CONSEJO DE LA UNIÓN EUROPEA

Bruselas, 19 de abril de 2011 (02.05)
(OR. en)

9324/11

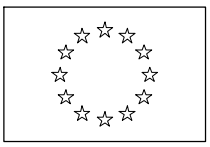
DAPIX 38
TELECOM 47
COPEN 85

NOTA DE TRANSMISIÓN

Emisor:	Por el Secretario General de la Comisión Europea, Sr. D. Jordi AYET PUIGARNAU, Director
Fecha de recepción:	18 de abril de 2011
Destinatario:	Sr. D. Pierre de BOISSIEU, Secretario General del Consejo de la Unión Europea
N.° doc. Ción:	COM(2011) 225 final
Asunto:	Informe de la Comisión al Consejo y al Parlamento Europeo - Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE)

Adjunto se remite a las Delegaciones el documento de la Comisión – COM(2011) 225 final.

Adj.: COM(2011) 225 final



COMISIÓN EUROPEA

Bruselas, 18.4.2011
COM(2011) 225 final

INFORME DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE)

INFORME DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE)

1. INTRODUCCIÓN

La Directiva de conservación de datos[1] (en lo sucesivo, «la Directiva») exige que los Estados miembros obliguen a los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones (en lo sucesivo, «operadores») a conservar los datos de tráfico y de localización entre seis meses y dos años con fines de investigación, detección y enjuiciamiento de delitos graves.

El presente informe de la Comisión evalúa, de conformidad con el artículo 14 de la Directiva, su aplicación 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, 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. Este informe también examina la incidencia de la Directiva en los derechos fundamentales, teniendo en cuenta las críticas que se han dirigido en general a la conservación de datos, y examina si se requieren medidas que aborden los aspectos ligados a la utilización de tarjetas SIM anónimas con fines delictivos[2].

En general, la evaluación ha demostrado que la conservación de datos es una herramienta valiosa para los sistemas de justicia penal en la UE y para la aplicación de la legislación. La contribución de la Directiva a la armonización de la conservación de datos ha sido escasa en términos, por ejemplo, de limitación de la finalidad y de períodos de conservación, y también en el ámbito del reembolso de los costes contraídos por los operadores, que no se incluyen en su ámbito de aplicación. Dadas las implicaciones y riesgos para el mercado interior y para el respeto del derecho a la intimidad y la protección de los datos personales, la UE debería 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. A la luz de estas conclusiones, la Comisión tiene la intención de proponer modificaciones a la Directiva, sobre la base de una evaluación de impacto.

---

1 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, pp. 54-63.

2 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 - Bruselas, 27-28 de noviembre de 2008.

2. CONTEXTO DE LA PRESENTE EVALUACIÓN

El presente informe de evaluación se nutre de amplios debates con los Estados miembros, expertos y partes interesadas y de contribuciones de todos ellos.

En mayo de 2009, la Comisión organizó una conferencia titulada «Evaluación de la Directiva de conservación de datos», a la que asistieron autoridades de protección de datos, el sector privado, la sociedad civil y los medios académicos. En septiembre de 2009, la Comisión envió un cuestionario a partes interesadas de estos grupos y recibió unas 70 respuestas[3]. La Comisión acogió una segunda conferencia en diciembre de 2010, denominada «Aplicación de la Directiva de conservación de datos», en la que participaron el mismo tipo de interesados, que compartieron las evaluaciones preliminares de la Directiva y debatieron los futuros retos.

La Comisión se reunió con representantes de cada Estado miembro y de países asociados del Espacio Económico Europeo entre octubre de 2009 y marzo de 2010, para debatir con más detalle cuestiones relativas a la aplicación de la Directiva. Los Estados miembros empezaron a aplicar la Directiva más tarde de lo previsto, especialmente en lo que se refiere a los datos relacionados con Internet. Los retrasos en la transposición supusieron que nueve Estados miembros pudieron, para 2008 o 2009, proporcionar a la Comisión todas las estadísticas requeridas por el artículo 10 de la Directiva, aunque 19 Estados miembros aportaron algunas estadísticas (véase el apartado 4.7). La Comisión se dirigió por escrito a los Estados miembros en julio de 2010 solicitando más información cuantitativa y cualitativa relativa a la necesidad de los datos conservados a efectos de obtener resultados en cuanto a la aplicación de las normas. Diez Estados miembros respondieron con detalles de casos concretos para los que resultó necesario contar con esos datos[4].

El presente informe se basa en los documentos adoptados, desde su creación en 2008, por la «Plataforma para la conservación de datos electrónicos con fines de investigación, detección y enjuiciamiento de los delitos graves»[5]. La Comisión ha tenido en cuenta los informes del Grupo de Trabajo del Artículo 29 sobre protección de datos[6] y, en particular, el informe sobre la segunda acción, es decir, su evaluación del cumplimiento por parte de los Estados miembros de los requisitos de la Directiva sobre protección y seguridad de los datos[7].

---

3 Las respuestas se han publicado en el sitio web de la Comisión (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm)

4 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.

5 Este grupo de expertos 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

6 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 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).

7 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

3. CONSERVACIÓN DE DATOS EN LA UNIÓN EUROPEA

3.1. Conservación de datos en el ámbito de la justicia penal y con fines policiales

Los proveedores de redes y servicios (en lo sucesivo, «operadores»), en el curso de sus actividades, tratan datos personales con el fin de transmitir una comunicación, facturación, pagos de conexión, comercialización y otros servicios de valor añadido. Dicho tratamiento implica datos que indican el origen, destino, fecha, hora, duración y tipo de una comunicación, así como el equipo de comunicación de los usuarios y, en el caso de la telefonía móvil, datos de la ubicación del equipo. En virtud de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (en lo sucesivo, «la Directiva sobre privacidad»)[8], tales datos de tráfico generados por el uso de servicios de comunicaciones electrónicas en principio deben borrarse o hacerse anónimos cuando esos datos ya no son necesarios para la transmisión de una comunicación, excepto cuando, y sólo en tanto, sean necesarios a efectos de facturación, o cuando el abonado o usuario haya dado su consentimiento. Los datos de localización sólo pueden tratarse si se hacen anónimos o con el consentimiento del usuario en cuestión, en la medida y durante el tiempo necesario para la prestación de un servicio de valor añadido.

Antes de la entrada en vigor de la Directiva, con sujeción a condiciones específicas, las autoridades nacionales solicitaban a los operadores el acceso a dichos datos, con el fin, por ejemplo, de identificar a los abonados que utilizan una dirección IP, analizar actividades de comunicación e identificar el emplazamiento de un teléfono móvil.

A nivel de la UE, la conservación y uso de los datos para fines policiales se abordó inicialmente en la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Esta Directiva proporcionó en primer lugar a los Estados miembros la posibilidad de adoptar tales medidas legislativas cuando fuera necesario para la protección de la seguridad pública, la defensa o el orden público, incluyendo el bienestar económico del Estado cuando las actividades trataban cuestiones de seguridad del Estado y a efectos de aplicación del Derecho penal.[9]

Esta disposición se desarrolló posteriormente en la Directiva sobre privacidad, que prevé la posibilidad de que los Estados miembros adopten medidas legales que constituyen una excepción al principio de confidencialidad de las comunicaciones, incluyendo bajo ciertas

---

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 (véase http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

[8] 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) (DO L 201 de 31.7.2002, pp. 37-47).

[9] Artículo 14, apartado 1, de 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 (DO L 24 de 30.1.1998, pp. 1-8).

condiciones la conservación, el acceso y la utilización de datos para fines policiales. El artículo 15, apartado 1, permite a los Estados miembros limitar los derechos y obligaciones de la intimidad, incluso mediante la conservación de datos por un período de tiempo limitado, 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, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas».

La función de los datos conservados en los sistemas de justicia penal y con fines policiales se analiza más pormenorizadamente en la sección 5.

3.2. Finalidad y base jurídica de la Directiva de conservación de datos

Como consecuencia de las disposiciones de la Directiva 97/66/CE y la Directiva sobre privacidad, que autorizan a los Estados miembros a adoptar legislación relativa a la conservación de datos, los operadores de algunos Estados miembros se vieron 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 interior. Además, las tendencias de los modelos empresariales y las ofertas de servicios, tales como la proliferación de tarifas planas, servicios de comunicaciones electrónicas de prepago o gratuitos, tuvieron como efecto que los operadores dejaron 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 ley. Los atentados terroristas de Madrid en 2004 y de Londres en 2005 añadieron urgencia a los debates a nivel de la UE sobre la forma de abordar estas cuestiones.

En este contexto, la Directiva de conservación de datos impuso a los Estados miembros la obligación de que los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones conservasen los datos de comunicaciones a efectos de la investigación, detección y enjuiciamiento de delitos graves, según lo definido por cada Estado miembro en la legislación nacional, y pretendió armonizar en la UE determinadas cuestiones conexas.

La Directiva modificó el artículo 15, apartado 1, de la Directiva sobre privacidad, añadiendo un párrafo que dispone que el artículo 15, apartado 1, no se aplicará a los datos conservados de conformidad con la Directiva de conservación de datos[10]. Por tanto, los Estados miembros (tal como se recoge en el considerando 12 de la Directiva) siguen teniendo la posibilidad de establecer excepciones al principio de confidencialidad de las comunicaciones. La Directiva (de conservación de datos) regula únicamente la conservación de datos para el fin más limitado de la investigación, detección y enjuiciamiento de delitos graves.

---

[10] El artículo 11 de la Directiva dispone: «En el artículo 15 de la Directiva 2002/58/CE se inserta el apartado siguiente: 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».

Esta compleja relación jurídica entre la Directiva y la Directiva sobre privacidad en las comunicaciones electrónicas, combinada con la ausencia de una definición en cualquiera de las dos Directivas de la noción de «delito grave», hace 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 artículo 15, apartado 1, de la Directiva sobre privacidad en las comunicaciones electrónicas[11]. Este aspecto se examina con mayor detalle en la sección 4.

Esta Directiva se basa en el artículo 95 del Tratado constitutivo de la Comunidad Europea (sustituido por el artículo 114 del Tratado de Funcionamiento de la Unión Europea) relativo al establecimiento y el funcionamiento del mercado interior. Tras la adopción de la Directiva, su base jurídica fue recurrida ante el Tribunal de Justicia Europeo, partiendo de la premisa de que el principal objetivo era la investigación, la detección y el enjuiciamiento de los delitos graves. El Tribunal sostuvo que la Directiva regula operaciones que son independientes de la ejecución de cualquier cooperación policial y judicial en materia penal y que no 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. Por tanto, concluyó que la Directiva se dirige esencialmente a las actividades de los operadores en el sector pertinente del mercado interior, y confirmó la base jurídica.[12]

3.3. Preservación de datos

La preservación de datos es distinta de la conservación de datos (también llamada «congelación rápida»), en virtud de la cual 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[13]. Casi todos los Estados participantes han establecido un punto de contacto, cuya función es garantizar la prestación de asistencia inmediata en investigaciones o procedimientos de ciberdelincuencia. Sin embargo, al parecer, no todas las 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[14]. 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 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,

---

11 El Grupo de Trabajo del Artículo 29 plantea si la Directiva [sobre conservación de datos] tenía como objetivo establecer una excepción a la obligación general de suprimir los datos de tráfico una vez concluida la comunicación electrónica o bien establecer la obligación de conservación para todos los proveedores de datos que ya estaban facultados para almacenarlos para sus propios fines profesionales.

