CONCLUSIONES DEL ABOGADO GENERAL
SR. HENRIK SAUGMANDSGAARD ØE
presentadas el 19 de julio de 2016 (1)

Asuntos acumulados C-203/15 y C-698/15

Tele2 Sverige AB
contra
Post- och telestyrelsen (asunto C-203/15)

y

Secretary of State for the Home Department
contra
Tom Watson,
Peter Brice,
Geoffrey Lewis (asunto C-698/15),
con intervención de:
Open Rights Group,
Privacy International,
Law Society of England and Wales

[peticiones de decisión prejudicial presentadas por el Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo, Suecia) y la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil) (Reino Unido)]]

«Cuestión prejudicial — Directiva 2002/58 — Tratamiento de datos de carácter personal y protección de la vida privada en el sector de las comunicaciones electrónicas — Legislación nacional que establece una obligación general de conservar los datos relativos a las comunicaciones electrónicas — Artículo 7 de la Carta — Derecho al respeto de la vida privada — Artículo 8 de la Carta — Derecho a la protección de datos de carácter personal — Injerencia grave — Justificación — Artículo 15, apartado 1, de la Directiva 2002/58 — Artículo 52, apartado 1, de la Carta — Requisitos — Objetivo legítimo de lucha contra los delitos graves — Requisito de una base legal de Derecho nacional — Requisito de estricta necesidad — Requisito de proporcionalidad en una sociedad democrática»

Sumario

I –Marco jurídico10

A –Directiva 2002/5810

B –Derecho sueco12

1.Sobre el alcance de la obligación de conservación13

2.Sobre el acceso a los datos conservados14

a)LEK14

b)RB15

c)Ley n.º 2012:27816

3.Sobre el período de conservación de los datos17

4.Sobre la protección y la seguridad de los datos conservados18

C –Derecho del Reino Unido19

1.Sobre el alcance de la obligación de conservación20

2.Sobre el acceso a los datos conservados22

3.Sobre el período de conservación de los datos23

4.Sobre la protección y la seguridad de los datos conservados23

II –Litigios principales y cuestiones prejudiciales25

A –Asunto C-203/1525

B –Asunto C-698/1528

III –Procedimiento ante el Tribunal de Justicia30

IV –Análisis de las cuestiones prejudiciales31

A –Sobre la admisibilidad de la segunda cuestión planteada en el asunto C-698/1534

B –Sobre la compatibilidad de una obligación general de conservar datos con el régimen establecido por la Directiva 2002/5838

1.Sobre la inclusión de una obligación general de conservar datos en el ámbito de aplicación de la Directiva 2002/5839

2.Sobre la posibilidad de establecer una excepción al régimen establecido por la Directiva 2002/58 creando una obligación general de conservar datos43

C –Sobre la aplicabilidad de la Carta a una obligación general de conservar datos50

D –Sobre la compatibilidad de una obligación general de conservar datos con los requisitos establecidos por el artículo 15, apartado 1, de la Directiva 2002/58, así como por los artículos 7, 8 y 52, apartado 1, de la Carta53

1.Sobre el requisito de tener una base legal de Derecho nacional57

2.Sobre el respeto del contenido esencial de los derechos reconocidos por los artículos 7 y 8 de la Carta65

3.Sobre la existencia de un objetivo de interés general reconocido por Unión susceptible de justificar una obligación general de conservar datos68

4.Sobre el carácter apropiado de una obligación general de conservar datos en relación con la lucha contra los delitos graves72

5.Sobre el carácter necesario de una obligación general de conservar datos en relación con la lucha contra los delitos graves77

a)Sobre el carácter estrictamente necesario de una obligación general de conservar datos80

b)Sobre el carácter imperativo de las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI en relación con el requisito de estricta necesidad89

6.Sobre el carácter proporcionado, en una sociedad democrática, de una obligación general de conservar datos en relación con el objetivo de lucha contra los delitos graves103

V –Conclusión112

1. En 1788, James Madison, uno de los autores de la Constitución de Estados Unidos, escribía: «If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself». (2)

2. Los presentes asuntos nos sitúan en el núcleo de la «gran dificultad» identificada por Madison. Se refieren a la compatibilidad con el Derecho de la Unión de regímenes nacionales que imponen a los proveedores de servicios de comunicación electrónica accesibles para el público (en lo sucesivo, «proveedores»), una obligación de conservación de los datos relativos a las comunicaciones electrónicas (en lo sucesivo, «datos relativos a las comunicaciones»), referida al conjunto de los medios de comunicación y al conjunto de usuarios (en lo sucesivo, «obligación general de conservar datos»).

3. Por una parte, la conservación de los datos relativos a las comunicaciones permite «al gobierno controlar a los gobernados», brindando a las autoridades competentes un medio de investigación que puede revestir cierta utilidad en la lucha contra delitos graves, en particular, en la lucha contra el terrorismo. En sustancia, la conservación de estos datos dota a las autoridades una capacidad limitada de «leer el pasado», accediendo a los datos relativos a las comunicaciones realizadas por una persona antes de que se sospechara su relación con un delito grave. (3)

4. Sin embargo, por otra parte, es imperativo «obligar [...] al gobierno a que se controle a sí mismo», tanto en lo que se refiere a la conservación, como al acceso a los datos conservados, habida cuenta de los graves riesgos que entraña la existencia de tales bases de datos, que abarcan la totalidad de las comunicaciones realizadas en el territorio nacional. En efecto, esas bases de datos, de considerable tamaño, permiten a cualquier persona que acceda a las mismas catalogar en un instante el conjunto de la población pertinente. (4) Es preciso valorar escrupulosamente estos riesgos, en particular, analizando si una obligación general de conservar datos, como las que son objeto de los litigios principales, es estrictamente necesaria y proporcionada.

