge, Fecha de publicación: 27/03/1991; Referencia: (MNE(2007)58028)

—Arrêté royal du 9 janvier 2003 portant exécution des articles 46bis, § 2, alinéa 1er, 88bis, § 2, alinéas 1er et 3, et 90quater, § 2, alinéa 3, du code d'instruction criminelle ainsi que de l'article 109ter, E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Acto jurídico: Arrêté royal; Diario

[1245] Completamente actualizadas en http://eur-lex.europa.eu/Notice.do?val=470453:cs&lang=es&list=425159:cs,470453:cs,&pos=2&page=2&nbl=12&pgs=10&hwords=directiva 2006/24/CE~&checktexte=checkbox&visu=#texte

Oficial: Moniteur Belge, Fecha de publicación: 10/02/2003; Referencia: (MNE(2007)58029)

Bulgaria:

—Закон за електронните съобщения. Acto jurídico: Закон; Diario Oficial: Държавен вестник, Número: 17, Fecha de publicación: 02/03/2010, Entrada en vigor: 10/05/2010; Referencia: (MNE(2010)51800)

—Закон за електронните съобщения. Acto jurídico: Закон; Diario Oficial: Държавен вестник, Número: 93, Fecha de publicación: 24/11/2009, Entrada en vigor: 27/11/2009; Referencia: (MNE(2010)50342)

—Закон за електронните съобщения. Acto jurídico: Закон; Diario Oficial: Държавен вестник, Número: 41, Fecha de publicación: 22/05/2007, Página: 00021-00085, Entrada en vigor: 26/05/2007; Referencia: (MNE(2007)54201)

—Наредба № 40 от 7 януари 2008 г. за категориите данни и реда, по който се съхраняват и предоставят от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, за нуждите на националната сигурност и за разкриване на престъпления. Acto jurídico: Наредба на министър/ръководител на ведомство; Diario Oficial: Държавен вестник , Número: 9, Fecha de publicación: 29/01/2008, Entrada en vigor: 01/02/2008; Referencia: (MNE(2008)50827)

Chipre:

—Ο Περί Διατήρησης Τηλεπικοινωνιακών Δεδομένων με Σκοπό τη Διεύρηνση Σοβαρών Ποινικών Αδικημάτων Νόμος του 2007. Acto jurídico: Νόμος, Número: N. 183(I)/2007; Diario Oficial: Cyprus Gazette, Número: 4154, Fecha de publicación: 31/12/2007, Página: 01466-01483, Entrada en vigor: 31/12/2007; Referencia: (MNE(2008)50638)

Dinamarca:

—Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik. Acto jurídico: Bekendtgørelse, Número: 988; Diario Oficial: Lovtidende A, Fecha de publicación: 13/10/2006, Entrada en vigor: 15/09/2007; Referencia: (MNE(2007)56962)

—Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen). Acto jurídico: Bekendtgørelse, Número: 988; Diario Oficial: Lovtidende A, Fecha de publicación: 13/10/2006, Entrada en vigor: 15/09/2007; Referencia: (MNE(2007)56970)

—Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik. Acto jurídico: Bekendtgørelse, Número: 988; Diario Oficial: Lovtidende A, Fecha de publicación: 13/10/2006, Entrada en vigor: 15/09/2007; Referencia: (MNE(2007)56966)

Eslovaquia:

—Zákon č. 117/2006 Z. z., ktorým sa mení a dopĺňa zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov a o zmene a doplnení niektorých predpisov. Acto jurídico: zákon, Número: 117/2006; Diario Oficial: Zbierka zákonov SR, Número: 48, Fecha de publicación: 01/03/2006, Entrada en vigor: 01/04/2006; Referencia: (MNE(2006)51626)

—Zákon č. 220/2007 Z. z. o digitálnom vysielaní programových služieb a poskytovaní iných obsahových služieb prostredníctvom digitálneho prenosu a o zmene a doplnení niektorých zákonov (zákon o digitálnom vysielaní). Acto jurídico: zákon, Número: 220/2007; Diario Oficial: Zbierka zákonov SR, Número: 99, Fecha de publicación: 05/05/2007, Entrada en vigor: 31/05/2007; Referencia: (MNE(2007)58281)

—Zákon č. 610/2003 Z. z. o elektronických komunikáciách. Acto jurídico: zákon; Diario Oficial: Zbierka zákonov SR, Número: 249, Fecha de publicación: 31/12/2003, Página: 5826-5857; Referencia: (MNE(2003)51967)

—Zákon č. 654/2007 Z. z., ktorým sa mení a dopĺňa zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov a o zmene niektorých zákonov.Acto jurídico: zákon, Número: 654/2007; Diario Oficial: Zbierka zákonov SR, Número: 264, Fecha de publicación: 29/12/2007, Entrada en vigor: 29/12/2007; Referencia: (MNE(2008)50357)

—Zákon č. 428/2002 Z. z. o ochrane osobných údajov. Acto jurídico: zákon, Número: 428/2002; Diario Oficial: Zbierka zákonov SR, Número: 167, Fecha de publicación: 31/07/2002, Entrada en vigor: 01/09/2002; Referencia: (MNE(2005)56339)

—Zákon č. 716/2004 Z. z., ktorým sa mení a dopĺňa zákon č. 610/2003 Z. z. o elektronických komunikáciách. Acto jurídico: zákon, Número: 716/2004; Diario Oficial: Zbierka zákonov SR, Número: 297, Fecha de publicación: 28/12/2004, Entrada en vigor: 28/12/2004; Referencia: (MNE(2008)50351)

—Zákon č. 69/2005 Z. z., ktorým sa mení a dopĺňa zákon Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov a o zmene a doplnení niektorých zákonov. Acto jurídico: zákon, Número: 69/2005; Diario Oficial: Zbierka zákonov SR, Número: 32, Fecha de publicación: 26/02/2005, Entrada en vigor: 01/05/2005; Referencia: (MNE(2005)50500)

—Zákon č. 90/2005 Z. z., ktorým sa mení a dopĺňa zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov. Acto jurídico: zákon, Número: 90/2005; Diario Oficial: Zbierka zákonov SR, Número: 40, Fecha de publicación: 12/03/2005, Entrada en vigor: 01/05/2005; Referencia: (MNE(2005)56340)

—Zákon č. 40/1964 Zb. Občiansky zákonník. Acto jurídico: zákon; Diario Oficial: Zbierka zákonov SR, Número: 19, Fecha de publicación: 05/03/1964, Página: 201-246; Referencia: (MNE(2003)51926)

—Zákon č. 47/1992 Zb. - úplné znenie Občianskeho zákonníka z 26. februára 1964 č. 40 Zb., ako vyplýva zo zmien, doplnení a úprav vykonaných zákonom z 5. júna 1969 č. 58 Zb., zákonom z 9. novembra 1982 č. 131 Zb., zákonom z 15. júna 1988 č. 94 Zb., zákonom zo 14. decembra 1988 č. 188 Zb., zákonom z 28. marca 1990 č. 87 Zb., zákonom z 18. apríla 1990 č. 105 Zb., zákonom z 23. apríla 1990 č. 116 Zb., zákonom z 21. februára 1991 č. 87 Zb. a zákonom z 5. novembra 1991 č. 509 Zb. Acto jurídico: zákon; Diario Oficial: Zbierka zákonov SR, Número: 10, Fecha de publicación: 07/02/1992, Página: 218-277; Referencia: (MNE(2003)51928)