12 TJCE, C-301/6 Irlanda contra Parlamento y Consejo, Rec. 2009, p. I-00593.

13 Artículo 16 del Convenio sobre la Ciberdelincuencia (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

14 Fuente: Consejo de Europa.

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 permite obtener pruebas sobre los movimientos de, por ejemplo, las víctimas o testigos de un delito[15].

4. TRANSPOSICIÓN DE LA DIRECTIVA DE CONSERVACIÓN DE DATOS

Los Estados miembros estaban obligados a transponer la Directiva antes del 15 de septiembre de 2007, con la posibilidad de aplazar hasta el 15 de marzo de 2009 la aplicación de las obligaciones de conservación relativas al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet.

El análisis que sigue se basa en las notificaciones de transposición recibidas por la Comisión procedentes de 25 Estados miembros, incluida Bélgica, que sólo ha transpuesto parcialmente la Directiva[16]. En Austria y Suecia el proyecto legislativo está en fase de debate. En esos dos Estados miembros 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. Tras la notificación inicial de transposición de la República Checa, Alemania y Rumanía, sus respectivos tribunales constitucionales anularon la legislación nacional de transposición de la Directiva y actualmente están estudiando cómo volver a transponerla[17].

---

15 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 (véase el apartado 4.9) (Bundesverfassungsgericht, 1 BvR 256/08, de 2 de marzo de 2010, apartado 208).

16 Los veinticinco Estados miembros que han notificado a la Comisión la transposición de la Directiva son Bélgica, Bulgaria, República Checa, Dinamarca, Alemania, Grecia, Estonia, Irlanda, España, Francia, Italia, Chipre, Letonia, Lituania, Luxemburgo, Hungría, Malta, Países Bajos, Polonia, Portugal, Rumanía, Eslovenia, Eslovaquia, Finlandia y Reino Unido. Bélgica informó a la Comisión de que la propuesta de legislación que completa la transposición está todavía en el Parlamento.

17 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.

En esta sección se analiza cómo los Estados miembros han incorporado las disposiciones pertinentes de la Directiva. También se examina si los Estados miembros han optado por reembolsar a los operadores los costes de conservar y permitir la obtención de datos, lo que no se contempla en la Directiva, y aborda la pertinencia para la Directiva de las sentencias de los tribunales constitucionales de Alemania, Rumanía y la República Checa.

4.1. Finalidad de la conservación de datos (artículo 1)

La Directiva obliga a los Estados miembros a adoptar medidas para garantizar que los datos sean conservados y se hallen disponibles para los fines de investigación, detección y enjuiciamiento de delitos graves, según lo definido por cada Estado miembro en su Derecho nacional. Sin embargo, los fines declarados para la conservación o acceso a los datos en la legislación nacional siguen variando en la UE. 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. 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. Los detalles figuran en el cuadro 1.

Cuadro 1: Limitación de finalidades de la conservación de datos recogidas en las legislaciones nacionales

Bélgica	Investigación y enjuiciamiento de delitos, enjuiciamiento del uso indebido del número de teléfono de los servicios de emergencia, investigación del abuso malicioso de redes o servicios de comunicaciones electrónicas, misiones de recogida de información de los servicios de inteligencia y seguridad[18].
Bulgaria	Descubrimiento e investigación de delitos graves y delitos en virtud del artículo 319a-319f del Código penal, así como búsqueda de personas[19].
República Checa	No transpuesta
Dinamarca	Investigación y enjuiciamiento de delitos[20].
Alemania	No transpuesta
Estonia	Podrán utilizarse si la recogida de pruebas por otros actos procedimentales se excluye o resulta especialmente complicada y el objeto de un procedimiento penal es un delito [en primer grado o un delito cometido intencionadamente en segundo grado con una pena de privación de libertad mínima de tres años][21].

18 Artículo 126, apartado 1, de la Ley de 13 de junio de 2005 relativa a las comunicaciones electrónicas.
19 Artículo 250 *bis*, apartado 2, de la Ley sobre Comunicaciones Electrónicas (modificada) de 2010.
20 Artículo 1, Orden de conservación de datos.
21 Artículo 110, apartado 1, del Código de enjuiciamiento penal.

Cuadro 1: Limitación de finalidades de la conservación de datos recogidas en las legislaciones nacionales	
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[22].
Grecia	Detección de delitos especialmente graves[23].
España	Detección, investigación y enjuiciamiento de los delitos graves contemplados en el Código Penal o en las leyes penales especiales[24].
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[25].
Italia	Detección y represión de delitos[26].
Chipre	Investigación de delitos graves[27].
Letonia	Protección de la seguridad pública y del Estado, investigación de delitos, enjuiciamiento penal y procedimientos penales[28].
Lituania	Investigación, detección y enjuiciamiento de delitos graves y muy graves, según lo definido en el Código Penal lituano[29].
Luxemburgo	Detección, investigación y enjuiciamiento de delitos que lleven aparejada una condena penal máxima de un año o más[30].
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[31].
Malta	Investigación, detección o enjuiciamiento de delitos graves[32].
Países Bajos	Investigación y enjuiciamiento de delitos graves para los que puedan imponerse penas privativas de libertad[33].
Austria	No transpuesta

22 Artículo 6 Comunicaciones (Ley de Conservación de Datos) de 2011.

23 Tales delitos se definen en el artículo 4 de la Ley 2225/1994; artículo 1 de la Ley 3917/2011.

24 Artículo 1, apartado 1, de la Ley 25/2007.

25 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.

26 Artículo 132, apartado 1, del Código de protección de datos.

27 Artículo 4, apartado 1, de la Ley 183 (I)/2007.

28 Artículo 71, apartado 1, de la Ley de comunicaciones electrónicas.

29 Artículo 65 de la Ley X-1835.

30 Artículo 1, apartado 1, de la Ley de 24 de julio de 2010.

31 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.

32 Artículo 20, apartado 1, Anuncio oficial 198/2008.

33 Artículo 126 del Código de enjuiciamiento penal.

Cuadro 1: Limitación de finalidades de la conservación de datos recogidas en las legislaciones nacionales	
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[34].
Portugal	Investigación, detección y enjuiciamiento de delitos graves[35].
Rumanía	No transpuesta
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[36].
Eslovaquia	Prevención, investigación, detección y enjuiciamiento de delitos[37].
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[38].
Suecia	No transpuesta
Reino Unido	Investigación, detección y enjuiciamiento de delitos graves[39].

La mayoría de los Estados miembros que han transpuesto la Directiva, de conformidad con su legislación, permiten el acceso y uso de los datos conservados con fines que van más allá de los cubiertos por la Directiva, incluida la prevención y la lucha contra la delincuencia en general y el riesgo para la vida y la integridad física. Si bien esto está permitido por la Directiva sobre privacidad, el grado de armonización alcanzado por la legislación de la UE en este campo sigue siendo limitado. Las diferencias entre las finalidades de la conservación de datos afectarán probablemente al volumen y la frecuencia de las solicitudes y a su vez a los costes generados por el cumplimiento de las obligaciones establecidas en la Directiva. Además, esta situación podría no ofrecer la previsibilidad suficiente, que constituye un requisito para cualquier medida legislativa que restrinja el derecho a la intimidad[40]. La

34 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.

35 Artículo 1, 3 (1), de la Ley 32/2008.

36 Artículo 170 *bis*, apartado 1, de la Ley de comunicaciones electrónicas.

37 Artículo 59 *bis*, apartado 6, de la Ley de comunicaciones electrónicas.

38 Artículo 14 *bis*, apartado 1, de la Ley de comunicaciones electrónicas.

39 Reglamento sobre la conservación de datos (Directiva CE) de 2009 (2009 nº 859).

40 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 (Protección de las personas físicas en lo que respecta al tratamiento de datos personales - Directiva 95/46/CE - Protección de la intimidad - Divulgación de datos sobre los ingresos de empleados de entidades sujetas al control del Rechnungshof).

Comisión evaluará la necesidad y las opciones para lograr un mayor grado de armonización en este ámbito[41].

4.2. Operadores que deben cumplir la obligación de conservación de datos (artículo 1)

La Directiva se aplica a los «proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones» (artículo 1, apartado 1). Dos Estados miembros (Finlandia y Reino Unido) no exigen a los pequeños operadores que conserven datos, ya que, según alegan, los costes tanto para el proveedor como para el Estado superarían las ventajas que se obtendrían para los sistemas de justicia penal y policial. Cuatro Estados miembros (Letonia, Luxemburgo, Países Bajos y Polonia) informan que han establecido disposiciones administrativas alternativas. 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 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. La Comisión examinará 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.

4.3. Acceso a los datos: autoridades, procedimientos y condiciones (artículo 4)

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». Corresponde a los Estados miembros definir en su Derecho 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».

En todos los Estados miembros, la policía y, salvo en las jurisdicciones de Derecho Común (Irlanda y Reino Unido), los fiscales, pueden acceder a los datos conservados. Catorce Estados miembros incluyen a los servicios de seguridad o de inteligencia o militares entre las autoridades competentes. Seis Estados miembros incluyen a las autoridades fiscales o aduaneras, y tres a 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

[41] Por lo que respecta a la adopción de la Directiva, la Comisión realizó una declaración sugiriendo que se considerara la lista de delitos en la orden de detención europea (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).

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.

Cuadro 2: Acceso a los datos conservados sobre telecomunicaciones		
	Autoridades nacionales competentes	*Procedimientos y condiciones*
Bélgica	Unidad de coordinación judicial, jueces de instrucción, fiscal o policía criminal.	El acceso deberá ser autorizado por un juez o un fiscal. Previa petición, los operadores deberán 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 deberán proporcionarse lo antes posible.
Bulgaria[42]	Direcciones y departamentos específicos de la Agencia Estatal de Seguridad Nacional, Ministerio del Interior, Servicio de Información Militar, Policía Militar, Ministerio de Defensa, Agencia Nacional de Investigación; autoridades judiciales y autoridades responsables de las actuaciones prejudiciales, con ciertas condiciones.	Acceso posible únicamente por orden del presidente de un tribunal regional.
República Checa	No transpuesta	
Dinamarca[43]	Policía.	El acceso exige una autorización judicial; el tribunal podrá autorizarlo si la solicitud cumple criterios estrictos en materia de sospecha, necesidad y proporcionalidad.
Alemania	No transpuesta	
Estonia[44]	Policía y Policía de Fronteras, Dirección de la Policía de Seguridad y, para los objetos y las comunicaciones electrónicas, la Dirección de Impuestos y Aduanas.	El acceso requiere la autorización de un juez de instrucción. Los operadores deben «presentar [los datos conservados] en casos urgentes, a más tardar en 10 horas y en otros casos en el plazo de diez días laborables [a partir de la fecha de recepción de la solicitud].»
Irlanda[45]	Miembros de la *Garda Síochána* (policía) con categoría de *Chief Superintendant* o superior; agentes de las Fuerzas de Defensa Permanentes de categoría equivalente o superior a coronel; funcionarios de la Administración Fiscal de categoría equivalente o superior a responsable principal.	Las solicitudes deben presentarse por escrito.
Grecia[46]	Autoridades judiciales, militares o policiales.	El acceso requiere una decisión judicial que

42 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).