5. De este modo, en el marco de los presentes asuntos, el Tribunal de Justicia y los órganos jurisdiccionales remitentes han de definir un punto de equilibrio entre la obligación que corresponde a los Estados miembros de garantizar la seguridad de los individuos que se encuentran en su territorio y el respeto de los derechos fundamentales a la vida privada y a la protección de los datos de carácter personal, consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

6. Examinaré, a la luz de esta «gran dificultad», las cuestiones planteadas al Tribunal de Justicia en los presentes asuntos. Éstas se refieren, más concretamente, a la compatibilidad de los regímenes nacionales que establecen una obligación general de conservar datos con la Directiva 2002/58/CE (5) y con los artículos 7 y 8 de la Carta. Para responder a dichas cuestiones, el Tribunal de Justicia deberá, en particular, perfilar la interpretación que debe darse en un contexto nacional a la sentencia Digital Rights Ireland y otros (en lo sucesivo, «sentencia DRI»), (6) en la que la Gran Sala del Tribunal de

Justicia declaró inválida la Directiva 2006/24/CE. (7)

7. Por los motivos que expondré a continuación, tengo la sensación de que una obligación general de conservar datos impuesta por un Estado miembro puede ser compatible con los derechos fundamentales consagrados por el Derecho de la Unión a condición de estar estrictamente delimitada por una serie de garantías que precisaré a lo largo de mi exposición.

I – Marco jurídico

A – *Directiva 2002/58*

8. El artículo 1 de la Directiva 2002/58, titulado «Objeto y ámbito de aplicación», dispone:

«1. La presente Directiva establece la armonización de las disposiciones nacionales necesaria para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la [Unión].

2. Las disposiciones de la presente Directiva especifican y completan la Directiva [95/46] a los efectos mencionados en el apartado 1. Además, protegen los intereses legítimos de los abonados que sean personas jurídicas.

3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del [TFUE], como las reguladas por las disposiciones de los títulos V y VI del [TUE], ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal.»

9. El artículo 15, apartado 1, de la Directiva 2002/58, intitulé «Aplicación de determinadas disposiciones de la Directiva [95/46]», está así redactado:

«Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva [95/46]. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 [TUE].»

B – *Derecho sueco*

10. La Directiva 2006/24, que ha dejado de tener validez en la actualidad, fue transpuesta al Derecho sueco a través de ciertas modificaciones de la lagen (2003:389) om elektronisk kommunikation (Ley sueca 2003:389 sobre comunicaciones electrónicas; en lo sucesivo, «LEK») y del förordningen (2003:396) om elektronisk kommunikation (Reglamento n.º 2003:396 sobre comunicaciones electrónicas; en lo sucesivo, «FEK»], que entraron en vigor el 1 de mayo de 2012.

1. Sobre el alcance de la obligación de conservación

11. De lo dispuesto en el artículo 16 a del capítulo 6 de la LEK se desprende que los proveedores están obligados a conservar los datos relativos a las comunicaciones necesarios para identificar el

origen y el destino de la comunicación, la fecha, hora y duración de la comunicación, el tipo de comunicación, el equipo de comunicación y la localización del equipo de comunicación móvil al comienzo y el término de la comunicación. Los tipos de datos que deben conservarse se regulan como mayor detalle en los artículos 38 a 43 del FEK.

12. Esta obligación de conservación se refiere a los datos tratados en relación con servicios telefónicos, servicios telefónicos a través de un punto de conexión móvil, transmisión de comunicaciones, acceso a Internet y prestación de capacidad para poder obtener acceso a Internet.

13. Los datos que deben conservarse incluyen no sólo todos los datos cuya conservación imponía la Directiva 2006/24, sino también los relativos a llamadas telefónicas infructuosas así como los relativas a la localización del lugar en que finalice una llamada de teléfono móvil. Al igual que ocurría en el régimen establecido por dicha Directiva, la obligación de conservación no incluye el contenido de las comunicaciones.

2. Sobre el acceso a los datos conservados

14. El acceso a los datos conservados se regula principalmente en tres normas: la LEK, el rättegångsbalken (Código de Procedimiento Judicial; en lo sucesivo, «RB») y la lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Ley sobre Obtención de Datos; en lo sucesivo, «Ley 2012:278»].

a) LEK

15. Del artículo 22, párrafo primero, número 2, del capítulo 6 de la LEK se deriva que los proveedores están obligados a facilitar al Ministerio Fiscal, a los cuerpos de policía, al Säkerhetspolisen (Policía de Seguridad sueca, conocida por «Säpo»; en lo sucesivo, «Säpo») y a cualquier otra autoridad que vaya a actuar contra un delito, a instancia de estos, datos sobre el abono cuando dichos datos tengan relación con la sospecha de comisión de un delito. Con arreglo a dicha disposición, no es necesario que se trate de un delito grave.

16. Se entiende por datos sobre el abono, principalmente, los datos sobre el nombre, título, dirección postal, número y dirección IP del abonado.

17. Con arreglo a la LEK, la cesión de datos sobre el abono no exige ningún control previo, aunque puede ser objeto de un control administrativo posterior. Por otra parte, no se establece un límite al número de autoridades que pueden tener acceso a los datos.

b) RB

18. En el RB se regula la intervención de comunicaciones electrónicas en el contexto de investigaciones preliminares.

19. En síntesis, la intervención las de comunicaciones electrónicas sólo podrá practicarse cuando se sospeche razonablemente que una persona determinada es autora de un delito sancionado con una pena no inferior a seis meses de prisión u otros delitos enumerados específicamente, y si la medida tiene una importancia especial para la investigación.

20. Asimismo, podrá practicarse tal intervención con la finalidad de investigar una infracción sancionada con una pena de prisión de al menos un año con el fin de determinar quién podría ser razonablemente sospechoso de ser el autor, si la medida tiene una importancia especial para la investigación.

21. Con arreglo al artículo 21 del capítulo 27 del RB, con carácter general, el Ministerio Fiscal debe obtener la autorización del juez competente antes de proceder a la intervención de las comunicaciones electrónicas.

22. En caso de riesgo de que la obtención de la autorización judicial para la intervención de la comunicación electrónica suponga una demora o un perjuicio de importancia esencial para la

investigación, la autorización de la medida será concedida por el Ministerio Fiscal a la espera de la resolución del juez. En tales casos, el Ministerio Fiscal notificará la medida por escrito al juez tan pronto como sea posible. A continuación, el juez controlará de modo urgente si existen motivos para la medida.

c) Ley n.º 2012:278

23. Con arreglo al artículo 1 de la Ley 2012:278, la policía nacional, la Säpo y la Tullverket (Administración de Aduanas sueca) podrán, de conformidad con los requisitos establecidos en dicha Ley, obtener datos relativos a las comunicaciones sin conocimiento del proveedor.

24. Conforme a los artículos 2 y 3 de la Ley 2012:278, podrán obtenerse datos cuando, habida cuenta de las circunstancias, la medida sea de especial importancia para prevenir, impedir o detectar actividades delictivas referidas a delitos castigados con una pena no inferior a dos años de prisión o delitos incluidos en la enumeración del artículo 3 (entre otros, diversas formas de sabotaje y espionaje).