—Trestný zákon č. 300/2005 Z. z. Acto jurídico: zákon, Número: 300/2005; Diario Oficial: Zbierka zákonov SR, Número: 129, Fecha de publicación: 02/07/2005, Entrada en vigor: 01/01/2006; Referencia: (MNE(2005)52821)

—Zákon č. 301/2005 Z. z. Trestný poriadok. Acto jurídico: zákon, Número: 301/2005; Diario Oficial: Zbierka zákonov SR, Número: 130, Fecha de publicación: 02/07/2005, Entrada en vigor: 01/01/2006; Referencia: (MNE(2007)50846)

Eslovenia:

—Pravilnik o načinu posredovanja hranjenih podatkov o prometu telefonskih in podatkovnih storitev v mobilnem in fiksnem elektronskem komunikacijskem omrežju. Acto jurídico: Pravilnik; Diario Oficial: Uradni list RS, Número: 103/2009, Fecha de publicación: 14/12/2009, Página: 13941-13942, Entrada en vigor: 13/01/2010; Referencia: (MNE(2010)52084)

—Pravilnik o načinu posredovanja hranjenih podatkov o prometu telefonskih storitev v mobilnem in fiksnem elektronskem komunikacijskem omrežju. Acto jurídico: Pravilnik; Diario Oficial: Uradni list RS, Número: 31/2008, Fecha de publicación: 28/03/2008, Página: 02833-02834, Entrada en vigor: 12/04/2008; Referencia: (MNE(2008)53080)

—Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah. Acto jurídico: Zakon; Diario Oficial: Uradni list RS, Número: 129/2006, Fecha de publicación: 12/12/2006, Página: 14113-14128, Entrada en vigor: 27/12/2006; Referencia: (MNE(2007)50469)

—Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-B). Acto jurídico: Zakon; Diario Oficial: Uradni list RS, Número: 110/2009, Fecha de publicación: 29/12/2009, Página: 14965-14974, Entrada en vigor: 28/01/2010; Referencia: (MNE(2010)51460)

España:

— Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Acto jurídico: Ley, Número: 25/2007; Diario Oficial: Boletín Oficial del Estado (B.O.E), Número: 251/2007, Fecha de publicación: 19/10/2007, Página: 42517-42523, Entrada en vigor: 08/11/2007; Referencia: (MNE(2007)57464)

Estonia:

—Elektroonilise Side Seaduse Ja Rahvatervise Seaduse Muutmise Seadus. Acto jurídico: seaduse parandus, Número: RTI, 07.12.2007, 63, 397; Diario Oficial: Elektrooniline Riigi Teataja, Número: RTI, 07.12.2007, 63, 397; Referencia: (MNE(2007)58607)

—Elektroonilise Side Seadus1. Acto jurídico: seadus, Número: RT I 2004, 87, 593; Diario Oficial: Elektrooniline Riigi Teataja, Número: RT I 2004, 87, 593, Entrada en vigor: 13/07/2008; Referencia: (MNE(2008)54522)

Finlandia:

—Viestintäviraston määräys tunnistamistietojen tallennusvelvollisuudesta / Kommunikationsverkets föreskrift om skyldighet att lagra identifieringsuppgifter. Acto jurídico: Määräys, Número: 53/2008 M; Diario Oficial: Hallinnolliset toimet, Número: 53/2008 M, Entrada en vigor: 05/06/2008; Referencia: (MNE(2008)53494)

—Laki sähköisen viestinnän tietosuojalain muuttamisesta / Lag om ändring av lagen om dataskydd vid elektronisk kommunikation. Acto jurídico: Laki, Número: 343/2008; Diario Oficial: Suomen Saadoskokoelma (SK), Número: 343, Fecha de publicación: 29/05/2008, Página: 00913-00916, Entrada en vigor: 01/06/2008; Referencia: (MNE(2008)53493)

Francia:

—Décret no 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques. Acto jurídico: Décret, Número: 2006-358; Diario Oficial: Journal Officiel de la République Française (JORF), Fecha de publicación: 26/03/2006, Entrada en vigor: 27/03/2006; Referencia: (MNE(2007)56763)

Página: 00106-00106, Entrada en vigor: 26/01/2011; Referencia: (MNE(2011)53014)

Grecia:

—Διατήρηση δεδομένων που παράγονται ή υποβάλλο−νται σε επεξεργασία σε συνάρτηση με την παροχήδιαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επι−κοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήσησυστημάτων επιτήρησης με τη λήψη ή καταγραφήήχου ή εικόνας σε δημόσιους χώρους και συναφείςδιατάξεις. Acto jurídico: Νόμος, Número: 3917; Diario Oficial: Εφημερίς της Κυβερνήσεως (ΦΕΚ) (Τεύχος Α), Número: 22, Fecha de publicación: 21/02/2011, Página: 00975-00981, Entrada en vigor: 21/02/2011; Referencia: (MNE(2011)51652)

Hungría:

—1972. évi V. TÖRVÉNYa Magyar Köztársaság ügyészségéről. Acto jurídico: Törvény, Número: 1972/V.; Diario Oficial: Magyar Közlöny, Número: 1972/52.; Referencia: (MNE(2008)52195)

—1995. évi CXXV.törvénya nemzetbiztonsági szolgálatokról. Acto jurídico: Törvény, Número: 1995/CXXV.; Diario Oficial: Magyar Közlöny, Número: 1995/116., Página: 07156-07193; Referencia: (MNE(2008)52161)

—A Kormány180/2004. (V. 26.) Korm.rendeleteaz elektronikus hírközlési feladatokat ellátószervezetek és a titkos információgyûjtésre, illetvetitkos adatszerzésre felhatalmazott szervezetekegyüttműködésének rendjéről. Acto jurídico: kormányrendelet, Número: 180/2004. KOR; Diario Oficial: Magyar Közlöny, Número: 2004/71., Página: 07246-07250; Referencia: (MNE(2008)52160)

—A Kormány38/2008. (II. 23.) Korm.rendeleteaz elektronikus hírközlési feladatokat ellátószervezetek és a titkos információgyûjtésre,illetve titkos adatszerzésre felhatalmazott szervezetekegyüttműködésének rendjéről szóló180/2004. (V. 26.) Korm. rendelet módosításáról. Acto jurídico: kormányrendelet, Número: 38/2008. KOR; Diario Oficial: Magyar Közlöny, Número: 2008/29., Página: 01308-01310; Referencia: (MNE(2008)52156)

—A Kormány300/2007. (XI. 9.) Korm.rendeletea 2008. évre vonatkozó Országos StatisztikaiAdatgyűjtési Program módosított és újadatgyűjtéseiről. Acto jurídico: kormányrendelet, Número: 300/2007. KOR; Diario Oficial: Magyar Közlöny, Número: 2007/151., Página: 10547-10570; Referencia: (MNE(2008)52154)

—2007. évi CLXXIV.törvényaz elektronikus hírközlésről szóló2003. évi C. törvény módosításáról. Acto jurídico: Törvény, Número: 2007/CLXXIV.; Diario Oficial: Magyar Közlöny, Número: 2007/184., Página: 14749-14755; Referencia: (MNE(2008)52152)