43 Capítulo 71 de la Ley de administración de justicia.

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

45 Artículo 6 de la Ley de comunicaciones (conservación de datos) de 2009.

Cuadro 2: Acceso a los datos conservados sobre telecomunicaciones		
	Autoridades nacionales competentes	*Procedimientos y condiciones*
		declare que la investigación por otros medios es imposible o extremadamente difícil.
España[47]	Fuerzas de policía responsables de la detección, investigación y enjuiciamiento de los delitos graves, Centro Nacional de Inteligencia y el Departamento de Aduanas.	El acceso a estos datos por las autoridades nacionales competentes exige una autorización judicial previa.
Francia[48]	Fiscalía y agentes de policía y gendarmes autorizados.	La policía debe aportar una justificación para cada solicitud de acceso a los datos conservados y deberá 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.
Italia[49]	Fiscalía; policía; abogado defensor del demandado o de la persona investigada.	El acceso exige un «auto motivado» dictado por la Fiscalía.
Chipre[50]	Tribunales, Ministerio Fiscal, policía.	El acceso deberá 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.
Letonia[51]	Funcionarios autorizados de las instituciones encargadas de la investigación prejudicial; personas que realizan funciones de investigación; funcionarios autorizados de los organismos de seguridad nacional; Fiscalía; tribunales.	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 podrán firmar un acuerdo con el operador, por ejemplo, para la codificación de los datos facilitados.
Lituania[52]	Organismos responsables de la investigación prejudicial, fiscal, tribunales (jueces) y funcionarios de inteligencia.	Las autoridades públicas autorizadas deben solicitar los datos conservados por escrito. Para acceder a las investigaciones prejudiciales es necesaria una orden judicial.
Luxemburgo[53]	Autoridades judiciales (jueces de instrucción, fiscales), autoridades de seguridad del Estado, defensa, seguridad pública y prevención, investigación, detección y enjuiciamiento de delitos.	El acceso exige una autorización judicial.

46 Artículos 3 y 4 de la Ley 2225/94.

47 Artículos 6 y 7 de la Ley 25/2007.

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

49 Artículo 132, apartado 3, del Código de protección de datos.

50 Artículo 4, apartado 2, y artículo 4, apartado 4, de la Ley 183 (I)/2007.

51 Artículo 71, apartado 1, de la Ley de comunicaciones electrónicas (autoridades); Reglamento del Consejo de Ministros nº 820 (procedimientos).

52 Artículo 77, apartados 1 y 2, de la Ley X-1835; informe oral a la Comisión.

53 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).

Cuadro 2: Acceso a los datos conservados sobre telecomunicaciones		
	Autoridades nacionales competentes	*Procedimientos y condiciones*
Hungría[54]	Policía, Administración fiscal y aduanera, servicios de seguridad nacional, Ministerio Fiscal y tribunales.	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.
Malta[55]	Fuerzas policiales de Malta; servicio de seguridad.	Las solicitudes deberán presentarse por escrito.
Países Bajos[56]	Funcionarios de policía responsables de investigaciones.	El acceso se otorgará previa orden de un fiscal o del juez instructor.
Austria	No transpuesta	
Polonia[57]	Policía, guardia fronteriza, inspectores fiscales, Agencia de seguridad interior, Agencia de inteligencia exterior, Oficina Central Anticorrupción, servicios de contrainteligencia militar, servicios de inteligencia militar, tribunales y Fiscalía.	Las solicitudes se presentarán por escrito y en el caso de la policía, guardia fronteriza e inspectores fiscales deberán ser autorizadas por el más alto funcionario de la organización.
Portugal[58]	Policía criminal, Guardia Nacional Republicana, Oficina de seguridad pública, Policía criminal militar, Servicio de inmigración y fronteras y Policía marítima.	La transmisión de datos exige una autorización judicial por el motivo de 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.
Rumanía	No transpuesta	
Eslovenia[59]	Policía, agencias de inteligencia y seguridad, organismos de defensa responsables de la inteligencia y la contrainteligencia y misiones de seguridad.	El acceso exige una autorización judicial.
Eslovaquia[60]	Servicios con funciones coercitivas y tribunales.	Las solicitudes deberán presentarse por escrito.
Finlandia[61]	Policía, guardia fronteriza y autoridades aduaneras (para los datos conservados relativos a abonados, tráfico y localización). Centro de Emergencias, servicios de salvamento marítimo y subcentro de salvamento marítimo (para datos de identificación y localización en situaciones de emergencia).	Podrán acceder a los datos del abonado todas las autoridades competentes sin autorización judicial. Otros datos exigen una orden judicial.

54 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.

55 Artículo 20, apartados 1 y 3, del Anuncio oficial 198/2008.

56 Artículo 126ni, Código de enjuiciamiento criminal.

57 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.

58 Artículo 2, apartado 1, artículo 3, apartado 2, y artículo 9 de la Ley 32/2008.

59 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.

60 Artículo 59a, apartado 8, de la Ley de comunicaciones electrónicas.

Cuadro 2: Acceso a los datos conservados sobre telecomunicaciones		
	Autoridades nacionales competentes	*Procedimientos y condiciones*
Suecia	No transpuesta	
Reino Unido[62]	Policía, servicios de inteligencia, autoridades fiscales y aduaneras y otras autoridades públicas designadas en la legislación secundaria.	Acceso permitido previa autorización de una «persona designada» y una 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.

La Comisión evaluará la necesidad y las opciones para lograr un mayor grado de armonización con respecto a las autoridades facultadas y los procedimientos para obtener acceso a los datos conservados. Entre las opciones pueden incluirse listas más claramente definidas de autoridades competentes, supervisión independiente o judicial de las solicitudes de datos y un nivel mínimo de los procedimientos para que los operadores proporcionen acceso a las autoridades competentes.

4.4. Alcance de la conservación de datos y categorías de datos cubiertos (artículo 1, apartado 2, artículo 3, apartado 2 y artículo 5)

La Directiva se aplica a los ámbitos de telefonía de red fija, telefonía móvil, acceso a Internet, correo electrónico por Internet y telefonía por Internet. También especifica (artículo 5) las categorías de datos que deben conservarse, a saber, los necesarios para identificar:

(a) el origen de una comunicación;

(b) el destino de una comunicación;

(c) la fecha, hora y duración de una comunicación;

(d) el tipo de comunicación;

(e) el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; y

(f) la localización del equipo de comunicación móvil.

La Directiva cubre asimismo (artículo 3, apartado 2) las llamadas telefónicas infructuosas, es decir, comunicaciones en las que se ha realizado con éxito una llamada telefónica pero no ha habido contestación o en las que ha habido una intervención por parte del gestor de la red, y

---

61 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.

62 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.

cuando los datos relativos a estas llamadas infructuosas son generados o tratados y conservados o registrados por los operadores. En virtud de la Directiva no pueden conservarse datos que revelen el contenido de la comunicación. 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[63].

Veintiún Estados miembros prevén en su legislación de transposición la conservación de cada una de estas categorías de datos. 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. Quienes respondieron al cuestionario de la Comisión no consideraron necesario modificar las categorías de datos que deben conservarse, aunque el Parlamento Europeo ha enviado a la Comisión una declaración escrita en la que pide que la Directiva se amplíe a los motores de búsqueda «para luchar rápidamente contra la pornografía infantil en línea y los abusos sexuales»[64]. En su informe sobre la segunda medida de ejecución, el Grupo de trabajo del artículo 29 alegó que las categorías establecidas en la Directiva deben considerarse exhaustivas, sin imponer a los operadores obligaciones adicionales de conservación de datos. La Comisión evaluará la necesidad de todas estas categorías de datos.

4.5. Períodos de conservación (artículo 6 y artículo 12)

Los Estados miembros están obligados a garantizar que las categorías de datos mencionados en el artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años. Todo Estado miembro que «deba hacer frente a circunstancias especiales que justifiquen una ampliación limitada del período máximo de conservación» podrá ampliar el período máximo de conservación; dicha ampliación deberá notificarse a la Comisión, que podrá decidir, en el plazo de seis meses a partir de la notificación, si aprobar o rechazar la ampliación. Si bien el período de conservación máximo puede ampliarse, no hay ninguna disposición que prevea su reducción a menos de seis meses. Todos los Estados miembros que han transpuesto la Directiva, excepto uno, aplican períodos de conservación dentro de estos límites, y no se ha notificado a la Comisión ninguna ampliación. Sin embargo, no existe un enfoque coherente a escala de la UE.

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; un Estado miembro (Letonia) especifica 1,5 años; 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 miembros 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

---

63 Dictamen del Grupo de Trabajo del Artículo 29 sobre cuestiones de protección de datos relacionadas con los motores de búsqueda, 4 de abril de 2008.

64 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.

año para los datos de acceso a Internet, correo electrónico por Internet y telefonía por Internet; un Estado miembro (Eslovenia) especifica catorce meses para los datos de telefonía y ocho para los datos de Internet; un Estado miembro (Eslovaquia) especifica un año para los datos de telefonía fija y móvil y seis meses para los datos de Internet; un Estado miembro (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. Un Estado miembro (Hungría) conserva todos los datos durante un año, excepto los de llamadas infructuosas, que sólo se conservan seis meses. Un Estado miembro (Bélgica) no ha especificado ningún período de conservación de datos para las categorías mencionadas en la Directiva. Los detalles figuran en el cuadro 3.

Cuadro 3: Períodos de conservación especificados en el Derecho nacional	
Bélgica[65]	Entre 1 año y 36 meses para los servicios telefónicos «accesibles al público». No hay disposiciones respecto de los datos de Internet
Bulgaria	1 año. Los datos a los que se ha accedido podrán conservarse un período adicional de 6 meses, previa solicitud
República Checa	No transpuesta
Dinamarca	1 año
Alemania	No transpuesta
Estonia	1 año
Irlanda	2 años para los datos de telefonía fija y telefonía móvil y 1 año para los datos de acceso a Internet, correo electrónico por Internet y telefonía por Internet
Grecia	1 año
España	1 año
Francia	1 año
Italia	2 años para los datos de telefonía fija y telefonía móvil y 1 año para los datos de acceso a Internet, correo electrónico por Internet y telefonía por Internet.
Chipre	6 meses
Letonia	18 meses
Lituania	6 meses
Luxemburgo	6 meses
Hungría	6 meses para llamadas infructuosas y 1 año para todos los demás datos
Malta	1 año para los datos de telefonía fija, móvil y por Internet y 6 meses para los datos de acceso a Internet y correo electrónico por Internet
Países Bajos	1 año
Austria	No transpuesta
Polonia	2 años
Portugal	1 año
Rumanía	No transpuesta (6 meses en virtud de la anterior legislación de transposición anulada)
Eslovenia	14 meses para los datos de telefonía y 8 meses para los datos de Internet
Eslovaquia	1 año para los datos de telefonía fija y telefonía móvil y 6 meses para los datos de acceso a Internet, correo electrónico por Internet y telefonía por Internet
Finlandia	1 año

[65] Artículo 126, apartado 2, de la Ley de 13 de junio de 2005 relativa a las comunicaciones electrónicas.

Cuadro 3: Períodos de conservación especificados en el Derecho nacional	
Suecia	No transpuesta
Reino Unido	1 año

Aunque la Directiva permite este enfoque diversificado, se considera que la Directiva prevé únicamente una seguridad jurídica limitada y la previsibilidad en toda la UE para los operadores activos en más de un Estado miembro y para los ciudadanos cuyas comunicaciones puedan almacenarse en distintos Estados miembros. Teniendo en cuenta la creciente internacionalización del tratamiento de datos y la externalización del almacenamiento de datos, deberían estudiarse las opciones para una mayor armonización de los períodos de conservación en la UE. 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 estudiará la aplicación de diferentes períodos para diferentes categorías de datos, para las distintas categorías de delitos graves o una combinación de ambos[66]. La información cuantitativa facilitada hasta ahora por los Estados miembros en lo que respecta a la antigüedad de los datos conservados indica que, cuando los servicios con funciones coercitivas realizan la solicitud de acceso (inicial), cerca del 90 % de los datos cuentan con una antigüedad de seis meses o menos y cerca del 70 % con una de tres meses o menos (véase el apartado 5.2).