25. La decisión de obtener datos es adoptada por el director de la administración de que se trate o por un empleado en el que dicho director haya delegado la facultad de tomar decisiones.

26. En la decisión, se indicará la actividad delictiva y el momento a que se refiere la decisión, así como el número de teléfono, cualquier otra dirección, el equipo de comunicación electrónica o ámbito geográfico a que se refiere la decisión. El período de tiempo al que se refiere la decisión no podrá ser superior al necesario y no podrá, respecto al tiempo posterior a la adopción de la decisión, superar un mes.

27. Para este tipo de obtención de datos no se exige ningún control previo. No obstante, con arreglo al artículo 6 de la Ley 2012:278, la Säkerhets- och integritetsskyddsnämnden (comisión de seguridad y de protección de la integridad, Suecia) deberá ser informada sobre las decisiones de obtención de datos. Conforme al artículo 1 de la lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Ley (2007:980) de control de ciertas actividades de lucha contra la delincuencia), dicho organismo controla la aplicación de la ley realizada por las autoridades encargadas de la lucha contra la delincuencia.

3. Sobre el período de conservación de los datos

28. Conforme al artículo 16d del capítulo 6 de la LEK, los datos a que se refiere el artículo 16a del mismo capítulo deberán conservarse durante seis meses contados a partir del día en que haya finalizado la comunicación. Posteriormente, esos datos deberán ser destruidos lo antes posible, salvo que el párrafo segundo del citado artículo 16d (del capítulo 6) disponga otra cosa. Con arreglo a estas últimas disposiciones, los datos cuya comunicación se hubiera solicitado antes de finalizar el período de conservación, pero que no se hubieran facilitado antes de dicha fecha, deberán destruirse lo antes posible tras su cesión

4. Sobre la protección y la seguridad de los datos conservados

29. El artículo 20, apartado 1, del capítulo 6 de la LEK prohíbe la difusión o utilización no autorizada de la información relativa a las comunicaciones.

30. Conforme a lo dispuesto en el artículo 3a del capítulo 6 de la LEK, los proveedores están obligados a adoptar las medidas técnicas y organizativas necesarias para proteger los datos conservados en caso de tratamiento. De los trabajos preparatorios de estas disposiciones se desprende que no se ha dejado margen para que se determine el nivel de protección mediante una ponderación de consideraciones técnicas, de los costes y de los riesgos de piratería y de injerencia en la intimidad de las personas.

31. El artículo 37 FEK establece otras disposiciones sobre protección de datos, al igual las instrucciones y directrices generales de la Post- och telestyrelsen (autoridad sueca de vigilancia del correo y de las telecomunicaciones; en lo sucesivo, «PTS») sobre medidas de seguridad en relación con

la conservación y tratamiento de datos con la finalidad de lucha contra la delincuencia (PTSFS n.º 2012:4). De las citadas disposiciones, se desprende, en particular, que los proveedores deberán adoptar medidas para proteger los datos de la destrucción accidental o ilícita, del almacenamiento, tratamiento y acceso o divulgación no autorizados. Los proveedores deberán desarrollar también una actividad de seguridad continuada y sistemática teniendo en cuenta los riesgos especiales que conlleva la obligación de conservación.

32. El Derecho sueco no prevé normas que regulen el lugar en el que deben conservarse los datos.

33. Con arreglo al capítulo 7 de la LEK, las autoridades de control pueden, en el caso de que un proveedor incumpla sus obligaciones, dirigirle órdenes y prohibiciones, que podrán ir acompañadas de multas, así como ordenar que cese toda actividad o una parte de la misma.

C – *Derecho del Reino Unido*

34. Las disposiciones sobre la conservación de los datos se encuentran en la Data Retention and Investigatory Powers Act 2014 (Ley de 2014 sobre conservación de datos y poderes de investigación; en lo sucesivo, «DRIPA»), en el Data Retention Regulations 2014 (SI 2014/2042) [Reglamento de 2014 sobre conservación de datos 2014 (SI 2014/2042; en lo sucesivo, «Reglamento de 2014»], así como en el Retention of Comunicaciones [Data] Code of Practice (Código de Buenas Prácticas en materia de Conservación de [Datos]); en lo sucesivo, «Código de Conservación de Datos»).

35. El acceso a los datos aparece regulado en el capítulo 2 de la parte 1 de la Regulation of Investigatory Powers Act 2000 (Ley de 2000 de regulación de las facultades de investigación; en lo sucesivo, «RIPA»), en el Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480)] [Decreto de 2010 sobre regulación de las facultades de investigación en materia de datos relativos a las comunicaciones (SI 2010/480)], en su versión modificada por el Regulation of Investigatory Powers (Communications Data) (Amendement) Order 2015 (SI 2015/228) [Decreto de 2015 sobre regulación de las facultades de investigación en materia de datos relativos a las comunicaciones (Enmienda) (en lo sucesivo, «Decreto»), así como en el Acquisition and Disclosure of Comunicaciones Data Code of Practice (Código de buenas prácticas relativo a la obtención y divulgación de datos sobre comunicaciones; en lo sucesivo, «Código sobre Obtención de Datos»).

1. Sobre el alcance de la obligación de conservación

36. Con arreglo al artículo 1 de la DRIPA, el Ministro puede imponer a los proveedores una obligación de conservar todos los datos relativos a las comunicaciones. Esta obligación puede afectar, fundamentalmente, al conjunto de datos generados con ocasión de una comunicación realizada a través de un servicio postal o de un sistema de telecomunicación, a excepción del propio contenido de la comunicación. Estos datos incluyen, en particular, la ubicación del usuario del servicio, así como los datos que permitan identificar la IP (dirección de protocolo de internet) u otro identificador perteneciente al remitente o destinatario de una comunicación.