—1978. évi IV. törvény a büntető törvénykönyvről. Acto jurídico: Törvény, Número: 1978/IV; Diario Oficial: Magyar Közlöny, Número: 1978/92, Fecha de publicación: 31/12/1978, Página: 01048-01144; Referencia: (MNE(2003)55557)

—1992. évi LXIII.törvénya személyes adatok védelmérőlés a közérdekű adatok nyilvánosságáról. Acto jurídico: Törvény, Número: 1992/LXIII; Diario Oficial: Magyar Közlöny, Número: 1992/116., Página: 03962-03967; Referencia: (MNE(2005)55972)

—1993. évi LIX. törvény az állampolgári jogok országgyűlési biztosáról. Acto jurídico: Törvény; Diario Oficial: Magyar Közlöny, Número: 81, Fecha de publicación: 01/06/1993, Página: 4433-4440; Referencia: (MNE(2003)55394)

—1994. évi XXXIV.törvénya Rendőrségről. Acto jurídico: Törvény, Número: 1994. XXXIV.; Diario Oficial: Magyar Közlöny, Número: 1994/41., Página: 01422-01443; Referencia: (MNE(2007)56959) Acto jurídico: Törvény, Número: 1998/19; Diario Oficial: Magyar Közlöny, Número: 1998/23., Página: 01776-01872; Referencia: (MNE(2004)53855)

—226/2003. (XII. 13.) kormányrendelet az elektronikus hírközlési szolgáltató adatkezelésének különös feltételeiről, az elektronikus hírközlési szolgáltatások adatbiztonságáról, valamint az azonosítókijelzés és hívásátirányítás szabályairól. Acto jurídico: kormányrendelet; Diario Oficial: Magyar Közlöny, Número: 144, Fecha de publicación: 13/12/2003, Página: 11109-11113; Referencia: (MNE(2003)55408)

—2003. évi C. törvény az elektronikus hírközlésről. Acto jurídico: Törvény, Número: 2003/C; Diario Oficial: Magyar Közlöny, Número: 2003/136, Fecha de publicación: 27/11/2003, Página: 10420-10483, Entrada en vigor: 01/01/2004; Referencia: (MNE(2003)54694)

—2004. évi XIX.törvénya Vám- és Pénzügyõrségrõl. Acto jurídico: Törvény, Número: 2004/XIX.; Diario Oficial: Magyar Közlöny, Número: 2004/50., Página: 04434-04445; Referencia: (MNE(2007)58991)

Irlanda:

—Communications (Retention Of Data) Bill 2009. Acto jurídico: Act (primary legislation); Diario Oficial: Iris Oifigiúl, Número: not yet published; Referencia: (MNE(2011)50869)

—Communications (Retention Of Data) Act 2011. Acto jurídico: Act (primary legislation), Número: Act Number 3 of 2011; Diario Oficial: Iris Oifigiúl, Fecha de publicación: 28/01/2011,

Italia:

—Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE. Acto jurídico: Decreto legislativo, Número: 109; Diario Oficial: Gazzetta Ufficiale della Repubblica Italiana, Número: 141, Fecha de publicación: 18/06/2008; Referencia: (MNE(2008)53834)

Letonia:

—Latvijas administratīvo pārkāpumu kodekss. Acto jurídico: Likums; Diario Oficial: LR Augstākās Padomes un Valdības Ziņotājs, Número: 51, Fecha de publicación: 20/12/1984, Entrada en vigor: 01/07/1985; Referencia: (MNE(2009)51799)

—Grozījumi Krimināllikumā. Acto jurídico: Likums; Diario Oficial: Latvijas Vēstnesis, Número: 155, Fecha de publicación: 30/09/2009, Entrada en vigor: 14/10/2009; Referencia: (MNE(2009)54444)

—Elektronisko sakaru likums. Acto jurídico: Likums; Diario Oficial: Latvijas Vēstnesis, Número: 183, Fecha de publicación: 17/11/2004, Entrada en vigor: 01/12/2004; Referencia: (MNE(2009)51910)

—Krimināllikums. Acto jurídico: Likums; Diario Oficial: Latvijas Vēstnesis, Número: 199/200, Fecha de publicación: 08/07/1998, Entrada en vigor: 01/04/1999; Referencia: (MNE(2009)51798)

—Kārtība, kādā pirmstiesas izmeklēšanas iestādes, operatīvās darbības subjekti, valsts drošības iestādes, prokuratūra un tiesa pieprasa un elektronisko sakaru komersants nodod saglabājamos datus, kā arī kārtība, kādā apkopo statistisko informāciju par saglabājamo datu pieprasījumiem un to izsniegšanu. Acto jurídico: Ministru Kabineta noteikumi, Número: 820; Diario Oficial: Latvijas Vēstnesis, Número: 197, Fecha de publicación: 07/12/2007, Entrada en vigor: 08/12/2007; Referencia: (MNE(2008)50003)

—Grozījumi Elektronisko sakaru likumā. Acto jurídico: Likums; Diario Oficial: Latvijas Vēstnesis, Número: 83, Fecha de publicación: 24/05/2007, Entrada en vigor: 07/06/2007; Referencia: (MNE(2007)54265)

Lituania:

—Lietuvos Respublikos elektroninių ryšių įstatymo 1, 3, 7, 12, 34, 77 straipsnių, devintojo skirsnio ir priedo pakeitimo ir papildymo bei Įstatymo papildymo nauju priedu įstatymas Nr. X-1835. Acto jurídico: Įstatymas, Número: X-1835/2008; Diario Oficial: Valstybės žinios, Número: 137, Fecha de publicación: 29/11/2008, Entrada en vigor: 15/03/2009; Referencia: (MNE(2008)56479)

—Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas Nr. X-1444. Acto jurídico: Įstatymas, Número: X-1444/2008; Diario Oficial: Valstybės žinios, Número: 22, Fecha de publicación: 23/02/2008, Entrada en vigor: 01/01/2009; Referencia: (MNE(2008)55189)

—Lietuvos Respublikos elektroninių ryšių įstatymas Nr. IX-2135. Acto jurídico: Įstatymas, Número: IX-2135/2004; Diario Oficial: Valstybės žinios, Número: 69, Fecha de publicación: 30/04/2004, Entrada en vigor: 01/05/2004; Referencia: (MNE(2008)55188)

—Lietuvos Respublikos Vyriausybės 2009 m. liepos 22 d. nutarimas Nr. 789 Dėl Statistinių duomenų, nurodytų Lietuvos Respublikos elektroninių ryšių įstatymo 70 straipsnyje, teikimo tvarkos aprašo patvirtinimo. Acto jurídico: Nutarimas, Número: 789/2009; Diario Oficial: Valstybės žinios, Número: 90, Fecha de publicación: 30/07/2009, Entrada en vigor: 31/07/2009; Referencia: (MNE(2009)53782)

—Lietuvos Respublikos Vyriausybės 2009 m. liepos 22 d. nutarimas Nr. 788 „Dėl Lietuvos Respublikos Vyriausybės 2004 m. gruodžio 6 d. nutarimo Nr. 1593 "Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą" pakeitimo". Acto jurídico: Nutarimas, Número: 788/2009; Diario Oficial: Valstybės žinios, Número: 90, Fecha de publicación: 30/07/2009, Entrada en vigor: 31/07/2009; Referencia: (MNE(2009)53781)