4.6. Protección y seguridad de los datos y autoridades de control (artículos 7 y 9)

La Directiva obliga a los Estados miembros a garantizar que los operadores respeten, como mínimo, cuatro principios de seguridad de los datos, a saber:

(g) que 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 [pública de comunicaciones];

(h) que 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;

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

(j) que los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación [para los fines recogidos en la Directiva].

[66] La propuesta de Directiva de conservación de datos de la Comisión de 2005 preveía un período de conservación de un año para los datos de telefonía y de seis meses para los datos de Internet.

En consonancia con la Directiva de protección de datos y la Directiva sobre privacidad, se prohíbe a los operadores utilizar para otros fines los datos conservados de conformidad con la Directiva, siempre que esos datos no se hubieran conservado también para esos fines[67]. Los Estados miembros designarán unas autoridades de control se encarguen de vigilar con plena independencia la aplicación de estos principios, y podrá tratarse de las mismas autoridades previstas en la Directiva de protección de datos.[68]

Quince Estados miembros 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. No está claro qué medidas de seguridad técnicas y organizativas, como la autenticación fuerte o una gestión detallada de los registros de acceso[69], se han aplicado. Veintidós Estados miembros cuentan con una autoridad de control responsable de la supervisión de la aplicación de los principios. En la mayoría de los casos se trata de la autoridad de protección de datos. Los detalles figuran en el cuadro 4.

Cuadro 4: Protección y seguridad de los datos y autoridades de control

Estado miembro	*Disposiciones sobre protección y seguridad de los datos en el Derecho nacional*	*Autoridad de control*
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[70]. No parece abordarse el principio de destrucción obligatoria de los datos al final del período de conservación.	Instituto de Servicios Postales y Telecomunicaciones
Bulgaria	Ley de transposición incluye la obligación de aplicar los cuatro principios[71].	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.
República Checa[72]	No transpuesta.	

67 Artículo 13, apartado 1, de la Directiva 95/46/CE.

68 Artículo 28 de la Directiva 95/46/CE.

69 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. La gestión detallada de los registros de acceso implica 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.

70 Artículo 6 del Real Decreto de 9 de enero de 2003.

71 Artículo 4, apartado 1, de la Ley sobre comunicaciones electrónicas (modificada) de 2010.

72 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.

Cuadro 4: Protección y seguridad de los datos y autoridades de control		
Estado miembro	*Disposiciones sobre protección y seguridad de los datos en el Derecho nacional*	*Autoridad de control*
Dinamarca	Se contemplan los cuatro principios[73].	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 permiten el acceso de la policía a la información sobre tráfico de telecomunicaciones.
Alemania	No transpuesta.	
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[74].	La Autoridad de Vigilancia Técnica es la autoridad responsable.
Irlanda[75]	La Ley de transposición incluye la obligación de aplicar los cuatro principios.	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.
Grecia[76]	La Ley de transposición incluye la obligación de aplicar los cuatro principios, así como el requisito adicional para que los operadores de elaborar y aplicar un plan para garantizar el cumplimiento, bajo la supervisión de un responsable de la seguridad de los datos.	Autoridad responsable de la protección de los datos personales y de la privacidad de las comunicaciones.
España[77]	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).	La autoridad responsable es la Agencia de Protección de Datos.
Francia[78]	La Ley de transposición incluye la obligación de aplicar los cuatro principios.	La Comisión Nacional de la Tecnología de la Información y de las Libertades supervisa el cumplimiento de las obligaciones.

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

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

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

[76] Artículo 6 de la Ley 3917/2011.

[77] 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).

[78] 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.

Cuadro 4: Protección y seguridad de los datos y autoridades de control		
Estado miembro	*Disposiciones sobre protección y seguridad de los datos en el Derecho nacional*	*Autoridad de control*
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[79].	La Autoridad de protección de datos supervisa el cumplimiento de la Directiva.
Chipre[80]	La legislación de transposición contempla los cuatro principios.	El Comisario para la Protección de los Datos Personales controla la aplicación de la legislación de transposición.
Letonia[81]	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.	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.
Lituania[82]	La legislación de transposición contempla los cuatro principios.	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.
Luxemburgo[83]	La legislación de transposición contempla los cuatro principios.	Autoridad de protección de datos.
Hungría[84]	La legislación de transposición contempla los cuatro principios.	Comisario Parlamentario para la Protección de Datos y la Libertad de Información.
Malta[85]	La legislación de transposición contempla los cuatro principios.	Comisario de Protección de Datos.
Países Bajos[86]	La legislación de transposición contempla los cuatro principios.	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.
Austria	No transpuesta.	
Polonia	La legislación de transposición contempla los cuatro principios[87].	Autoridad de protección de datos.
Portugal	La legislación de transposición contempla los cuatro principios[88].	Autoridad portuguesa de protección de datos.

79 Artículos 123 y 126 del Código de Protección de Datos.

80 Artículos 14 y 15 de la Ley 183 (I)/2007.

81 Artículo 4, apartado 4, y artículo 71, apartados 6 a 8, de la Ley de comunicaciones electrónicas.

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

83 Artículo 1, apartado 5, de la Ley de 24 de julio de 2010.

84 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.

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

86 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.*

87 Artículos 180a y 180e de la Ley de telecomunicaciones.

Cuadro 4: Protección y seguridad de los datos y autoridades de control		
Estado miembro	*Disposiciones sobre protección y seguridad de los datos en el Derecho nacional*	*Autoridad de control*
Rumanía	No transpuesta.	
Eslovenia[89]	La legislación de transposición contempla los cuatro principios.	Comisario de Información.
Eslovaquia[90]	La legislación de transposición contempla los cuatro principios.	La autoridad de regulación de precios en el ámbito de las comunicaciones electrónicas supervisa la protección de los datos personales.
Finlandia	La legislación de transposición sólo prevé expresamente la obligación de destruir los datos al final del período de conservación[91].	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.
Suecia	No transpuesta.	
Reino Unido	La legislación de transposición contempla los cuatro principios[92].	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).

La transposición del artículo 7 es incoherente. Los datos conservados constituyen potencialmente datos muy personales y sensibles, por lo que se precisa un alto nivel de protección y seguridad de los datos en todo el proceso de almacenamiento, recuperación y uso, que deberá realizarse de forma coherente y visible a fin de minimizar el riesgo de violaciones de la intimidad y para mantener la confianza de los ciudadanos. La Comisión estudiará 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. También tendrá en cuenta las recomendaciones efectuadas en el informe relativo a la segunda acción común de control y ejecución por el Grupo de Trabajo del Artículo 29 sobre protección de datos, en el sentido de adoptar normas mínimas y medidas salvaguardia y de seguridad técnica y organizativa[93].

---

88 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.

89 Artículo 107a, apartado 6) y 107c de la Ley de comunicaciones electrónicas.

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

91 Artículo 16, apartado 3, de la Ley de comunicaciones electrónicas.

92 Artículo 6 del Reglamento de conservación de datos.

93 Dictamen 3/2006 del Grupo de Trabajo del Artículo 29 sobre protección de datos (WP119); Informe 01/2010.

4.7. Estadísticas (artículo 10)

Los Estados miembros velarán por que se faciliten anualmente a la Comisión las estadísticas sobre la conservación de datos. 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 (es decir, la antigüedad de los datos); y

– los casos en que no pudieron satisfacerse las solicitudes de datos.

Al solicitar estadísticas de conformidad con esta disposición, la Comisión pidió a los Estados miembros que facilitasen información detallada sobre los casos de solicitudes individuales de datos. No obstante, las estadísticas proporcionadas diferían en alcance y detalle: algunos Estados miembros distinguieron en sus respuestas entre los diferentes tipos de comunicación, algunos señalaron la antigüedad de los datos en el momento de la solicitud, mientras que otros sólo facilitaron estadísticas anuales sin desglose detallado. Diecinueve Estados miembros[94] proporcionaron estadísticas sobre el número de solicitudes de datos para 2009 o 2008; entre ellos figuraban 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 ha sido anulada. Siete Estados miembros que han transpuesto la Directiva no facilitaron estadísticas, aunque Bélgica facilitó una estimación del volumen anual de las solicitudes de datos de telefonía (300 000).

La disponibilidad de datos cualitativos y cuantitativos fiables es esencial para demostrar la necesidad y la importancia de medidas de seguridad como la conservación de datos. Esto ya fue reconocido en el plan de acción de 2006 para evaluar la delincuencia y la justicia penal[95], que incluyó un objetivo consistente en desarrollar métodos para la recogida periódica de datos, de acuerdo con la Directiva, y en incluir las estadísticas en la base de datos de Eurostat (siempre que cumplan las normas de calidad). No ha sido posible cumplir este objetivo, dado que la mayoría de los Estados miembros no han transpuesto completamente la Directiva hasta los dos últimos años y utilizan diferentes interpretaciones respecto de la fuente de las estadísticas. La Comisión, en su futura propuesta para revisar el marco de la conservación de datos, junto con la revisión del plan de acción sobre estadísticas, intentará desarrollar 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.

---

94 República Checa, Dinamarca, Alemania, Estonia, Irlanda, Grecia, España, Francia, Chipre, Letonia, Lituania, Malta, Países Bajos, Austria, Polonia, Eslovenia, Eslovaquia, Finlandia y Reino Unido,

95 Comunicación (2006)437 de la Comisión «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».

4.8. Transposición en los países del EEE

Existe legislación sobre conservación de datos en Islandia, Liechtenstein y Noruega[96].

4.9. Decisiones de los tribunales constitucionales respecto de las leyes de transposición

El Tribunal Constitucional rumano en octubre de 2009, el Tribunal Constitucional Federal alemán en marzo de 2010 y el Tribunal Constitucional checo en marzo de 2011 anularon las leyes que transponían la Directiva en sus respectivas jurisdicciones por el motivo de que eran inconstitucionales. El Tribunal rumano[97] 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. Sin embargo, sobre la base de la jurisprudencia del Tribunal Europeo de Derechos Humanos[98], 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 artículo 8 del Convenio Europeo de Derechos Humanos.

El Tribunal Constitucional alemán[99] 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 usos estrictamente limitados, junto con una seguridad de los datos suficientemente elevada, no viola necesariamente la Ley Fundamental alemana. 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 deberán 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.

El Tribunal Constitucional de la República Checa[100] anuló la legislación de transposición sobre la base de que, como medida que interfiere con los derechos fundamentales, la legislación de transposición no es suficientemente clara y precisa en su formulación. El Tribunal criticó la limitación de la finalidad por no ser suficientemente restrictiva, habida

---

96 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. En Noruega, la legislación de transposición se aprobó el 5 de abril de 2011, y actualmente se encuentra pendiente de sanción real.

97 Decisión nº 1258 del Tribunal Constitucional rumano de 8 de octubre de 2009.

98 Tribunal Europeo de Derechos Humanos, Rotaru contra Rumania, 2000; Sunday Times contra Reino Unido, 1979; y Príncipe Hans-Adam de Liechtenstein contra Rumania, 2001.

99 Bundesverfassungsgericht, 1 BvR 256/08, apartados 1–345.

100 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.

cuenta de la escala y alcance del requisito de conservación de datos. Alegó 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 de poder de las autoridades públicas. El Tribunal no criticó a la propia Directiva y declaró que permitía un margen de maniobra suficiente para que República Checa la transpusiera de conformidad con la Constitución. Sin embargo, el Tribunal, *obiter dictum,* manifestó dudas en 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 el uso de tarjetas SIM anónimas.