37. Entre los fines que pueden justificar la adopción de tal medida de conservación se incluyen la seguridad nacional, impedir o detectar la comisión de delitos o de impedir desórdenes, el bienestar económico del Reino Unido, en la medida en que tal interés sea igualmente relevante para los intereses de la seguridad nacional, la seguridad pública, proteger la salud pública, liquidar o recaudar cualquier impuesto, contribución u otra cantidad pagadera a la administración pública, impedir, en caso de emergencia, cualquier daño para la salud física o mental, prestar ayuda en investigaciones de errores judiciales, identificar a personas fallecidas o que no sean capaces de identificarse a sí mismas por causas que no sean la comisión de un delito (como, por ejemplo, un desastre natural o un accidente), desempeñar funciones relativas a la regulación de los servicios y mercados financieros o a la estabilidad financiera así como cualquier otro objetivo especificado en una orden adoptada por el Ministro en virtud del artículo 22, apartado 2, de la DRIPA.

38. En la legislación nacional no se exige que la expedición de una notificación de conservación esté sujeta a la autorización previa de un órgano jurisdiccional o de un organismo administrativo autónomo. El Ministro debe comprobar que la obligación de conservación sea «necesaria y proporcionada» a efectos de uno o varios de los fines por los que pueden conservarse los datos de

comunicaciones relevantes.

2. Sobre el acceso a los datos conservados

39. En virtud del artículo 22, apartado 4, de la RIPA, las autoridades públicas podrán exigir, mediante notificación, a los proveedores que les entreguen datos de comunicaciones. La forma y el contenido de estas notificaciones se regula en el artículo 23, apartado 2, de la RIPA. La vigencia de estas notificaciones está limitada en virtud de disposiciones sobre cancelación y renovación.

40. La obtención de datos de comunicaciones deberá ser necesaria y proporcionada para uno o más de los fines establecidos en el artículo 22 de la RIPA, que se corresponden con los objetivos que pueden justificar la conservación de los datos descritos en el punto 37 de las presentes conclusiones.

41. Del Código sobre Obtención de Datos se desprende que se exigirá una orden judicial, en concreto, cuando se soliciten datos de comunicaciones para identificar las fuentes de periodistas así como cuando sean las autoridades locales las que formulen la solicitud de acceso.

42. Fuera de esos casos, el acceso de las autoridades está supeditado a la obtención de una autorización de las personas designadas de la autoridad pública pertinente. Una persona designada es una persona que ocupa un cargo, rango o posición prescrito en el seno de una autoridad pública pertinente que ha sido designada en el Decreto de 2015 sobre regulación de las facultades de investigación en materia de datos relativos a las comunicaciones, en su versión modificada.

43. No se exigirá ninguna autorización judicial o de un órgano independiente para acceder a datos de comunicaciones sujetos al secreto entre un abogado y su cliente ni a datos de comunicaciones relativos a médicos, miembros del Parlamento o ministros de cultos religiosos. El Código sobre Obtención de Datos sólo precisa que debe atribuirse particular importancia a la necesidad y a la proporcionalidad de la solicitud.

3. Sobre el período de conservación de los datos

44. El artículo 1, apartado 5, de la DRIPA y el artículo 4, apartado 2, del Reglamento de 2014 establecen un período máximo de conservación de datos de 12 meses. Según el Código de Conservación de Datos, dicho período tendrá únicamente la duración necesaria y deberá ser proporcionado. El artículo 6 del Reglamento de 2014 exige al ministro que someta a revisión las notificaciones de conservación.

4. Sobre la protección y la seguridad de los datos conservados

45. En virtud del artículo 1 de la DRIPA, los proveedores no podrán comunicar los datos conservados excepto de conformidad con el capítulo 2 de la parte 1 de la RIPA, una orden de un tribunal o cualquier otra autorización o mandamiento judicial, o lo previsto en reglamento adoptado por el Ministro con arreglo al artículo 1 de la DRIPA.

46. Con arreglo a lo dispuesto en los artículos 7 y 8 del Reglamento de 2014, los proveedores deberán garantizar su integridad y seguridad; protegerlos de una destrucción accidental o ilegal, pérdida o modificación accidental o de una conservación, procesamiento, acceso o divulgación no autorizada o ilícita; destruir los datos para hacer imposible el acceso si la conservación de los datos deja de estar autorizada, y establecer sistemas de seguridad adecuados. Lo dispuesto en el artículo 9 del Reglamento de 2014 impone al Information Commissioner (Comisario de Información) la obligación de examinar el cumplimiento de estas obligaciones por parte de los proveedores.

47. Las autoridades a las que los proveedores comunican datos relativos a las comunicaciones deben tratar y almacenar dichos datos, así como todas las copias, extractos o resúmenes de los mismos en condiciones de seguridad. Con arreglo al Código sobre Obtención de Datos, deben respetarse los requisitos establecidos en la Data Protection Act (Ley de Protección de Datos; en lo sucesivo, «DPA»), que transpuso la Directiva 95/46.

48. La RIPA prevé la existencia de un Interception of Comunications Commissioner (Comisario

para la Interceptación de Comunicaciones; en lo sucesivo, «Comisario para la Interceptación de Comunicaciones») cuya función consiste en supervisar con carácter independiente el ejercicio y el cumplimiento de las facultades y deberes establecidos en el capítulo II de la parte I de la RIPA. Este Comisario no supervisa la aplicación del artículo 1 de la DRIPA. Se prevé la publicación de informes y su entrega al Parlamento (artículos 57, apartado 2, y 58 de la RIPA). Tiene la obligación de elaborar regularmente informes dirigidos al público y al Parlamento (artículos 57, apartado 2, y 58 del RIPA) y llevar un registro de los datos conservados por las autoridades públicas y de los informes elaborados por éstas (artículos 6.1 a 6.8 del Código sobre Obtención de Datos Pueden presentarse reclamaciones ante el Investigatory Powers Tribunal (Tribunal encargado de los poderes de investigación) si se cree que los datos han sido obtenidos de forma inadecuada (artículo 65 de la RIPA).

49. A tenor del Código sobre Obtención de Datos, el Comisario no está facultado para someter un asunto a ese Tribunal. Únicamente puede informar a una persona de un supuesto uso ilícito de facultades si puede «demostrar que una persona ha resultado negativamente afectada por un incumplimiento intencionado o negligente». Sin embargo, el Comisario no podrá comunicar su existencia cuando ello ponga en riesgo la seguridad nacional aun cuando el Comisario tenga la convicción de que se ha cometido un incumplimiento intencionado o negligente.

II – Litigios principales y cuestiones prejudiciales

A – *Asunto C-203/15*

50. El día 9 de abril de 2014, es decir, al día siguiente de que se dictara la sentencia DRI, Tele2 Sverige envió un escrito a PTS comunicándole que iba a dejar de conservar datos con arreglo al capítulo 6 de la LEK. Tele2 Sverige también iba a proceder a eliminar los datos conservados anteriormente con arreglo a dicho capítulo. Tele2 Sverige consideraba que la normativa sueca de transposición de la Directiva 2006/24 no era conforme a la Carta.