—Lietuvos Respublikos Vyriausybės 2010 m. lapkričio 3 d. nutarimas Nr. 1569 "Dėl Duomenų apie elektroninių ryšių įvykius viešuosiuose ryšių tinkluose teikimo Lietuvos Respublikos kompetentingoms institucijoms tvarkos aprašo patvirtinimo". Acto jurídico: Nutarimas, Número: 1569/2010; Diario Oficial: Valstybės žinios, Número: 133, Fecha de publicación: 13/11/2010, Entrada en vigor: 14/11/2010; Referencia: (MNE(2010)56836)

Luxemburgo:

—Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle. Acto jurídico: Loi;

Diario Oficial: Mémorial Luxembourgeois A, Número: 122, Fecha de publicación: 29/07/2010, Página: 02060-02061; Referencia: (MNE(2010)55061)

—Règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics. Acto jurídico: Règlement Grand-ducal; Diario Oficial: Mémorial Luxembourgeois A, Número: 122, Fecha de publicación: 29/07/2010, Página: 02061-02062; Referencia: (MNE(2010)55062)

—Loi du 30 mai 2005– relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des donnéesà caractère personnel dans le secteur des communications électroniques et– portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle. Acto jurídico: Loi; Diario Oficial: Mémorial Luxembourgeois A, Número: 73, Fecha de publicación: 07/06/2005, Página: 01168-01173; Referencia: (MNE(2008)52016)

—Loi du 27 juillet 2007 portant modification– de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement desdonnées à caractère personnel;– des articles 4 paragraphe (3) lettre d); 5 paragraphe (1) lettre a); 9 paragraphe (1) lettre a)et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur descommunications électroniques et– de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expressiondans les médias. Acto jurídico: Loi; Diario Oficial: Mémorial Luxembourgeois A, Número: 131, Fecha de publicación: 08/08/2007, Página: 02330-02338; Referencia: (MNE(2008)52017)

—Texte coordonné de la loi du 2 août 2002 relative à la protection des personnes à l'égard dutraitement des données à caractère personnel modifiée parla loi du 31 juillet 2006,la loi du 22 décembre 2006,la loi du 27 juillet 2007. Acto jurídico: Loi; Diario Oficial: Mémorial Luxembourgeois A, Número: 131, Fecha de publicación: 08/08/2007, Página: 02339-02361; Referencia: (MNE(2008)52019)

Malta:

—L.N. 199 of 2008ELECTRONIC COMMUNICATIONS (REGULATION) ACT(CAP. 399)Electronic Communications (Personal Data and Protection ofPrivacy) (Amendment) Regulations, 2008. Acto jurídico: Regulation, Número: LN199/08; Diario Oficial: The Malta government gazette, Número: 18302, Fecha de publicación: 29/08/2008, Página: 02995-02996; Referencia: (MNE(2008)54916)

—L.N. 198 of 2008DATA PROTECTION ACT(CAP. 440)Processing of Personal Data(Electronic Communications Sector) (Amendment)Regulations, 2008. Acto jurídico: Regulation, Número: LN198/08; Diario Oficial: The Malta government gazette, Número: 18302, Fecha de publicación: 29/08/2008, Página: 02979-02994; Referencia: (MNE(2008)54915)

Países Bajos:

— Besluit van 25 augustus 2009 tot vaststelling van het tijdstip van inwerkingtreding van de Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet en de Wet op deeconomische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wetbewaarplicht telecommunicatiegegevens). Acto jurídico: Besluit; Diario Oficial: Staatsblad (Bulletin des Lois et des Décrets royaux), Número: 360, Fecha de publicación: 28/08/2009, Página: 00001-00002; Referencia: (MNE(2009)53724)

—Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wetbewaarplicht telecommunicatiegegevens). Acto jurídico: Wet; Diario Oficial: Staatsblad (Bulletin des Lois et des Décrets royaux), Número: 333, Fecha de publicación: 30/07/2009, Página: 00001-00008, Entrada en vigor: 01/09/2009; Referencia: (MNE(2009)53723)

—Besluit van 11 augustus 2009, houdende wijziging van het Besluit beveiliging gegevens aftappen telecommunicatie in verband met het bewaren van

telecommunicatiegegevens (Besluit beveiliging gegevens telecommunicatie). Acto jurídico: Besluit; Diario Oficial: Staatsblad (Bulletin des Lois et des Décrets royaux), Número: 350, Fecha de publicación: 28/08/2009, Página: 00001-00018; Referencia: (MNE(2009)53735)

Polonia:

—Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Acto jurídico: Ustawa; Diario Oficial: Dziennik Ustaw, Número: 2004/171/1800, Fecha de publicación: 03/08/2004, Entrada en vigor: 03/09/2004; Referencia: (MNE(2004)50474)

—Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania. Acto jurídico: Rozporządzenie, Número: 2009/226/1828; Diario Oficial: Dziennik Ustaw, Número: 2009/226/1828; Referencia: (MNE(2010)50067)

—Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw. Acto jurídico: Nowelizacja, Número: 2009/85/716; Diario Oficial: Dziennik Ustaw, Número: 2009/85/716; Referencia: (MNE(2009)52452)

—Rozporządzenie Ministra Infrastruktury z dnia 30 grudnia 2009 r. w sprawie wzoru formularza służącego do przekazywania przez przedsiębiorcę telekomunikacyjnego Prezesowi Urzędu Komunikacji Elektronicznej informacji dotyczących udostępniania danych. Acto jurídico: Rozporządzenie, Número: 2010/3/15; Diario Oficial: Dziennik Ustaw, Número: 2010/3/15; Referencia: (MNE(2010)50431)

—Rozporządzenie Prezesa Rady Ministrów z dnia 22 marca 2010 r. w sprawie sposobu przekazywania i udostępniania danych w przypadku ogłoszenia upadłości operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych. Acto jurídico: Rozporządzenie, Número: 2010/48/281; Diario Oficial: Dziennik Ustaw, Número: 2010/48/281; Referencia: (MNE(2010)52270)

Portugal:

—Assembleia da República-Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações. Acto jurídico: Lei, Número: Lei n.º 32/2008; Diario Oficial: Diaro da Republica, Número: DR n.º 137, Fecha de publicación: 17/07/2008, Página: 04454-04458; Referencia: (MNE(2008)54123)

Reino Unido:

—The Data Retention (EC Directive) Regulations 2009. Acto jurídico: Statutory instrument (SI), Número: 2009 no 859; Diario Oficial: Her Majesty's Stationery Office (HMSO), Número: SI 2009 no 859, Entrada en vigor: 06/04/2009; Referencia: (MNE(2010)53135)

—The Data Retention (EC Directive) Regulations 2007. Acto jurídico: Statutory instrument (SI), Número: Statutory Instrument 20; Diario Oficial: Her Majesty's Stationery Office (HMSO), Número: ISBN 978 0 11 078328 4 , Entrada en vigor: 01/10/2007; Referencia: (MNE(2007)57200)

República Checa:

—Zákon č. 247/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. Acto jurídico: Zákon, Número: 247/2008; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 04/07/2008; Referencia: (MNE(2008)55679)

—Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Acto jurídico: Zákon, Número: 101/2000; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 25/04/2000; Referencia: (MNE(2003)56450)