Estos tres Estados miembros están ahora estudiando cómo volver a transponer la Directiva. También se han presentado asuntos de conservación de datos ante los tribunales constitucionales de Bulgaria, lo que dio lugar a una revisión de la Ley de transposición; de Chipre, donde se consideró que las resoluciones judiciales dictadas con arreglo a la ley de transposición eran anticonstitucionales; y de Hungría, donde está pendiente un asunto relativo a la omisión de los fines legales del tratamiento de datos en la legislación de transposición[101].

La Comisión estudiará las cuestiones planteadas por la jurisprudencia nacional en su futura propuesta para revisar el marco de la conservación de datos.

4.10. Aplicación en curso de la Directiva

La Comisión espera que los 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, lo hagan lo antes posible. De no ser este el caso, la Comisión se reserva el derecho de ejercer sus competencias en virtud de los Tratados de la UE. En la actualidad, el Tribunal de Justicia ha considerado que dos Estados miembros que no la han transpuesto (Austria y Suecia) han violado sus obligaciones conforme al Derecho de la UE[102]. En abril de 2011, la Comisión decidió llevar por segunda vez a Suecia ante el Tribunal de Justicia por incumplimiento de la sentencia en el asunto C- 185/09, que solicitaba la imposición de sanciones financieras en virtud del artículo 260 del Tratado de Funcionamiento de la Unión Europea, a raíz de una Decisión del Parlamento de Suecia de posponer doce meses la adopción de legislación de transposición. La Comisión sigue estrechamente la situación en Austria, que ha proporcionado un calendario para la adopción inminente de la legislación de transposición.

---

101 Tribunal Supremo Administrativo búlgaro, Decisión n° 13627 de 11 de diciembre de 2008; Tribunal Supremo de Chipre, recurso nº 65/2009, 78/2009, 82/2009 y 15/2010-22/2010 de 1 de febrero de 2011; la solicitud de apreciación de la constitucionalidad fue presentada por la Unión de Libertades Civiles de Hungría el 2 de junio de 2008.

102 Asuntos C-189/09 y C-185/09, respectivamente.

5. PAPEL DE LOS DATOS CONSERVADOS EN LA JUSTICIA PENAL Y EN LA APLICACIÓN DE LA LEY

La presente sección resume las funciones de los datos conservados según lo descrito por los Estados miembros en sus contribuciones al proceso de evaluación de la aplicación de la Directiva.

5.1. Volumen de datos conservados a que han accedido las autoridades nacionales competentes

El volumen tanto del tráfico de telecomunicaciones como de las solicitudes de acceso a los datos de tráfico está aumentando. Las estadísticas facilitadas por diecinueve Estados miembros para 2008 o 2009 indican que, en general en la UE, cada año se presentaron más de 2 millones de solicitudes de datos, con grandes diferencias entre los Estados miembros: desde menos del 100 al año (Chipre) a más de un millón (Polonia). Según la información sobre el tipo de datos solicitados que facilitaron doce Estados miembros, para 2008 o 2009, el tipo de datos solicitado con mayor frecuencia estaba relacionado con la telefonía móvil (véanse los cuadros 5, 8 y 12). 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.

No hay una explicación clara para estas variaciones, aunque el tamaño de la población, las tendencias delictivas predominantes, las limitaciones de fines y las condiciones para el acceso y los costes de la adquisición de datos son factores relevantes.

5.2. Antigüedad de los datos conservados a los que se ha accedido

Sobre la base del desglose estadístico facilitado por nueve Estados miembros[103] para 2008 (véase resumen en el cuadro 5 y otros detalles en el anexo), en el momento de presentarse la solicitud (inicial) de acceso, alrededor del 90 % de los datos consultados por las autoridades competentes ese año tenían una antigüedad de seis meses o menos, y alrededor del 75 % tenían una antigüedad de tres meses o menos.

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 %

[103] República Checa, Dinamarca, Estonia, Irlanda, España, Chipre, Letonia, Malta y Reino Unido.

Según la mayoría de los Estados miembros, el uso de los datos conservados con una antigüedad mayor de tres e incluso seis meses es menos frecuente, pero puede ser de crucial importancia; su uso tiende a dividirse en tres categorías. En primer lugar, los datos de Internet suelen solicitarse después de otras formas de prueba en el curso de las investigaciones penales. El análisis de los datos de telefonía móvil y fija genera a menudo posibles pistas que conducen a la solicitud de datos más antiguos. Por ejemplo, si durante una investigación se descubre un nombre gracias a los datos de telefonía móvil o de red fija, los investigadores pueden querer identificar la dirección del Protocolo de Internet (IP) que dicha persona ha estado utilizando y pueden querer identificar con quien ha estado en contacto durante un período de tiempo determinado utilizando esa dirección IP. En tal caso, es probable que los investigadores soliciten datos que les permitan rastrear también las comunicaciones con otras direcciones IP y la identidad de las personas que han utilizado esas direcciones IP.

En segundo lugar, las investigaciones de delitos particularmente graves, de una serie de delitos, de la delincuencia organizada y de atentados terroristas tienden a basarse en datos conservados más antiguos que reflejen el tiempo que se necesita para planificar estos delitos, a fin de identificar las pautas de comportamiento criminal y las relaciones entre los cómplices de un delito, y establecer la intencionalidad delictiva. Las actividades relacionadas con los delitos financieros complejos no se detectan a menudo hasta pasados varios meses. En tercer lugar, y excepcionalmente, los Estados miembros han solicitado datos de tráfico conservados en otro Estado miembro, que generalmente sólo pueden comunicarse previa autorización judicial en respuesta a una comisión rogatoria cursada por un juez del Estado miembro solicitante. Este tipo de asistencia judicial puede ser un proceso muy largo, lo que explica por qué algunos datos solicitados tienen en estos casos una antigüedad superior a seis meses.

5.3. Solicitudes transfronterizas de datos conservados

Los enjuiciamientos e investigaciones penales pueden incluir pruebas, testigos o acontecimientos, que hayan tenido lugar en más de un Estado miembro. Según las estadísticas facilitadas por los Estados miembros, menos del 1 % de todas las solicitudes de datos conservados se referían a datos conservados en otro Estado miembro. Los servicios con funciones coercitivas indicaron que preferían solicitar datos a operadores nacionales, que pueden tener almacenados los datos pertinentes, en lugar de iniciar procedimientos de asistencia judicial que pueden requerir mucho tiempo y sin ninguna garantía de que se concederá el acceso. La Decisión Marco 2006/960/JAI del Consejo sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea[104], en la que se fijan plazos para la comunicación de información a raíz de una petición de otro Estado miembro, no es aplicable, porque los datos conservados se consideran información obtenida por medios coercitivos, lo que queda fuera del ámbito de este instrumento. Sin embargo, ningún Estado miembro ni servicio con funciones coercitivas ha solicitado que se facilite en mayor medida este intercambio transfronterizo.

---

[104] 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 de 29.12.2006, pp. 89-100 y DO L 200 de 1.8.2007, pp. 637-648.

5.4. Valor de los datos conservados en los enjuiciamientos e investigaciones penales

Si bien el número absoluto de solicitudes de datos no refleja necesariamente el valor de los datos en las investigaciones de delitos, los Estados miembros en general han comunicado que la conservación de datos es valiosa cuanto menos, y en algunos casos indispensable[105], para la prevención y la lucha contra la delincuencia, incluida la protección de las víctimas y la absolución de inocentes en procedimientos penales. Las condenas efectivas se basan en la confesión de culpabilidad, las declaraciones de testigos o pruebas forenses. Se ha comunicado que los datos de tráfico conservados han resultado ser necesarios para ponerse en contacto con testigos que de otra manera no habrían sido identificados, y para aportar pruebas o pistas para determinar la complicidad en un delito. Algunos Estados miembros[106] alegaron asimismo que el uso de datos conservados contribuyó a absolver a personas sospechosas de delitos sin tener que recurrir a otros métodos de vigilancia, como las escuchas telefónicas y los registros domiciliarios, que podrían considerarse más intrusivos.

No existe ninguna definición general de «delito grave» en la UE y, por consiguiente, no existen estadísticas comunitarias sobre la incidencia de los delitos graves ni los enjuiciamientos o investigaciones de delitos graves, aunque se publican periódicamente datos sobre delincuencia y justicia. El volumen total de las solicitudes de acceso a datos conservados, según lo comunicado por los 19 Estados miembros que proporcionaron datos para 2009 o 2008, fue de alrededor de 2,6 millones. Frente a las últimas estadísticas disponibles sobre delincuencia y justicia penal para estos 19 Estados miembros (que se refieren a todos los delitos notificados, no sólo a los delitos graves) puede decirse que se presentaron algo más de dos solicitudes por agente de policía al año, o aproximadamente once solicitudes por cada 100 delitos registrados[107].

Sobre la base de las estadísticas y los ejemplos ilustrativos proporcionados, que vinculan el uso de los datos de comunicaciones históricas conservados con el número de condenas, sentencias absolutorias, casos archivados y delitos evitados, pueden sacarse varias conclusiones en cuanto al papel y valor de los datos conservados en la investigación penal.

Establecimiento de pistas de investigación

En primer lugar, los datos conservados permiten establecer pistas de prueba sobre un delito. Se utilizan para comprender o para corroborar otras formas de prueba sobre las actividades y

---

105 La República Checa considera que la conservación de datos es «completamente indispensable en un gran número de casos»; Hungría declaró que es «indispensable en las actividades normales de [los servicios con funciones coercitivas]»; Eslovenia declaró que la ausencia de datos conservados «paralizaría el funcionamiento de los servicios con funciones coercitivas»; un servicio de policía del Reino Unido describió la disponibilidad de los datos de tráfico como «absolutamente crucial … para investigar la amenaza del terrorismo y las formas graves de delincuencia».

106 Alemania, Polonia, Eslovenia y Reino Unido.

107 En 2007 había 1,7 millones de agentes de policía en la UE-27, de los cuales 1,2 millones en los 19 Estados miembros que proporcionaron estadísticas sobre solicitudes de acceso a los datos conservados; en 2007 se produjeron 29,2 millones de delitos registrados por la policía en la UE, de los que 24 millones se registraron en los 19 Estados que proporcionaron estadísticas (fuente: Eurostat 2009).

los vínculos entre sospechosos. Los datos de localización, en particular, han sido utilizados tanto por los servicios con funciones coercitivas como por los acusados para excluir a sospechosos de escenas del delito y verificar coartadas. Estas pruebas pueden por tanto excluir a personas de investigaciones penales, suprimiendo así la necesidad de investigaciones más intrusivas, o dar lugar a sentencias absolutorias. Bélgica citó la condena en 2008 de los autores del secuestro de un empleado del tribunal penal de Amberes, donde los datos de localización que vincularon sus actividades en tres ciudades fueron decisivos para convencer al jurado de su complicidad. En otro caso, un asesinato cometido en 2007 y que estaba relacionado con una banda de moteros, los datos de localización de los teléfonos móviles de los delincuentes demostraron que se encontraban en la zona cuando se produjo el asesinato y ello dio lugar a una confesión parcial[108]. Según Bélgica, Irlanda y el Reino Unido, algunos delitos que suponen la comunicación por Internet *sólo* pueden investigarse mediante la conservación de datos: por ejemplo, las amenazas de violencia proferidas en foros de debate sólo dejan rastro en los datos de tráfico en el ciberespacio. Una situación similar se aplica en el caso de los delitos perpetrados por teléfono. Hungría y Polonia citaron un caso de fraude contra personas mayores a finales de 2009 y principios de 2010 realizado por medio de llamadas en que los autores pretendían ser familiares necesitados de un préstamo, que sólo pudieron ser identificados gracias a los datos de telefonía conservados.