51. El 15 de abril de 2014, la Rikspolisstyrelsen (Dirección General de la Policía Nacional; en lo sucesivo, «RPS») presentó una queja ante PTS denunciando que Tele2 Sverige había dejado de comunicarle datos relativos a determinadas comunicaciones electrónicas. En su queja, la RPS alegaba que la negativa Tele2 Sverige tenía graves consecuencias para el trabajo de la policía en esta materia.

52. Mediante orden de 27 de junio de 2014, PTS ordenó a Tele2 Sverige que, a más tardar el 25 de julio de 2014, volviera a conservar datos con arreglo al artículo 16a del capítulo 6 de la LEK y a los artículo 37 a 43 del FEK.

53. Tele2 Sverige recurrió la decisión de PTS ante el Förvaltningsrätten i Stockholm [Tribunal de Primera Instancia de lo Contencioso-Administrativo de Estocolmo]. Dicho Tribunal desestimó el recurso mediante sentencia de 13 de octubre de 2014.

54. Tele2 Sverige presentó un recurso de apelación contra la sentencia del Förvaltningsrätten i Stockholm [Tribunal de Primera Instancia de lo Contencioso-Administrativo de Estocolmo] ante el órgano jurisdiccional remitente solicitando la anulación de la resolución recurrida.

55. El Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo), al considerar que existían motivos tanto a favor como en contra de considerar que una obligación de conservación de tal amplitud como la establecida en el artículo 16a del capítulo 6 de la LEK es compatible con el artículo 15, apartado 1, de la Directiva 2002/58, con los artículos 7, 8 y 52, apartado 1, de la Carta, resolvió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) Una obligación general de conservar datos de tráfico que se refiere a todas las personas, todos los medios de comunicación electrónica y todos los datos de tráfico sin establecer ninguna distinción, limitación o excepción en función del objetivo de la lucha contra la delincuencia [como se describe en los apartados 13 a 18 de la resolución de remisión], ¿es compatible con el artículo 15, apartado 1, de la Directiva 2002/58/CE habida cuenta de los artículos 7, 8 y 52, apartado 1, de la Carta?

2) En caso de respuesta negativa a la primera cuestión, ¿puede en todo caso ser admisible la conservación:

a) si el acceso de las autoridades nacionales a los datos conservados se determina como [se describe en los apartados 19 a 36 de la resolución de remisión], y

b) si las exigencias de protección y de seguridad se regulan como [se describe en los apartados 38 a 43 de la resolución de remisión], y

c) si todos los datos de que se trata deben conservarse durante seis meses contados a partir del día en que haya finalizado la comunicación y posteriormente destruirse como [se describe en el apartado 37 de la resolución de remisión]?»

B – *Asunto C-698/15*

56. Los Sres. Tom Watson, Peter Brice y Goofrey Lewis interpusieron ante la High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) [Tribunal Superior de Justicia (Inglaterra y País de Gales), (Sección de lo Contencioso-Administrativo)] recursos contecioso-administrtativos («judicial review») contra la normativa sobre conservación de datos establecida en el artículo 1 de la DRIPA, por la que se faculta al Ministro del Interior a imponer a los operadores de telecomunicaciones públicos la obligación de conservar todos los dato relativos a comunicaciones por un periodo máximo de doce meses, excluyéndose el propio contenido de las comunicaciones de que se trate.

57. Se autorizó a Open Rights Group, Privacy Internacional y a la Law Society of England and Wales a intervenir en todos los procedimientos.

58. Mediante sentencia de 17 de julio de 2015, dicho órgano jurisdiccional declaró que tal normativa era contraria al Derecho de la Unión al no cumplir los requisitos establecidos en la sentencia DRI, que consideraba aplicables a las normativas de los Estados miembros en materia de conservación de datos relativos a comunicaciones electrónicas y al acceso a tales datos. El Ministro del Interior recurrió en apelación dicha sentencia ante el órgano jurisdiccional remitente.

59. Mediante sentencia de 20 noviembre 2015, la Court of Appeal declaró, con carácter provisional, que la sentencia DRI no había determinado requisitos imperativos específicos de Derecho de la Unión, de obligado cumplimiento por las legislaciones nacionales, sino que se había limitado a determinar y describir medios de protección no previstos en la normativa armonizada de la Unión.

60. Sin embargo, al considerar que las respuestas a dichas cuestiones de Derecho de la Unión Europea no están claras y que eran necesarias para dictar sentencia en esos procedimientos, la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil) (Reino Unido)] resolvió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1. ¿Determina la sentencia [DRI] (en particular, en sus apartados 60 a 62), requisitos imperativos de Derecho de la Unión que resulten aplicables al régimen nacional de un Estado miembro que regule el acceso a datos conservados de conformidad con la legislación nacional, al objeto de dar cumplimiento a los artículos 7 y 8 de la [Carta]?

2. ¿Amplía la sentencia [DRI] el alcance de los artículos 7 y/u 8 de la Carta más allá del ámbito de aplicación del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales ("CEDH"), consagrado en la jurisprudencia del Tribunal Europeo de Derechos Humanos ("TEDH")?»

III – Procedimiento ante el Tribunal de Justicia

61. Las peticiones de decisión prejudicial fueron registradas en la Secretaría del Tribunal de Justicia el 4 de mayo de 2015, en el asunto C-203/15, y el 28 de diciembre de 2015, en el asunto C-698/15.

62. Mediante auto de 1 de febrero de 2016, el Tribunal de Justicia acordó tramitar el asunto C-698/15 por el procedimiento acelerado establecido en el artículo 105, apartado 1, del Reglamento de Procedimiento del Tribunal de Justicia.

63. En el asunto C-203/15, Tele2 Sverige, los Gobiernos checo, danés, alemán, estonio, irlandés, español, húngaro, neerlandés, sueco y del Reino Unido y la Comisión Europea han presentado observaciones escritas.

64. En el asunto C-698/15, los Sres. Watson, Brice y Lewis, Open Rights Group, Privacy International, la Law Society of England and Wales, los Gobiernos checo, danés, alemán estonio, irlandés, francés, chipriota, polaco, finlandés y del Reino Unido y la Comisión han presentado observaciones escritas.