—Zákon č. 150/2002 Sb., soudní řád správní. Acto jurídico: Zákon, Número: 150/2002 ; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 17/04/2002; Referencia: (MNE(2003)56626)

—Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Acto jurídico: Zákon, Número: 127/2005; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 31/03/2005; Referencia: (MNE(2005)50325)

—Zákon č. 290/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o Vojenském zpravodajství. Acto jurídico: Zákon, Número: 290/2005; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 18/07/2005; Referencia: (MNE(2007)54106)

—Vyhláška č. 336/2005 Sb., o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv. Acto jurídico: Vyhláška, Número: 336/2005; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 29/08/2005; Referencia: (MNE(2007)54107)

—Zákon č. 361/2005 Sb., kterým se mění zákon č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů, a některé další zákony. Acto jurídico: Zákon, Número: 361/2005; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 19/09/2005; Referencia: (MNE(2005)60135)

—Vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. Acto jurídico: Vyhláška, Número: 485/2005; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 15/12/2005; Referencia: (MNE(2007)54108)

—Zákon č. 310/2006 Sb., o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území České republiky a o změně některých dalších zákonů (zákon o nakládání s bezpečnostním materiálem). Acto jurídico: Zákon, Número: 310/2006; Diario Oficial: Sbirka Zakonu CR, Fecha de publicación: 22/06/2006; Referencia: (MNE(2007)54099)

Rumania:

—Lege privind reținerea datelor generate sau prelucrate de furnizorii de servicii de comunicații electronice destinate publicului sau de rețele publice de comunicații, precum și pentru modificarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice. Acto jurídico: Lege, Número: 298; Diario Oficial: Monitorul Oficial al României, Número: 780, Fecha de publicación: 21/11/2008, Página: 00003-00006, Entrada en vigor: 20/01/2009; Referencia: (MNE(2008)56339)

Suecia: SIN REFERENCIA

ANEXO. Texto íntegro de la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos.

Reproducimos a continuación el texto íntegro, en su versión española, de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, tal como fue publicado en el Diario Oficial de la Unión Europea, n° L 105, de 13 de abril de 2006, p. 0054 - 0063.

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

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado por el que se establece la Comunidad Europea y, en particular, su artículo 95,

Vista la propuesta de la Comisión,

Visto el dictamen del Comité Económico y Social Europeo[1246],

De conformidad con el procedimiento establecido en el artículo 251 del Tratado[1247],

Considerando lo siguiente:

[1246] Dictamen emitido el 19 de enero de 2006 (no publicado aún en el Diario Oficial).

[1247] Dictamen del Parlamento Europeo de 14 de diciembre de 2005 (no publicado aún en el Diario Oficial) y Decisión del Consejo de 21 de febrero de 2006.

(1) La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[1248], exige que los Estados miembros protejan los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de datos personales y, en particular, su derecho a la intimidad, para asegurar el libre flujo de datos personales en la Comunidad.

(2) 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[1249], traduce los principios establecidos en la Directiva 95/46/CE a normas específicas para el sector de las comunicaciones electrónicas.

(3) Los artículos 5, 6 y 9 de la Directiva 2002/58/CE definen las normas aplicables al tratamiento, por los proveedores de red y de servicios, de los datos de tráfico y de localización generados por el uso de servicios de comunicaciones electrónicas. Estos datos deben borrarse o hacerse anónimos cuando ya no se necesiten para la transmisión, salvo los datos necesarios para la facturación o los pagos por interconexión. Previo consentimiento, determinados datos pueden también tratarse con fines comerciales y la prestación de servicios de valor añadido.

(4) El artículo 15, apartado 1, de la Directiva 2002/58/CE fija las condiciones en que los Estados miembros pueden limitar el alcance de los derechos y obligaciones que se establecen en el artículo 5, el artículo 6, el artículo 8, apartados 1 a 4, y el artículo 9 de dicha Directiva. Tales restricciones deben constituir medidas necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas.

[1248] DO L 281 de 23.11.1995, p. 31. Directiva modificada por el Reglamento (CE) no 1882/2003 (DO L 284 de 31.10.2003, p. 1).

[1249] DO L 201 de 31.7.2002, p. 37.

(5) Varios Estados miembros han adoptado legislación que prevé la conservación de datos por los prestadores de servicios para la prevención, investigación, detección y enjuiciamiento de delitos. Estas disposiciones de las normativas nacionales varían considerablemente.

(6) Las diferencias legales y técnicas entre disposiciones nacionales sobre conservación de datos con fines de prevención, investigación, detección y enjuiciamiento de delitos crean obstáculos en el mercado interior de las comunicaciones electrónicas; los prestadores de servicios deben cumplir requisitos diferentes en cuanto a los tipos de datos de tráfico y de localización que deben conservarse, así como en cuanto a las condiciones y los períodos de conservación.

(7) Las conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002 destacan que, a causa del crecimiento significativo de las posibilidades de las comunicaciones electrónicas, los datos relativos al uso de comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en la prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada.

(8) La Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo el 25 de marzo de 2004, encargó al Consejo que examinara medidas para establecer normas sobre la conservación por los prestadores de servicios de datos de tráfico de las comunicaciones.

(9) De conformidad con el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), toda persona tiene derecho al respeto de su vida privada y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de ese derecho salvo cuando esa injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria, entre otras cosas, para la seguridad nacional o la seguridad pública, la prevención de desórdenes o delitos, o la protección de los derechos y las libertades de terceros. Dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición

de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva. Por consiguiente, la adopción de un instrumento de conservación de datos que cumpla los requisitos del artículo 8 del CEDH es una medida necesaria.

(10) El 13 de julio de 2005, el Consejo reafirmó en su declaración de condena de los atentados terroristas de Londres la necesidad de adoptar cuanto antes medidas comunes sobre conservación de datos de telecomunicaciones.

(11) Dada la importancia de los datos de tráfico y de localización para la investigación, detección y enjuiciamiento de delitos, según demuestran la investigación y la experiencia práctica de varios Estados miembros, existe la necesidad de asegurar a escala europea que los datos generados o tratados, en el marco de la prestación de servicios de comunicaciones, por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones se conservan durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva.

(12) El artículo 15, apartado 1, de la Directiva 2002/58/CE sigue aplicándose a los datos, incluidos los datos relativos a las llamadas telefónicas infructuosas, cuya conservación no se prescribe específicamente en la presente Directiva y que, por consiguiente, quedan fuera del ámbito de aplicación de la misma, así como a la conservación a efectos, incluidos judiciales, diferentes de los contemplados en la presente Directiva.

(13) La presente Directiva sólo se refiere a los datos generados o tratados como consecuencia de una comunicación o de un servicio de comunicación y no a los datos que constituyen el contenido de la información comunicada. Los datos deben conservarse de tal manera que se evite que se conserven más de una vez. Los datos generados o tratados, cuando se presten servicios de comunicaciones electrónicas, se refieren a los datos accesibles. En particular, en lo referente a la conservación de datos relativos a los correos electrónicos y la telefonía por internet, la obligación de conservar datos sólo puede aplicarse con respecto a los datos de los servicios propios de los proveedores o de los proveedores de redes.