Inicio de investigaciones penales

En segundo lugar, ha habido casos en los que, a falta de pruebas forenses o de testigos oculares, la única manera de iniciar una investigación penal era consultar datos conservados. Alemania citó el ejemplo del asesinato de un agente de policía, en que el autor del crimen escapó en el vehículo de la víctima, que luego abandonó. Fue posible determinar que posteriormente había pedido por teléfono otro medio de transporte. No existían pruebas forenses ni testigos oculares de la identidad del asesino, y las autoridades recurrieron a la disponibilidad de estos datos de tráfico para proseguir la investigación. En los casos de abuso sexual infantil por Internet, la conservación de datos ha sido indispensable para el éxito de las investigaciones. Junto con otras técnicas de investigación, los datos conservados han permitido la identificación de los consumidores de contenidos de abusos infantiles[109], y han ayudado a identificar y proteger a los menores víctimas de estos abusos. La República Checa comunicó que sin acceso a los datos de Internet conservados habría sido imposible iniciar las investigaciones en la «Operación Vilma» sobre una red de usuarios y difusores de pornografía infantil. A escala de la UE, la eficacia de la Operación Rescate (bajo los auspicios de Europol) para la protección de menores contra abusos se vio perjudicada porque la falta de legislación de transposición en materia de conservación de datos impidió a ciertos Estados miembros investigar a miembros de una gran red de pederastas internacional utilizando direcciones IP con una antigüedad de hasta un año.

---

108 National Policing Improvement Agency (Reino Unido), *The Journal of Homicide and Major Incident Investigation*, Volumen 5, nº 1, primavera de 2009, pp. 39-51.

109 El proyecto «medición y análisis de la actividad de P2P (*peer to peer*) contra contenidos pedófilos», financiado en el marco del programa para una Internet más segura, proporcionó información precisa sobre las actividades pedófilas en el sistema *peer to peer* eDonkey, permitiendo la identificación de 178 000 usuarios que solicitaron contenidos pedófilos (de un total de 89 millones de usuarios controlados).

En la investigación de la ciberdelincuencia, una dirección IP es a menudo la primera pista. Los servicios con funciones coercitivas, mediante la obtención de datos de tráfico, pueden identificar al abonado al que corresponde la dirección IP, antes de determinar si puede iniciarse una investigación penal. También puede permitir a la policía prevenir a las víctimas potenciales de ciberataques: cuando la policía consigue neutralizar un servidor de mando y control utilizado por los operadores de *Botnet*, sólo pueden ver las direcciones IP vinculadas a ese servidor; pero al acceder a los datos conservados la policía puede identificar y advertir a las víctimas potenciales propietarias de las direcciones IP.

Los datos conservados forman parte integrante de la investigación penal

En tercer lugar, aunque los tribunales y servicios con funciones coercitivas en la mayoría de los Estados miembros no mantienen estadísticas sobre qué tipo de pruebas han resultado cruciales para la imposición de condenas o sentencias absolutorias, los datos conservados forman parte integrante del enjuiciamiento y la investigación penal en la UE. Algunos Estados miembros manifestaron que no podían siempre separar el impacto de los datos conservados en el éxito de los enjuiciamientos y las investigaciones penales, porque los tribunales tienen en cuenta todas las pruebas presentadas y raramente consideran que un único elemento de prueba es concluyente[110]. Los Países Bajos comunicaron que, de enero a julio de 2010, los datos de tráfico histórico fueron un factor decisivo en 24 resoluciones judiciales. Finlandia comunicó que en el 56 % de las 3 405 solicitudes, los datos conservados resultaron ser «importantes» o «indispensables» para la detección o enjuiciamiento de delitos. El Reino Unido facilitó información destinada a cuantificar el impacto de la conservación de datos en las actuaciones penales; comunicó que, en tres de sus organismos con funciones coercitivas, los datos conservados fueron necesarios en la mayor parte, si no la totalidad, de las investigaciones que dieron lugar a enjuiciamientos o condenas.

5.5. Evolución tecnológica y uso de tarjetas SIM de prepago

Los servicios con funciones coercitivas deben seguir el ritmo de la evolución tecnológica que se utiliza para cometer delitos. La conservación de datos figura entre las herramientas de investigación penal necesarias para equiparlos para hacer frente a los retos de la delincuencia moderna en su diversidad, volumen y velocidad, de una manera viable y rentable. Una serie de formas de comunicación cada vez más comunes están fuera del ámbito de aplicación de la Directiva. Las redes virtuales privadas (VPN) de, por ejemplo, universidades o grandes empresas, permiten a varios usuarios acceder a Internet a través de un punto de acceso único utilizando la misma dirección IP. Sin embargo, actualmente se está introduciendo nueva tecnología que permite la atribución de direcciones a usuarios individuales de VPN.

La proporción de usuarios de telefonía móvil que utilizan los servicios de prepago varía en la UE. Algunos Estados miembros han alegado que las tarjetas SIM de prepago anónimas, especialmente cuando se han adquirido en otro Estado miembro, también podrían ser utilizadas por los implicados en actividades delictivas como medio para evitar su

[110] Bélgica, República Checa y Lituania.

identificación en las investigaciones penales[111]. Seis Estados miembros (Dinamarca, España, Italia, Grecia, Eslovaquia y Bulgaria) han adoptado medidas que exigen el registro de las tarjetas SIM de prepago. Estos y otros Estados miembros (Polonia, Chipre y Lituania) han abogado por una medida de la UE para el registro obligatorio de la identificación de los usuarios de los servicios de prepago. No se han facilitado pruebas en cuanto a la eficacia de tales medidas nacionales. Se han puesto de relieve las potenciales limitaciones, por ejemplo, en los casos de usurpación de identidad, o cuando una tarjeta SIM es adquirida por un tercero, o cuando un usuario utiliza la itinerancia con una tarjeta adquirida en un tercer país. En general, la Comisión no está convencida de la necesidad de adoptar medidas en este ámbito a nivel de la UE de momento.

6. EFECTOS DE LA CONSERVACIÓN DE DATOS EN LOS OPERADORES Y CONSUMIDORES

6.1. Operadores y consumidores

En una declaración conjunta a la Comisión, cinco grandes asociaciones industriales afirmaron que el impacto económico de la Directiva era «relevante» o «enorme» para los «pequeños proveedores de servicios», porque «la Directiva deja un amplio margen de maniobra»[112]. Ocho operadores presentaron estimaciones muy diversas de los costes de aplicación de la Directiva en términos de gastos de capital y de explotación. Estas alegaciones se ven confirmadas por las declaraciones de los niveles de reembolso de los costes de los operadores notificados por cuatro de los Estados miembros (véase el cuadro 6).

Un estudio realizado antes de la transposición de la Directiva en la mayoría de los 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 EUR el primer año y 9 870 EUR al mes de costes de funcionamiento en adelante[113], y los costes de creación de un sistema de extracción de datos en 131 190 EUR, con unos costes de funcionamiento de 28 960 EUR al mes. Sin embargo, 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»[114]. Los costes unitarios de conservación de datos son inversamente proporcionales al tamaño del operador y al nivel de normalización adoptado por un Estado miembro para la interacción con los operadores[115].

---

111 Conclusiones del Consejo sobre la lucha contra la utilización delictiva y la utilización anónima de las comunicaciones electrónicas.

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

113 *Wilfried Gansterer & Michael Ilger, Data Retention – The EU Directive 2006/24/EC from a Technological Perspective, Wien: Verlag Medien und Recht*, 2008.

114 Bundesverfassungsgericht, 1 BvR 256/08 de 2 de marzo de 2010, apartado 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx

La mayoría de los operadores, en su respuesta al cuestionario de 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.

No hay pruebas de ningún efecto cuantificable o sustancial de la Directiva en los precios al consumo de los servicios de comunicaciones electrónicas; los representantes de los consumidores no realizaron contribuciones a la consulta pública de 2009. 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, no hay pruebas que corroboren que se ha producido un cambio de comportamiento en Alemania ni en la UE en general[116].

La Comisión tiene previsto evaluar el impacto de las futuras modificaciones de la Directiva para la industria y los consumidores, incluyendo en su caso, una encuesta específica de Eurobarómetro para medir la percepción del público.

6.2. Reembolso de costes

La Directiva no regula el reembolso de los costes incurridos por los operadores como consecuencia del requisito de conservación de datos. Estos costes pueden considerarse:

(k) *gastos operativos,* es decir, los gastos de explotación o gastos recurrentes relacionados con el funcionamiento de la empresa, un dispositivo, un componente, el equipo o las instalaciones; y

(l) *gastos de capital,* es decir, los gastos de creación de beneficios futuros, o el coste de desarrollar o proporcionar partes no consumibles para el producto o sistema, que pueden incluir el coste de los trabajadores y gastos de las instalaciones, tales como alquileres y servicios públicos.

Todos los Estados miembros garantizan alguna forma de reembolso si se solicitan datos en el marco de un procedimiento penal. Dos Estados miembros comunicaron que reembolsan tanto gastos operativos como de capital. Seis reembolsan únicamente los gastos operativos. No se ha notificado ningún otro régimen de reembolso a la Comisión. Véanse los detalles en el cuadro 6.

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)

[116] La encuesta fue realizada por Forsa y encargada por AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

[117] Antes de la anulación de la legislación de transposición checa, la República Checa reembolsó tanto los gastos operativos como de capital y notificó unos costes de reembolso de 6,8 millones EUR para 2009.

Bulgaria	No	No	-
República Checa	No transpuesta[117]		
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)

De lo anterior puede concluirse que la Directiva no ha alcanzado plenamente su objetivo de establecer unas condiciones de competencia equitativas para los operadores en la UE. La Comisión estudiará 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.

7. IMPLICACIONES DE LA CONSERVACIÓN DE DATOS EN LOS DERECHOS FUNDAMENTALES

7.1. El derecho a la intimidad y la protección de los datos personales

La conservación de datos constituye una limitación del derecho a la intimidad y la protección de los datos personales, que son derechos fundamentales en la UE[118]. Cualquier limitación

[118] El artículo 7 y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (DO C 83 de 30.3.2010, p. 389) garantizan el derecho de toda persona a «la protección de los datos de carácter

deberá ser, con arreglo al artículo 52, apartado 1, de la Carta de los Derechos Fundamentales, «establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. 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». En la práctica, esto significa que toda limitación debe:[119]

(m) expresarse de una manera precisa y previsible;

(n) ser necesarias para alcanzar un objetivo de interés general o para proteger los derechos y libertades de otros;

(o) ser proporcional al objetivo perseguido; y

(p) ajustarse al contenido esencial de los derechos fundamentales en cuestión.

El artículo 8, apartado 2, del Convenio Europeo de Derechos Humanos reconoce también que la ingerencia de la autoridad pública en el ejercicio del respeto de la vida privada puede justificarse si es necesaria para la seguridad nacional, la seguridad pública o la prevención de las infracciones penales[120]. El artículo 15, apartado 1, de la Directiva sobre privacidad y los considerandos de la Directiva de conservación de datos reiteran estos principios en los que se basa el enfoque de la UE sobre la conservación de datos.

La posterior jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos ha definido las condiciones que debe cumplir cualquier limitación del derecho a la intimidad. Estas sentencias son pertinentes para establecer si debe modificarse la Directiva, en particular en lo que respecta a las condiciones de acceso y utilización de los datos conservados.

Toda limitación del derecho a la intimidad debe ser precisa y permitir la previsibilidad

En el asunto *Österreichischer Rundfunk*, el Tribunal de Justicia sostuvo que 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».