65. Mediante resolución de 10 de marzo de 2016, el Tribunal de Justicia ordenó acumular los dos asuntos a efectos de la fase oral y de la sentencia.

66. A la vista oral, celebrada el 12 de abril de 2016 comparecieron para presentar sus observaciones los representantes de Tele2 Sverige, los Sres. Watson, Brice y Lewis, Open Rights Group, Privacy Internacional y la Law Society of England and Wales, los Gobiernos checo, danés, alemán estonio, irlandés, español, francés, finlandés, sueco y del Reino Unido y la Comisión.

IV – Análisis de las cuestiones prejudiciales

67. Mediante la primera cuestión prejudicial planteada en el asunto C-203/15, el órgano jurisdiccional remitente pregunta al Tribunal de Justicia si, a la luz de la sentencia DRI, el artículo 15, apartado 1, de la Directiva 2002/58, así como los artículos 7, 8 y 52, apartado 1, de la Carta han de interpretarse en el sentido de que se oponen a que un Estado miembro imponga a los proveedores una obligación general de conservar datos, como la obligación de la que se trata en los litigios principales, y ello con independencia de las garantías que lleve aparejadas tal obligación.

68. En el supuesto de que esta cuestión deba recibir una respuesta negativa, la segunda cuestión planteada en el asunto C-203/15 y la primera cuestión planteada en el asunto C-698/15 van dirigidas a determinar si dichas disposiciones han de interpretarse en el sentido de que se oponen a que un Estado miembro imponga a los proveedores una obligación general de conservar datos cuando tal obligación no lleve aparejado el conjunto de garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI en relación con el acceso a los datos, el período de conservación así como la protección y seguridad de los datos.

69. En la medida en que las tres cuestiones van íntimamente ligadas, las examinaré conjuntamente en mi exposición.

70. En cambio, la segunda cuestión planteada en el asunto C-698/15 requiere un tratamiento separado. Mediante dicha cuestión, el órgano jurisdiccional remitente pregunta al Tribunal de Justicia si la sentencia DRI ha extendido el ámbito de aplicación de los artículos 7 y/o 8 de la Carta más allá del artículo 8 del CEDH. En la sección siguiente, expondré los motivos por los que considero que dicha cuestión ha de desestimarse por inadmisible.

71. Antes de acometer el examen de dichas cuestiones, considero útil recordar a qué tipo de datos se refieren las obligaciones de conservación de que se trata en los litigios principales. A tenor de lo expuesto por los órganos jurisdiccionales remitentes, el alcance de dichas obligaciones es, en lo esencial, equivalente al de la obligación que establecía el artículo 5 de la Directiva 2006/24. (8) De forma esquemática, los datos relativos a las comunicaciones que son objeto de tales obligaciones de conservación pueden clasificarse en cuatro categorías: (9)

– los datos que permiten identificar tanto el origen de la comunicación como su destino;

– los datos que permiten localizar tanto el origen como el destino de la comunicación;

– los datos relativos a la fecha, hora y duración de la comunicación, y

– los datos que permitan determinar en tipo de comunicación y el tipo de material utilizado.

72. El contenido de las comunicaciones queda excluido de las obligaciones generales de conservación de datos de que se trata en los asuntos principales, a ejemplo de lo que establecía el artículo 5, apartado 2, de la Directiva 2006/24.

A – *Sobre la admisibilidad de la segunda cuestión planteada en el asunto C-698/15*

73. Con la segunda cuestión planteada en el asunto C-698/15 se solicita al Tribunal de Justicia que aclare si la sentencia DRI extiende el ámbito de aplicación de los artículos 7 y/u 8 de la Carta más allá del artículo 8 del CEDH en la interpretación que recibe del TEDH.

74. Esta cuestión refleja, en particular, un argumento invocado por el Secretary of State for the Home Department (Ministro del Interior) ante el órgano jurisdiccional remitente, según el cual la jurisprudencia del TEDH no exige, por una parte, que el acceso a los datos esté supeditado a la previa autorización de un órgano administrativo independiente ni, por otra parte, que la conservación y el acceso a los mismos deba circunscribirse al ámbito de la lucha contra delitos graves.

75. Considero que esta cuestión ha de declararse inadmisible por los siguientes motivos. Es evidente que los fundamentos y las soluciones adoptados por el Tribunal de Justicia en la sentencia DRI revisten una importancia determinante para dirimir los litigios principales. Sin embargo la cuestión de si dicha sentencia pudo ampliar el ámbito de aplicación de los artículos 7 y/u 8 de la Carta más allá del artículo 8 del CEDH no es pertinente, de por sí, para resolver dichos litigios.

76. A este respecto, es preciso recordar que, con arreglo al artículo 6 TUE, apartado 3, los derechos fundamentales que garantiza el CEDH forman parte del Derecho de la Unión como principios generales. Sin embargo, al no haberse adherido la Unión a dicho Convenio, el mismo no constituye un instrumento jurídico integrado formalmente en el ordenamiento jurídico de la Unión. (10)

77. Ciertamente, la primera frase del artículo 52, apartado 3, de la Carta establece una pauta de interpretación según el cual, en la medida en que la Carta contenga derechos que correspondan a derechos garantizados por el CEDH, «su sentido y alcance serán iguales a los que les confiere dicho Convenio».

78. Sin embargo, a tenor de la segunda frase del artículo 52, apartado 3, de la Carta, «esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa». En mi opinión, de esta frase se desprende que, si lo considera necesario en el ámbito del Derecho de la Unión, el Tribunal de Justicia puede extender el ámbito de aplicación de las disposiciones de la Carta más allá del de las disposiciones correlativas del CEDH.

79. Debo añadir, con carácter subsidiario, que el artículo 8 de la Carta, interpretado por el Tribunal de Justicia en la sentencia DRI, crea un derecho que no se corresponde con ningún derecho garantizado por el CEDH, a saber el derecho a la protección de los datos personales, lo que, por otra parte corroboran las explicaciones relativas al artículo 52 de la Carta. (11) Por lo tanto, la pauta de interpretación establecida en el artículo 52, apartado 3, primera frase, de la Carta no es, en ningún caso, aplicable a interpretación del artículo 8 de la Carta, como señalaron los Sres. Brice y Lewis, Open Rights Group y Privacy International, la Law Society of England and Wales, así como los Gobiernos checo, irlandés y finlandés.