(14) Las tecnologías relativas a las comunicaciones electrónicas están cambiando rápidamente y los legítimos requisitos de las autoridades competentes pueden evolucionar. Para obtener asesoramiento y fomentar el intercambio de experiencias de las mejores prácticas sobre estos asuntos, la Comisión tiene intención de crear un grupo integrado por autoridades policiales de los Estados miembros, asociaciones del sector de las comunicaciones electrónicas, representantes del Parlamento Europeo y autoridades de protección de datos, incluido el Supervisor Europeo de Protección de Datos.

(15) La Directiva 95/46/CE y la Directiva 2002/58/CE son plenamente aplicables a los datos conservados de conformidad con la presente Directiva; el artículo 30, apartado 1, letra c), de la Directiva 95/46/CE exige la consulta al GT29 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, establecido de conformidad con el artículo 29 de dicha Directiva.

(16) Las obligaciones impuestas a los proveedores de servicios en relación con las medidas para garantizar la calidad de los datos, derivadas del artículo 6 de la Directiva 95/46/CE, y sus obligaciones relativas a la garantía de la confidencialidad y seguridad del tratamiento de datos, derivadas de los artículos 16 y 17 de dicha Directiva, son plenamente aplicables a los datos conservados a efectos de la presente Directiva.

(17) Es esencial que los Estados miembros adopten medidas legislativas para asegurar que los datos conservados de conformidad con la presente Directiva solamente se faciliten a las autoridades nacionales competentes de conformidad con la legislación nacional, respetando plenamente los derechos fundamentales de las personas afectadas.

(18) En este contexto, el artículo 24 de la Directiva 95/46/CE impone a los Estados miembros la obligación de establecer sanciones por el incumplimiento de las disposiciones adoptadas en virtud de dicha Directiva. El artículo 15, apartado 2, de la Directiva 2002/58/CE impone la misma obligación respecto de las disposiciones nacionales adoptadas en virtud de la Directiva 2002/58/CE. La Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los

sistemas de información[1250], establece que el acceso intencionado e ilícito a un sistema de información, incluido a los datos conservados dentro del mismo, debe ser sancionable como delito.

(19) El derecho de toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva 95/46/CE, a obtener la reparación del perjuicio sufrido, de conformidad con el artículo 23 de dicha Directiva, se aplica también al tratamiento ilícito de cualquier tipo de datos personales con arreglo a la presente Directiva.

(20) El Convenio del Consejo de Europa de 2001 sobre la delincuencia cibernética y el Convenio del Consejo de Europa de 1981 sobre la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal abarcan igualmente los datos conservados en el sentido de la presente Directiva.

(21) Dado que los objetivos de la presente Directiva, a saber, armonizar las obligaciones de los proveedores de conservar determinados datos y asegurar que éstos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la normativa nacional de cada Estado miembro, como el terrorismo y la delincuencia organizada, no pueden ser alcanzados de manera suficiente por los Estados miembros y, debido a la dimensión y los efectos de la presente Directiva, pueden lograrse mejor a nivel comunitario, la Comunidad puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.

(22) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea. En especial, la presente Directiva, junto con la Directiva 2002/58/CE, intenta garantizar el pleno cumplimiento de los derechos fundamentales de los ciudadanos al

[1250] DO L 69 de 16.3.2005, p. 67.

respeto de la vida privada y de las comunicaciones y a la protección de los datos de carácter personal, consagrados en los artículos 7 y 8 de la Carta.

(23) Dado que la obligación de los proveedores de servicios de comunicación electrónica debe ser proporcionada, la Directiva exige que se conserven exclusivamente los datos generados o tratados en el proceso del suministro de servicios de comunicación. Siempre que dichos datos no hayan sido generados o tratados por dichos proveedores, no es obligatorio conservarlos. La presente Directiva no tiene por objeto la armonización de la tecnología de conservación de datos, cuya elección es una cuestión que debe resolverse a nivel nacional.

(24) Con arreglo al punto 34 del Acuerdo interinstitucional "Legislar mejor"[1251], se alienta a los Estados miembros a establecer, en su propio interés y en el de la Comunidad, sus propios cuadros, que muestren, en la medida de lo posible, la concordancia entre la presente Directiva y las medidas de transposición, y a hacerlos públicos.

(25) La presente Directiva se entiende sin perjuicio de la facultad de los Estados miembros para adoptar medidas legislativas relativas al derecho de acceso y de utilización de los datos por parte de las autoridades nacionales tal como determinen los mismos. Las cuestiones relativas al acceso por parte de las autoridades nacionales a datos conservados con arreglo a la presente Directiva para las actividades contempladas en el artículo 3, apartado 2, primer guión, de la Directiva 95/46/CE, quedan fuera del ámbito de aplicación del Derecho comunitario. Sin embargo, pueden estar sometidas a la legislación nacional o a una acción como las previstas por las disposiciones del título VI del Tratado de la Unión Europea. Dichas leyes o acciones deben respetar plenamente los derechos fundamentales que se derivan de tradiciones constitucionales comunes de los Estados miembros y están garantizados por el CEDH. Con arreglo al artículo 8 del CEDH, según la interpretación del Tribunal Europeo de Derechos Humanos, la injerencia de las autoridades públicas en el derecho a la vida privada debe respetar los requisitos de necesidad y proporcionalidad y debe, por consiguiente, servir

[1251] DO C 321 de 31.12.2003, p. 1.

a propósitos específicos, explícitos y legítimos y ejercerse de una manera adecuada, pertinente y no excesiva en relación con el objeto de la injerencia.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1
Objeto y ámbito

1. La presente Directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

2. La presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2
Definiciones

1. A efectos de la presente Directiva, se aplicarán las definiciones de la Directiva 95/46/CE, de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco)[1252], y de la Directiva 2002/58/CE.

[1252] DO L 108 de 24.4.2002, p. 33.

2. A efectos de la presente Directiva, se entenderá por:

a) "datos": los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario;

b) "usuario": toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público, con fines privados o comerciales, sin haberse necesariamente abonado a dicho servicio;

c) "servicio telefónico": las llamadas (incluida la transmisión de voz, buzones vocales, conferencias y datos), los servicios suplementarios (incluido el reenvío o transferencia de llamadas) y los servicios de mensajería y servicios multimedia (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia);

d) "identificador de usuario": un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a internet o a un servicio de comunicaciones por internet, o de su registro en uno de dichos servicios;

e) "identificador de celda": la identidad de la celda desde la que se origina o termina una llamada de teléfono móvil;

f) "llamada telefónica infructuosa": una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación o en la que ha habido una intervención por parte del gestor de la red.

Artículo 3
Obligación de conservar datos

1. Como excepción a los artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.

2. La obligación de conservar datos mencionada en el apartado 1 incluirá la conservación de los datos especificados en el artículo 5 en relación con las llamadas telefónicas infructuosas en las que los datos los generan o tratan, y conservan (en lo que a los datos telefónicos se refiere) o registran (en lo que a los datos de internet se refiere), proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo la jurisdicción del Estado miembro de que se trate en el marco de la prestación de los servicios de comunicaciones en cuestión. La conservación de datos en relación con las llamadas no conectadas no será obligatoria con arreglo a la presente Directiva.

Artículo 4
Acceso a los datos

Los Estados miembros adoptarán medidas para garantizar que los datos conservados de conformidad con la presente Directiva solamente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional. Cada Estado miembro definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del Derecho de la Unión o del Derecho internacional público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos.