Toda limitación del derecho a la intimidad debe ser necesaria y proporcionar unas garantías mínimas

---

personal que la conciernan». El artículo 16 del Tratado de Funcionamiento de la Unión Europea (DO C 83 de 30.3.2010, p. 1) consagra también el derecho de toda persona a «la protección de los datos de carácter personal que le conciernan».

119 Véase la lista de control de los Derechos Fundamentales de la Comisión control para todas las propuestas legislativas que figura en la Comunicación de la Comisión COM (2010) 573/4, «Estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea».

120 Artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (STE nº 5), Consejo de Europa, 4.11.1950.

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 Europeo de Derechos Humanos sostuvo que tal limitación del derecho a la intimidad sólo puede considerarse necesaria sobre la base de la legislación nacional pertinente[121]. 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[122]. 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[123]. En cuanto a las escuchas telefónicas, la vigilancia secreta y los servicios de inteligencia, «[sería] 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».

Toda limitación del derecho a la intimidad debe ser proporcionada al interés general

Del mismo modo, el Tribunal de Justicia Europeo, en su sentencia en el asunto Schecke & Eifert relativo a la publicación de todos los beneficiarios de subvenciones agrícolas en Internet[124], constató que no parece que el legislador de la UE haya 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 Tribunal 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 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».

7.2. Críticas al principio de conservación de datos

Varias organizaciones de la sociedad civil se dirigieron a la Comisión alegando que la conservación de datos constituye, en principio, una restricción injustificada e innecesaria del derecho de los individuos a su intimidad. Consideran que la conservación «global e indiscriminada» de los datos de tráfico de telecomunicaciones, de localización y de los abonados constituyen una restricción ilegal de los derechos fundamentales. A raíz de un

---

121 Copland contra Reino Unido, sentencia del Tribunal Europeo de Derechos Humanos, Estrasburgo, 3.4.2007, p. 9.

122 Marper contra Reino Unido, sentencia del Tribunal Europeo de Derechos Humanos, Estrasburgo, 4.12.2008, p. 31.

123 Marper, p. 30.

124 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.

asunto planteado ante los tribunales de un Estado miembro (Irlanda) por un grupo de derechos civiles, está previsto que el Tribunal de Justicia Europeo aborde la cuestión de la legalidad de la Directiva[125]. También el Supervisor Europeo de Protección de Datos expresó sus dudas sobre la necesidad de la medida.

7.3. Peticiones de refuerzo de las normas de seguridad y de protección de los datos

El informe del Grupo de Trabajo del Artículo 29 sobre la segunda medida de ejecución alegó 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 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. El Grupo de Trabajo comunicó 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 «cc». Por tanto, el Grupo de Trabajo pide que se aclare que las categorías son exhaustivas, y que no pueden imponerse a los operadores otras obligaciones de conservación de datos.

El Supervisor Europeo de Protección de Datos ha declarado que la Directiva «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[126]. Ha declarado que un instrumento de la UE que contenga normas sobre la conservación obligatoria de datos deberá, en caso de demostrarse su necesidad, contener también normas sobre el acceso de los servicios con funciones coercitivas y sobre su ulterior utilización. Ha invitado a la UE a que adopte 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».

Las autoridades de protección de datos en general han alegado que la conservación de datos supone en sí misma un riesgo de posibles violaciones de la intimidad que la Directiva no aborda a nivel de la UE, exigiendo en vez a los Estados miembros que garanticen el respeto de las normas de protección de datos nacionales. Si bien no hay ejemplos concretos de casos graves de vulneración de la intimidad, el peligro de violación de la seguridad de los datos seguirá existiendo, y podrá incrementarse con la evolución de la tecnología y de las formas de comunicaciones, con independencia de si los datos se almacenan para fines comerciales o de seguridad, dentro o fuera de la UE, a menos que se establezcan nuevas salvaguardias.

8. CONCLUSIONES Y RECOMENDACIONES

Este informe ha puesto de relieve una serie de beneficios derivados del actual régimen de conservación de datos de la UE, y los ámbitos en los que se puede mejorar. La UE adoptó la

---

125 El 5 de mayo de 2010, el Irish High Court autorizó a Digital Rights Ireland Limited a acudir al Tribunal de Justicia de conformidad con el artículo 267 del Tratado de Funcionamiento de la Unión Europea.

126 Discurso pronunciado por Peter Hustinx en la conferencia «*Taking on the Data Retention Directive*», 3 de diciembre de 2010.

Directiva en un momento en que los riesgos de atentados terroristas inminentes eran elevados. La evaluación de impacto que la Comisión tiene intención de realizar ofrece la ocasión de evaluar la conservación de datos en la UE frente a los criterios de necesidad y proporcionalidad, habida cuenta y en interés de la seguridad interior, el buen funcionamiento del mercado interior y el refuerzo del respeto a la vida privada y del derecho fundamental a la protección de los datos personales. La propuesta de la Comisión sobre la revisión del marco para la conservación de datos debe inspirarse en las conclusiones y recomendaciones que se exponen a continuación.

8.1. La UE deberá apoyar y regular la conservación de datos como medida de seguridad

La mayoría de los Estados miembros consideran que las normas de la UE 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. Las pruebas facilitadas por los Estados miembros en forma de estadísticas y ejemplos son limitadas en algunos aspectos, pero no obstante son muestra del importante papel que desempeñan los datos conservados en la investigación penal. Estos datos proporcionan valiosas pistas y pruebas en la prevención y enjuiciamiento de delitos y para garantizar la justicia penal. Su utilización ha dado lugar a condenas por delitos que, sin la conservación de datos, nunca podrían haberse resuelto. También ha dado lugar a sentencias absolutorias de personas inocentes. La armonización de normas en este ámbito deberá 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 UE elevados niveles de respeto de la intimidad y protección de los datos personales.

8.2. La transposición ha sido desigual

La legislación de transposición está en vigor en 22 Estados miembros. La considerable libertad de que gozan los Estados miembros para adoptar las medidas de conservación de datos con arreglo al artículo 15, apartado 1, de la Directiva sobre privacidad hace que la evaluación de la Directiva de conservación de datos sea muy problemática. Existen considerables diferencias entre la legislación de transposición en los ámbitos de la limitación de la finalidad, el acceso a los datos, los períodos de conservación, la protección de datos y la seguridad de los datos y las estadísticas. Tres Estados miembros incumplen la Directiva puesto que su legislación de transposición fue anulada por sus respectivos tribunales constitucionales. Otros dos Estados miembros aún tienen que transponerla. La Comisión seguirá colaborando con todos los Estados miembros con el fin de garantizar la aplicación efectiva de la Directiva. También continuará con su función de velar por la aplicación de la legislación de la UE, recurriendo en última instancia a los procedimientos de infracción en caso necesario.

8.3. 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

La Directiva ha garantizado que en la mayoría de Estados miembros se conserven los datos. La Directiva no garantiza por sí misma que los datos conservados se almacenen, recuperen y

utilicen en el pleno respeto del derecho a la intimidad y la protección de los datos personales. La responsabilidad de garantizar estos derechos corresponde a los Estados miembros. La Directiva sólo busca una armonización parcial de los enfoques sobre conservación de datos; por lo tanto, no es de extrañar que 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. Sin embargo, más allá del grado de variación previsto expresamente por la Directiva, las diferencias en la aplicación nacional de la conservación de datos han presentado considerables dificultades para los operadores.

8.4. Deben reembolsarse sistemáticamente a los operadores los gastos en que incurran

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.

8.5. Garantizar la proporcionalidad en el proceso integrado de almacenamiento, recuperación y utilización

La Comisión velará 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. Reconocerá que las excepciones o limitaciones en lo que respecta a la protección de los datos personales sólo se aplicarán en la medida en que sean necesarias. Evaluará cuidadosamente las implicaciones para la eficacia y eficiencia del sistema de justicia penal y para la aplicación de la ley, para la intimidad y para los costes de la administración pública y los operadores, de una regulación más estricta de la conservación, el acceso y el uso de los datos de tráfico. En la evaluación de impacto deberán examinarse los siguientes ámbitos en particular:

- 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.

La Comisión estudiará 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[127], la Comisión estudiará cada uno de estos ámbitos a la luz de los principios 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[128].

8.6. Próximos pasos

A la luz de esta evaluación, la Comisión propondrá una revisión del actual marco de conservación de datos. Establecerá 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. Estudiará en profundidad la percepción del público sobre la conservación de datos y su impacto en el comportamiento. Estas conclusiones se incorporarán a una evaluación de impacto de las opciones estratégicas señaladas, que servirá de base para la propuesta de la Comisión.

---

127 Véase *supra* la referencia a la Comunicación relativa a la aplicación de la Carta de los derechos fundamentales; «Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia», COM (2010) 385 de 20.7.2010.

128 COM (2010) 609 de 4.11.2010.

Anexo: Estadísticas adicionales sobre la conservación de datos de tráfico

Notas para el anexo:

1. Antigüedad de los datos: el tiempo transcurrido entre la fecha en que se conservaron los datos y la fecha en que la autoridad competente solicitó la transmisión de los mismos.

2. Datos de Internet: los datos relativos al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet.

3. Las estadísticas para la República Checa, Letonia y Polonia son objeto de reservas (véase la sección 5.1).

Estadísticas presentadas por los Estados miembros para 2008

Cuadro 7: Solicitudes de datos de tráfico conservados por antigüedad en 2008									
Antigüedad de los datos solicitados (meses)/Estado miembro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	No consta								
Bulgaria	No consta								
República Checa	102691	18440	10110	319	0	0	0	0	131560
Dinamarca	2669	672	185	37	23	2	7	4	3599
Alemania	9363	2336	985	0	0	0	0	0	12684
Estonia	2773	733	157	827	0	0	0	0	4 490
Irlanda	8981	2016	936	1855	90	85	78	54	14095
Grecia	No consta el desglose por antigüedad								584
España	22629	15868	10298	4783	0	0	0	0	53578
Francia	No consta el desglose por antigüedad								503437
Italia	No consta								
Chipre	30	4	0	0	0	0	0	0	34
Letonia	10539	2739	1368	1211	597	438	0	0	16892
Lituania	55735	23817	5251	512	0	0	0	0	85315
Luxemburgo	No consta								
Hungría	No consta								
Malta	810	59	0	0	0	0	0	0	869
Países Bajos	No consta el desglose por antigüedad								85000
Austria	No consta el desglose por antigüedad								3093
Polonia	No consta								
Portugal	No consta								
Rumanía	No consta								
Eslovenia	No consta el desglose por antigüedad								2821
Eslovaquia	No consta								
Finlandia	9134	1144	448	214	268				4008
Suecia	No consta								
Reino Unido	315350	88339	34665	19398	6385	2973	1536	1576	470222
Total	**533504**	**156167**	**64403**	**29156**	**7095 ***	**3230 ***	**1353 ***	**1366 ***	**1392281**

* Con exclusión de Finlandia

Cuadro 8: Solicitudes de datos de tráfico conservados por tipo de datos en 2008 (entre paréntesis: número de casos en que no pudieron satisfacerse las solicitudes de datos – si consta)				
Tipo de datos/ Estado miembro	**Telefonía de red fija**	**Telefonía móvil**	**Internet**	**Total**
Bélgica	No consta			
Bulgaria	No consta			
República Checa	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Dinamarca	192 (0)	3273 (5)	134 (0)	3599 (5)
Alemania	No consta el desglose por tipo de datos			12684 (931)
Estonia	4114 (1519)	376 (7)	No consta	4 490 (1526)
Irlanda	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Grecia	No consta el desglose por tipo de datos			584
España	4448 (0)	40013 (0)	9117 (0)	53578 (0)
Francia	No consta el desglose por tipo de datos			503437
Italia	No consta			
Chipre	3 (0)	31 (5)	0 (0)	34 (5)
Letonia	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Lituania	765 (72)	84550 (5657)	No consta	85315 (5729)
Luxemburgo	No consta			
Hungría	No consta			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Países Bajos	No consta el desglose por tipo de datos			85000
Austria	No consta el desglose por tipo de datos			3093
Polonia	No consta			
Portugal	No consta			
Rumanía	No consta			
Eslovenia	No consta el desglose por tipo de datos			2821
Eslovaquia	No consta			
Finlandia	No consta el desglose por tipo de datos			4008
Suecia	No consta			
Reino Unido	90747 (0)	329421 (0)	50054 (0)	470222 (0)
Total				1392281