80. De lo anterior se infiere que el Derecho de la Unión no se opone a que los artículos 7 y 8 de la Carta confieran una protección más amplia que la prevista en el CEDH. Por lo tanto, el hecho de que la sentencia DRI haya podido ampliar el ámbito de aplicación de dichas disposiciones de la Carta más allá del artículo 8 del CEDH no es, en sí mismo, relevante a efectos de la resolución de los litigios principales. La solución que haya de darse a dichos litigios depende fundamentalmente de los requisitos necesarios para que obligación general de conservar datos pueda considerarse compatible con el artículo 15, apartado 1, de la Directiva 2002/58, así como con los artículos 7, 8 y 52, apartado 1,

de la Carta, interpretados a la luz de la sentencia DRI, extremo que, precisamente, es el objeto de las otras tres cuestiones planteadas en los presentes asuntos.

81. Según reiterada jurisprudencia, la negativa a pronunciarse sobre una cuestión planteada por un órgano jurisdiccional nacional sólo es posible cuando resulta patente que la interpretación solicitada del Derecho de la Unión no tiene relación alguna con la realidad o con el objeto del litigio principal o también cuando el problema es de naturaleza hipotética o cuando el Tribunal de Justicia no dispone de los elementos de hecho o de Derecho necesarios para responder eficazmente a las cuestiones planteadas. (12)

82. En el presente asunto, y por los motivos antes expuestos, considero que segunda cuestión planteada en el asunto C-698/15 reviste únicamente un interés teórico, dado que una eventual respuesta a la misma no permitiría obtener elementos interpretativos del Derecho de la Unión que el órgano jurisdiccional remitente pudiera aplicar útilmente para resolver, en función de dicho Derecho, el litigio pendiente ante él. (13)

83. En estas circunstancias, estimo que dicha cuestión ha de declararse inadmisible como señalaron, con razón, el Sr. Watson, la Law Society of England and Wales y el Gobierno checo.

B – *Sobre la compatibilidad de una obligación general de conservar datos con el régimen establecido por la Directiva 2002/58*

84. El presente apartado trata de la posibilidad de que los Estados miembros puedan hacer uso de la facultad ofrecida por el artículo 15, apartado 1, de la Directiva 2002/58 a efectos de imponer una obligación general de conservar datos. En cambio, no se examina en él los requisitos particulares que deben cumplir los Estados miembros que deseen hacer uso de esta facultad. Dichos requisitos serán analizados ampliamente más adelante. (14)

85. En efecto, Open Rights Group y Privacy International han alegado que tal obligación resulta incompatible con el régimen armonizado establecido por la Directiva 2002/58, y ello con independencia de que se cumplan los requisitos establecidos en el artículo 15, apartado 1, de la Directiva 2002/58, en razón de que reduce a la nada lo esencial de los derechos y del régimen establecidos en dicha Directiva.

86. Antes de examinar este argumento, es preciso determinar si una obligación general de conservar datos está incluida en el ámbito de aplicación de dicha Directiva.

1. Sobre la inclusión de una obligación general de conservar datos en el ámbito de aplicación de la Directiva 2002/58

87. Ninguna de las partes que ha presentado observaciones ante Tribunal de Justicia ha puesto en duda el hecho de que una obligación general de conservar datos, como la que es objeto de los litigios principales, es subsumible en el concepto de «tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la [Unión]», en el sentido del artículo 3 de la Directiva 2002/58.

88. Sin embargo, los Gobiernos checo, francés, polaco y del Reino Unido han alegado que una obligación general de conservar datos está comprendida en la exclusión establecida en el artículo 1, apartado 3, de la Directiva 2002/58. Consideran, por una parte, que las disposiciones nacionales que regulan el acceso a los datos y la explotación de éstos por parte de las autoridades policiales o judiciales de los Estados miembros afectan a la seguridad pública, a la defensa o a la seguridad del Estado o, cuando menos, tendrían que ver con la materia penal. Añaden, por otra parte, que la única finalidad de la conservación de los datos sería permitir a dichas autoridades policiales o judiciales el acceso a los mismos y su explotación. Concluyen que la obligación de conservación de los datos queda excluida del ámbito de aplicación de dicha Directiva con arreglo a la citada disposición.

89. Este razonamiento no consigue convencerme por las siguientes razones.

90. En primer lugar, la redacción del artículo 15, apartado 1, de la Directiva 2002/58 confirma que

las obligaciones de conservación impuestas por los Estados miembros están incluidas en el ámbito de aplicación de dicha Directiva. En efecto, a tenor de dicha disposición, «los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado». Me parece, cuando menos, difícil sostener que las obligaciones de conservación estén excluidas del ámbito de aplicación de dicha Directiva cuando su propio artículo 15, apartado 1, regula la facultad de adoptar tales obligaciones.

91. En realidad, como han alegado el Sr. Watson, los Sres. Brice y Lewis, los Gobiernos belga, danés, alemán, finlandés, así como la Comisión, una obligación general de conservar datos, como la que es objeto de los litigios principales, no hace sino aplicar el artículo 15, apartado 1, de la Directiva 2002/58.

92. En segundo lugar, el hecho de que las disposiciones que regulan el acceso puedan estar contempladas en la exclusión establecida en el artículo 1, apartado 3, de la Directiva 2002/58 (15) no implica que la obligación de conservación también lo esté y se sitúe, por tanto, fuera del ámbito de aplicación de dicha Directiva.

93. Sobre esta cuestión, el Tribunal de Justicia ya tuvo la oportunidad de aclarar que las actividades citadas en el primer guión del artículo 3, apartado 2, de la Directiva 95/46/CE, (16) cuya redacción tiene un contenido equivalente a la del artículo 1, apartado 3, de la Directiva 2002/58, eran actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares. (17)

94. Pues bien, las obligaciones de conservación de que se trata en los litigios principales son impuestas a operadores privados en el marco de actividades privadas de prestación de servicios de comunicación electrónica, como señaló la Comisión. Además, dichas obligaciones se imponen con independencia de que se cursen solicitudes de acceso por parte de autoridades policiales o judiciales, así como, más en general, de cualquier acto de las autoridades estatales en relación con la seguridad pública, la defensa, la seguridad del Estado o el Derecho penal.