Artículo 5
Categorías de datos que deben conservarse

1. Los Estados miembros garantizarán que las siguientes categorías de datos se conserven de conformidad con la presente Directiva:

a) datos necesarios para rastrear e identificar el origen de una comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil:

i) el número de teléfono de llamada,

ii) el nombre y la dirección del abonado o usuario registrado;

2) con respecto al acceso a internet, correo electrónico por internet y telefonía por internet:

i) la identificación de usuario asignada,

ii) la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía,

iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo internet (IP), una identificación de usuario o un número de teléfono;

b) datos necesarios para identificar el destino de una comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil:

i) el número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas,

ii) los nombres y las direcciones de los abonados o usuarios registrados;

2) con respecto al correo electrónico por internet y a la telefonía por internet:

i) la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por internet,

ii) los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación;

c) datos necesarios para identificar la fecha, hora y duración de una comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la comunicación,

2) con respecto al acceso a internet, correo electrónico por internet y telefonía por internet:

i) la fecha y hora de la conexión y desconexión del servicio de acceso a internet, basadas en un determinado huso horario, así como la dirección del Protocolo internet, ya sea dinámica o estática, asignada por el proveedor de acceso a internet a una comunicación, así como la identificación de usuario del abonado o del usuario registrado,

ii) la fecha y hora de la conexión y desconexión del servicio de correo electrónico por internet o del servicio de telefonía por internet, basadas en un determinado huso horario;

d) datos necesarios para identificar el tipo de comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado,

2) con respecto al correo electrónico por internet y a la telefonía por internet: el servicio de internet utilizado;

e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1) con respecto a la telefonía de red fija: los números de teléfono de origen y destino,

2) con respecto a la telefonía móvil:

i) los números de teléfono de origen y destino,

ii) la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada,

iii) la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada,

iv) la IMSI de la parte que recibe la llamada,

v) la IMEI de la parte que recibe la llamada,

vi) en el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio;

3) con respecto al acceso a internet, correo electrónico por internet y telefonía por internet:

i) el número de teléfono de origen en caso de acceso mediante marcado de números,

ii) la línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación;

f) datos necesarios para identificar la localización del equipo de comunicación móvil:

1) la etiqueta de localización (identificador de celda) al comienzo de la comunicación,

2) los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación.

Artículo 6
Períodos de conservación

Los Estados miembros garantizarán que las categorías de datos mencionadas en el artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación.

Artículo 7
Protección y seguridad de los datos

Sin perjuicio de lo dispuesto en las disposiciones adoptadas de conformidad con las Directivas 95/46/CE y 2002/58/CE, los Estados miembros velarán por que los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones cumplan, en lo que respecta a los datos conservados de conformidad con la presente Directiva, como mínimo los siguientes principios de seguridad de los datos:

a) los datos conservados serán de la misma calidad y estarán sometidos a las mismas normas de seguridad y protección que los datos existentes en la red;

b) los datos estarán sujetos a las medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos;

c) los datos estarán sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas,

y

d) los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación.

Artículo 8
Requisitos de almacenamiento para los datos conservados

Los Estados miembros garantizarán que los datos especificados en el artículo 5 se conservan de conformidad con la presente Directiva de manera que los datos conservados y cualquier otra información necesaria con ellos relacionada puedan transmitirse sin demora cuando las autoridades competentes así lo soliciten.

Artículo 9
Autoridades de control

1. Cada Estado miembro nombrará una o más autoridades públicas responsables de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros de conformidad con el artículo 7 en relación con la seguridad de los datos conservados. Dichas autoridades podrán ser las mencionadas en el artículo 28 de la Directiva 95/46/CE.

2. Las autoridades mencionadas en el apartado 1 actuarán con plena independencia en el ejercicio del control a que se refiere el apartado 1.

Artículo 10
Estadísticas

1. Los Estados miembros velarán por que se faciliten anualmente a la Comisión las estadísticas sobre la conservación de datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones. Tales estadísticas incluirán:

- los casos en que se haya facilitado información a las autoridades competentes de conformidad con el Derecho nacional aplicable,

- el tiempo transcurrido entre la fecha en que se conservaron los datos y la fecha en que la autoridad competente solicitó su transmisión,

- los casos en que no pudieron satisfacerse las solicitudes de datos.

2. Tales estadísticas no contendrán datos personales.

Artículo 11
Modificación de la Directiva 2002/58/CE

En el artículo 15 de la Directiva 2002/58/CE se inserta el apartado siguiente:

"1 bis. El apartado 1 no se aplicará a los datos que deben conservarse específicamente de conformidad con la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de

15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[1253], para los fines recogidos en el artículo 1, apartado 1, de dicha Directiva.

Artículo 12
Medidas futuras

1. Todo Estado miembro que deba hacer frente a circunstancias especiales que justifiquen una ampliación limitada del período máximo de conservación recogido en el artículo 6 podrá adoptar las medidas que se impongan. El Estado miembro en cuestión informará inmediatamente a la Comisión y a los demás Estados miembros sobre las medidas adoptadas de conformidad con el presente artículo e indicará las razones que le llevan a adoptarlas.

2. En un plazo de seis meses tras la notificación mencionada en el apartado 1, la Comisión aprobará o rechazará las medidas nacionales en cuestión después de haber examinado si constituyen una discriminación arbitraria o una restricción encubierta al comercio entre los Estados miembros o constituyen un obstáculo para el funcionamiento del mercado interior. En caso de que la Comisión no adopte ninguna decisión en dicho plazo se considerará que las medidas nacionales han sido aprobadas.

3. Cuando, en virtud del apartado 2, las medidas nacionales adoptadas por un Estado miembro se aparten de las disposiciones de la presente Directiva, la Comisión examinará la oportunidad de proponer la modificación de la presente Directiva.

Artículo 13
Recursos judiciales, responsabilidad y sanciones

1. Cada Estado miembro adoptará las medidas que se impongan para velar por que se apliquen plenamente, en lo que se refiere al tratamiento de datos en el marco de la

[1253] DO L 105 de 13.4.2006, p. 54

presente Directiva, las medidas nacionales de aplicación del capítulo III de la Directiva 95/46/CE relativas al establecimiento de recursos judiciales, responsabilidad y sanciones.

2. Cada Estado miembro adoptará, en particular, las medidas que se impongan para velar por que cualquier acceso intencionado o la transferencia de datos conservados de conformidad con la presente Directiva que no estén permitidos por la legislación nacional adoptada de conformidad con la presente Directiva se castiguen con sanciones, incluidas sanciones administrativas o penales, que sean eficaces, proporcionadas y disuasorias.

Artículo 14
Evaluación

1. A más tardar el 15 de septiembre de 2010, la Comisión presentará al Parlamento Europeo y al Consejo una evaluación de la aplicación de la presente Directiva y su impacto en operadores económicos y consumidores, teniendo en cuenta los avances en la tecnología de las comunicaciones electrónicas y las estadísticas proporcionadas a la Comisión de conformidad con el artículo 10 a fin de determinar si es necesario modificar las disposiciones de la presente Directiva, en particular por lo que se refiere a la lista de datos del artículo 5 y a los períodos de conservación establecidos en el artículo 6. Los resultados de esta evaluación se harán públicos.

2. Con este fin, la Comisión examinará todas las observaciones que le comuniquen los Estados miembros o el GT29 de protección de las personas en lo que respecta al tratamiento de datos personales creado por el artículo 29 de la Directiva 95/46/CE.