Cuadro 9: Solicitudes de datos de tráfico *de telefonía de red fija* conservados que se transmitieron, por antigüedad, en 2008									
Antigüedad de los datos solicitados (meses)/Estado miembro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	No consta								
Bulgaria	No consta								
República Checa	3669	916	143	124	0	0	0	0	4 852
Dinamarca	133	28	31	0	0	0	0	0	192
Alemania	No consta								
Estonia	1876	161	74	484	0	0	0	0	2595
Irlanda	4118	712	197	182	32	21	23	16	5301
Grecia	No consta								
España	1948	1431	741	328	0	0	0	0	4448
Francia	No consta								
Italia	No consta								
Chipre	3	0	0	0	0	0	0	0	3
Letonia	698	213	167	193	104	137	0	0	1512
Lituania	251	442	0	0	0	0	0	0	693
Luxemburgo	No consta								
Hungría	No consta								
Malta	28	1	0	0	0	0	0	0	29
Países Bajos	No consta								
Austria	No consta								
Polonia	No consta								
Portugal	No consta								
Rumanía	No consta								
Eslovenia	No consta								
Eslovaquia	No consta								
Finlandia	No consta								
Suecia	No consta								
Reino Unido	54805	27052	5340	753	1135	437	1050	175	90747
Total	**67529**	**30956**	**6693**	**2064**	**1271**	**595**	**1073**	**191**	**110372**

Cuadro 10: Solicitudes de datos de tráfico *de telefonía móvil* conservados que se transmitieron, por antigüedad, en 2008									
Antigüedad de los datos solicitados (meses)/Estado miembro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	No consta								
Bulgaria	No consta								
República Checa	98232	17013	7518	1	0	0	0	0	122764
Dinamarca	2433	628	143	33	20	1	7	3	3268
Alemania	No consta								
Estonia	248	58	35	28	0	0	0	0	369
Irlanda	4326	820	230	240	57	63	52	37	5825
Grecia	No consta								
España	17403	12114	7444	3052	0	0	0	0	40013
Francia	No consta								
Italia	No consta								
Chipre	23	3	0	0	0	0	0	0	26
Letonia	8928	2298	1085	746	394	257	0	0	13708
Lituania	55484	23375	14	20	0	0	0	0	78893
Luxemburgo	No consta								
Hungría	No consta								
Malta	575	53	0	0	0	0	0	0	628
Países Bajos	No consta								
Austria	No consta								
Polonia	No consta								
Portugal	No consta								
Rumanía	No consta								
Eslovenia	No consta								
Eslovaquia	No consta								
Finlandia	No consta								
Suecia	No consta								
Reino Unido	229375	52241	26228	16040	3333	521	339	1344	329421
Total	**417027**	**108603**	**42697**	**20160**	**3804**	**842**	**398**	**1384**	**594915**

Cuadro 11: Solicitudes de datos de tráfico *de Internet* conservados que se transmitieron, por antigüedad, en 2008									
Antigüedad de los datos solicitados (meses)/Estado miembro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	No consta								
Bulgaria	No consta								
República Checa	737	412	137	168	0	0	0	0	1454
Dinamarca	102	14	11	2	3	1	0	1	134
Alemania	No consta								
Estonia	No consta								
Irlanda	492	460	498	1422	0	0	0	0	2872
Grecia	No consta								
España	3278	2323	2113	1403	0	0	0	0	9117
Francia	No consta								
Italia	No consta								
Chipre	0	0	0	0	0	0	0	0	0
Letonia	424	150	75	219	74	34	0	0	976
Lituania	No consta								
Luxemburgo	No consta								
Hungría	No consta								
Malta	76	3	0	0	0	0	0	0	79
Países Bajos	No consta								
Austria	No consta								
Polonia	No consta								
Portugal	No consta								
Rumanía	No consta								
Eslovenia	No consta								
Eslovaquia	No consta								
Finlandia	No consta								
Suecia	No consta								
Reino Unido	31170	9046	3097	2605	1917	2015	147	57	50054
Total	**36279**	**12408**	**5931**	**5819**	**1994**	**2050**	**147**	**58**	**64686**

Estadísticas presentadas por los Estados miembros para 2009

Cuadro 12: Solicitudes de datos conservados por antigüedad en 2009									
Antigüedad de los datos solicitados (meses)/Estado miembro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	No consta								
Bulgaria	No consta								
República Checa	210975	56623	11620	1053	0	0	0	0	280271
Dinamarca	2980	685	179	104	54	38	12	14	4066
Alemania	No consta								
Estonia	4299	1836	1210	1065	0	0	0	0	8410
Irlanda	8117	1652	805	297	168	134	69	41	11283
Grecia	No consta								
España	29775	19346	13999	6970	0	0	0	0	70090
Francia	No consta el desglose por antigüedad								514813
Italia	No consta								
Chipre	31	8	1	0	0	0	0	0	40
Letonia	20758	2414	1088	796	565	475	0	0	26096
Lituania	30247	35456	5886	884	0	0	0	0	72473
Luxemburgo	No consta								
Hungría	No consta								
Malta	3336	362	151	174	0	0	0	0	4023
Países Bajos	No consta								
Austria	No consta								
Portugal	No consta								
Rumanía	No consta								
Polonia	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Eslovenia	No consta el desglose por antigüedad								1918
Eslovaquia	No consta el desglose por antigüedad								5214
Finlandia	2000	1310	532	152	76	0	0	0	4070
Suecia	No consta								
Reino Unido	No consta								
Total	**954845**	**297998**	**110996**	**64021**	**27961**	**24571**	**14065**	**34683**	**2051085**

Cuadro 13: Solicitudes de datos de tráfico conservados por tipo de datos en 2009 (entre paréntesis: número de casos en que no pudieron satisfacerse las solicitudes de datos – si consta)				
Tipo de datos/ Estado miembro	**Telefonía de red fija**	**Telefonía móvil**	**Internet**	**Total**
Bélgica	No consta			
Bulgaria	No consta			
República Checa	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Dinamarca	133 (0)	3771 (10)	162 (1)	4066 (11)
Alemania	No consta			
Estonia	6422 (2279)	902 (21)	1086 (468)	8410 (/2768]
Irlanda	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Grecia	No consta			
España	5055 (0)	(0) 56133	8902 (0)	70090 (0)
Francia	No consta el desglose por tipo de datos			514813
Italia	No consta			
Chipre	0 (0)	23 (3)	14 (0)	40 (3)
Letonia	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Lituania	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Luxemburgo	No consta			
Hungría	No consta			
Malta	156 (10)	(882) 3693	174 (10)	(902) 4023
Países Bajos	No consta			
Austria	No consta			
Polonia	No consta el desglose por tipo de datos			1048318
Portugal	No consta			
Rumanía	No consta			
Eslovenia	No consta el desglose por tipo de datos			1918 (48)
Eslovaquia	No consta el desglose por tipo de datos			5214 (157)
Finlandia	No consta el desglose por tipo de datos			4070
Suecia	No consta			
Reino Unido	No consta			
Total				2051082 (1069885)

Cuadro 14: Solicitudes de datos de tráfico *de telefonía de red fija* conservados que se transmitieron, por antigüedad, en 2009									
Antigüedad de los datos solicitados (meses)/Estado miembro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	No consta								
Bulgaria	No consta								
República Checa	9919	2907	47	36	0	0	0	0	12909
Dinamarca	105	19	7	2	0	0	0	0	133
Alemania	No consta								
Estonia	2254	866	599	424	0	0	0	0	4143
Irlanda	3934	337	69	70	50	39	16	11	4 526
Grecia	No consta								
España	2371	1492	844	348	0	0	0	0	5055
Francia	No consta								
Italia	No consta								
Chipre	0	0	0	0	0	0	0	0	0
Letonia	744	253	157	143	68	89	0	0	1454
Lituania	469	773	73	6	0	0	0	0	1321
Luxemburgo	No consta								
Hungría	No consta								
Malta	83	25	18	20	0	0	0	0	146
Países Bajos	No consta								
Austria	No consta								
Polonia	No consta								
Portugal	No consta								
Rumanía	No consta								
Eslovenia	No consta								
Eslovaquia	No consta								
Finlandia	No consta								
Suecia	No consta								
Reino Unido	No consta								
Total	**19879**	**6672**	**1814**	**1049**	**118**	**128**	**16**	**11**	**29687**

Cuadro 15: Solicitudes de datos de tráfico *de telefonía móvil* conservados que se transmitieron, por antigüedad, en 2009									
Antigüedad de los datos solicitados (meses)/Estado miembro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	No consta								
Bulgaria	No consta								
República Checa	197620	48841	472	0	0	0	0	0	246933
Dinamarca	2777	639	162	98	47	19	12	7	3761
Alemania	No consta								
Estonia	318	397	96	70	0	0	0	0	881
Irlanda	3669	835	220	210	115	92	50	28	5219
Grecia	No consta								
España	24065	15648	11147	5273	0	0	0	0	56133
Francia	No consta								
Italia	No consta								
Chipre	17	16	0	0	0	0	0	0	23
Letonia	18832	1912	778	515	394	263	0	0	22694
Lituania	25713	19595	28	0	0	0	0	0	45336
Luxemburgo	No consta								
Hungría	No consta								
Malta	2332	246	111	122	0	0	0	0	2811
Países Bajos	No consta								
Austria	No consta								
Polonia	No consta								
Portugal	No consta								
Rumanía	No consta								
Eslovenia	No consta								
Eslovaquia	No consta								
Finlandia	No consta								
Suecia	No consta								
Reino Unido	No consta								
Total	**275343**	**88119**	**13014**	**6288**	**556**	**374**	**62**	**35**	**383791**

Cuadro 16: Solicitudes de datos de tráfico *de Internet* conservados que se transmitieron, por antigüedad, en 2009									
Antigüedad de los datos solicitados (meses)/Estado miembro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	No consta								
Bulgaria	No consta								
República Checa	3369	4811	861	942	0	0	0	0	9983
Dinamarca	98	27	10	4	4	7	0	1	151
Alemania	No consta								
Estonia	315	145	56	102	0	0	0	0	618
Irlanda	489	455	502	0	0	0	0	0	1446
Grecia	No consta								
España	3339	2206	2008	1349	0	0	0	0	8902
Francia	No consta								
Italia	No consta								
Chipre	12	2	0	0	0	0	0	0	14
Letonia	852	198	74	90	88	86	0	0	1388
Lituania	4060	15087	1	88	0	0	0	0	19236
Luxemburgo	No consta								
Hungría	No consta								
Malta	150	14	0	0	0	0	0	0	164
Países Bajos	No consta								
Austria	No consta								
Polonia	No consta								
Portugal	No consta								
Rumanía	No consta								
Eslovenia	No consta								
Eslovaquia	No consta								
Finlandia	No consta								
Suecia	No consta								
Reino Unido	No consta								
Total	**12684**	**22945**	**3512**	**2575**	**92**	**93**	**0**	**1**	**41902**