Artículo 15
Transposición

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar el 15 de septiembre de 2007. Informarán de ello inmediatamente a la Comisión. Cuando los Estados miembros adopten dichas disposiciones, éstas harán

referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

3. Cada Estado miembro podrá aplazar hasta el 15 de marzo de 2009 la aplicación de la presente Directiva en lo que se refiere a la conservación de los datos de comunicaciones en relación con el acceso a internet, la telefonía por internet y el correo electrónico por internet. Los Estados miembros que se propongan recurrir al presente apartado lo notificarán al Consejo y a la Comisión, mediante una declaración, en el momento de la adopción de la presente Directiva. Tal declaración se publicará en el Diario Oficial de la Unión Europea.

Artículo 16
Entrada en vigor

La presente Directiva entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.

Artículo 17
Destinatarios

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en Estrasburgo, el 15 de marzo de 2006.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
J. Borrell Fontelles	H. Winkler

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

Reproducimos a continuación el texto íntegro de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, tal como fue publicado en el Boletín Oficial del Estado, núm. 251, viernes 19 de octubre de 2007, páginas 42517 a 42523.

JUAN CARLOS I
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos. A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentre al alcance de cualquier persona y en cualquier rincón del mundo.

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones

electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

En relación con esta última precisión, cabe señalar que la Directiva se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por delitos graves, definidos éstos de acuerdo con la legislación interna de cada Estado miembro.

II

La Ley cuenta con diez artículos que se agrupan en tres capítulos.

El Capítulo I («Disposiciones Generales») se inicia describiendo su objeto, que básicamente se circunscribe a la determinación de la obligación de conservar los datos enumerados en el artículo 3, que se hayan generado o tratado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones. Igualmente, se precisan los fines que, exclusivamente, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece.

En este capítulo también se precisan las limitaciones sobre el tipo de datos a retener, que son los necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos, pero nunca datos que revelen el contenido de la comunicación. Igualmente, la Ley impone la obligación de conservación de datos que permitan determinar el momento y duración de una determinada comunicación, su tipo, así como datos necesarios para identificar el equipo de comunicación empleado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización.

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o internet. Estos datos, que, se repite, en ningún caso revelarán el

contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

En las disposiciones contenidas en la parte final se incluyen contenidos diversos. Por un lado, y a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de

prepago, se establece, como obligación de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Por último, la Ley incorpora en las disposiciones finales una modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para adaptarla al contenido de esta Ley, una referencia a su amparo competencial, una habilitación general al Gobierno para su desarrollo y un período de seis meses para que las operadoras puedan adaptarse a su contenido.

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto de la Ley.

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. Sujetos obligados.

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas

disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. Datos objeto de conservación.

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.

ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a internet, correo electrónico por internet y telefonía por internet:

i) La identificación de usuario asignada.

ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.

iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.

ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por internet y la telefonía por internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por internet.

ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.

2.° Con respecto al acceso a internet, al correo electrónico por internet y a la telefonía por internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo internet, ya sea dinámica o estática, asignada por el proveedor de acceso a internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.

ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por internet o del servicio de telefonía por internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).

2.° Con respecto al correo electrónico por internet y a la telefonía por internet: el servicio de internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.

2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.

ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.

iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a internet, correo electrónico por internet y telefonía por internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. Obligación de conservar datos.

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. Período de conservación de los datos.

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

Artículo 6. Normas generales sobre cesión de datos.

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.

2. La cesión de la información se efectuará únicamente a los agentes facultados.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica

2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. Procedimiento de cesión de datos.

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. Protección y seguridad de los datos.

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. Excepciones a los derechos de acceso y cancelación.

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. Régimen aplicable al incumplimiento de obligaciones contempladas en esta Ley.

El incumplimiento de las obligaciones previstas en esta Ley se sancionará de acuerdo con lo dispuesto en la Ley 32/2003, de 3 de noviembre, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

Disposición adicional única. Servicios de telefonía mediante tarjetas de prepago.

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.

La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

5. Sin perjuicio del régimen sancionador establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, constituyen infracciones a lo previsto en la presente disposición las siguientes:

a) Son infracciones muy graves tanto el incumplimiento de la llevanza del libro-registro referido, como la negativa a la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

b) Son infracciones graves la llevanza incompleta de dicho libro-registro, así como la demora injustificada, en más de setenta y dos horas, en la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

6. A las infracciones previstas en el apartado anterior les será de aplicación el régimen sancionador establecido en la Ley 32/2003, de 3 de noviembre, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

7. La obligación de inscripción en el libro-registro de los datos identificativos de los compradores que adquieran tarjetas inteligentes, así como el resto de obligaciones contenidas en la presente disposición adicional, comenzarán a ser exigibles a partir de la entrada en vigor de esta Ley.

8. No obstante, por lo que se refiere a las tarjetas adquiridas con anterioridad a la entrada en vigor de esta Ley, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las obligaciones de inscripción a que se refiere el apartado 1 de la presente disposición adicional.

Transcurrido el aludido plazo de dos años, los operadores vendrán obligados a anular o a desactivar aquellas tarjetas de prepago respecto de las que no se haya podido cumplir con las obligaciones de inscripción del referido apartado 1 de esta disposición adicional, sin perjuicio de la compensación que, en su caso, corresponda al titular de las mismas por el saldo pendiente de consumo.

Disposición transitoria única. Vigencia del régimen de interceptación de telecomunicaciones.

Las normas dictadas en desarrollo del Capítulo III del Título III de la Ley 32/2003, de 3 de noviembre, continuarán en vigor en tanto no se opongan a lo dispuesto en esta Ley.

Disposición derogatoria única. Derogación normativa.

1. Quedan derogados los artículos 12, 38.2 c) y d) y 38.3 a) de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

Disposición final primera. Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. Secreto de las comunicaciones.

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en

la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante

un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

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

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios internet.

f) Dirección de correo electrónico.

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

8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o

cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

Dos. El último párrafo del apartado 5 del artículo 38 pasa a tener la siguiente redacción:

«Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

Tres. En el artículo 53, se modifican los párrafos o) y z), que quedan redactados de la siguiente forma:

«o) El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de esta Ley y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

«z) La vulneración grave o reiterada de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.»

Cuatro. En el artículo 54 se modifican los párrafos ñ) y r), que quedan redactados de la siguiente forma:

«ñ) El incumplimiento, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de la presente Ley y el incumplimiento de las obligaciones de conservación de los datos

establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, salvo que deban considerarse como infracción muy grave, conforme a lo dispuesto en el artículo anterior.»

«r) La vulneración de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, y el incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, salvo que deban considerarse como infracción muy grave.»

Disposición final segunda. Competencia estatal.

Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21.ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones.

Disposición final tercera. Desarrollo reglamentario.

Se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley.

Disposición final cuarta. Formato de entrega de los datos.

1. La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley.

2. Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos.

Disposición final quinta. Entrada en vigor.

Esta Ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

Por tanto,

Mando a todos los españoles, particulares y autoridades que guarden y hagan guardar esta ley.

Madrid, 18 de octubre de 2007.

JUAN CARLOS R.

El Presidente del Gobierno,

JOSÉ LUIS RODRÍGUEZ ZAPATERO