95. En tercer lugar, la solución adoptada por el Tribunal de Justicia en la sentencia Irlanda/Parlamento y Consejo confirma que una obligación general de conservar datos no está comprendida en la materia penal. (18) En efecto, el Tribunal de Justicia consideró que la Directiva 2006/24, que establecía tal obligación, no estaba comprendida en el ámbito penal, sino que tenía que ver con el funcionamiento del mercado interior, de manera que el artículo 95 CE (convertido en el artículo 114 TFUE) constituía la base jurídica apropiada para la adopción de dicha Directiva.

96. Para llegar a tal conclusión, el Tribunal de Justicia constató, en particular, que las disposiciones de dicha Directiva se limitaban en esencia a las actividades de los prestadores de servicios y no regulaban el acceso a los datos ni la explotación de éstos por las autoridades policiales o judiciales de los Estados miembros. (19) De ello deduzco que unas disposiciones de Derecho nacionales que establezcan una obligación de conservación similar a la prevista por la Directiva 2006/24 tampoco se sitúan en el ámbito penal.

97. A la vista de lo que antecede, soy de la opinión de que una obligación general de conservar datos no está comprendida en la exclusión contemplada en el artículo 1, apartado 3, de la Directiva 2002/58 y, por lo tanto, está comprendida en el ámbito de aplicación de dicha Directiva.

2. Sobre la posibilidad de establecer una excepción al régimen establecido por la Directiva 2002/58 creando una obligación general de conservar datos

98. Procede determinar si una obligación general de conservar datos es compatible con el régimen establecido por la Directiva 2002/58.

99. La cuestión que se plantea a este respecto es si un Estado miembro puede hacer uso de la facultad ofrecida por el artículo 15, apartado 1, de la Directiva 2002/58 con vistas a imponer tal obligación.

100. Son cuatro los argumentos aducidos contra tal posibilidad, en particular, por Open Rights Group y

Privacy International.

101. Según un primer argumento, conceder a los Estados miembros la facultad de imponer una obligación general de conservar datos comprometería el objetivo de armonización que constituye la razón de ser de la Directiva 2002/58. Según su artículo 1, apartado 1, dicha Directiva establece, en efecto, una armonización de las disposiciones nacionales necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y a la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como a la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Unión.

102. Por ello, no cabe interpretar que el artículo 15, apartado 1, de la Directiva 2002/58 conceda a los Estados miembros la facultad de establecer una excepción al régimen establecido por dicha Directiva de tal amplitud que prive de efecto útil a estos esfuerzos de armonización.

103. De acuerdo con un segundo argumento, la redacción del artículo 15, apartado 1, de la Directiva 2002/58 también se opone a una interpretación tan extensa de la facultad de los Estados miembros de establecer excepciones al régimen establecido por dicha Directiva. En efecto, a tenor de dicha disposición, «los Estados miembros podrán adoptar medidas legales para *limitar el alcance* de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de [dicha] Directiva» (el subrayado es mío).

104. Pues bien, según el mismo argumento, tal obligación general de conservar datos no se contenta con «limitar el alcance» de los derechos y de las obligaciones mencionados en dicha disposición, sino que reduce a la nada tales derechos y obligaciones. Así ocurriría con:

– la obligación de garantizar la confidencialidad de los datos de tráfico y la obligación de supeditar el almacenamiento de información al consentimiento del usuario previstas, respectivamente, en los apartados 1 y 3 del artículo 5 de la Directiva 2002/58;

– la obligación de eliminar o hacer anónimos los datos de tráfico, prescrita en el artículo 6, apartado 1, de dicha Directiva, y

– la obligación de hacer anónimos los datos de localización o de obtener el consentimiento del usuario para tratar tales datos, impuesta por el artículo 9, apartado 1, de dicha Directiva.

105. Considero que estos dos primeros argumentos deben desestimarse por los siguientes motivos.

106. De una parte, la redacción del artículo 15, apartado 1, de la Directiva 2002/58 menciona la posibilidad de que los Estados miembros adopten «medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado». Esta referencia explícita a las obligaciones de conservación de datos confirma que tales obligaciones no son, en sí mismas, incompatibles con el régimen establecido por la Directiva 2002/58. Si bien es cierto que esta formulación no contempla expresamente la posibilidad de establecer una obligación *general* de conservar datos, ha de reconocerse que tampoco se opone a la misma.

107. Por otra parte, el considerando 11 de la Directiva 2002/58 precisa que la misma no altera «el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de [dicha] Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal». En consecuencia, «[dicha] Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el [CEDH]».

108. En mi opinión, de este considerando 11 se desprende que la intención del legislador de la Unión no era menoscabar la facultad de los Estados miembros para adoptar las medidas contempladas en el artículo 15, apartado 1, de la Directiva 2002/58, sino sujetar tal facultad a las exigencias referidas,

especialmente, al fin que se pretenda alcanzar y a la proporcionalidad de dichas medidas. En otros términos, una obligación general de conservar datos no es, en mi opinión, incompatible con el régimen establecido por dicha Directiva, siempre y cuando cumpla determinados requisitos.

109. Según un tercer argumento, el artículo 15, apartado 1, de la Directiva 2002/58 debiera, en tanto en cuanto constituye una excepción al régimen establecido por Directiva, ser objeto de una interpretación estricta, y ello, en virtud de una regla interpretativa que resulta de la reiterada jurisprudencia del Tribunal de Justicia. Según el mismo argumento, esta regla de interpretación estricta prohíbe interpretar dicha disposición en el sentido de que ofrece la posibilidad de imponer una obligación general de conservar datos.

110. En este sentido, mi impresión es que la facultad a que se refiere el artículo 15, apartado 1, de la Directiva 2002/58 no puede calificarse de excepción ni puede, por consiguiente, ser interpretada estrictamente, como ha alegado, con razón, la Comisión. En efecto, me parece difícil calificar de excepción tal facultad a la luz del considerando 11, antes citado, según el cual dicha Directiva no afecta a la capacidad de los Estados miembros para adoptar las medidas contempladas en dicha disposición. Por lo demás, debo señalar que el artículo 15 de dicha Directiva se titula «Aplicación de determinadas disposiciones de la Directiva 95/46», mientras que el artículo 10 de esa misma Directiva se titula expresamente «Excepciones». Estos títulos me confirman en la idea de que la facultad contemplada en el citado artículo 15 no puede calificarse de «excepción».

111. Según un cuarto y último argumento, la incompatibilidad de una obligación general de conservar datos con el régimen establecido por la Directiva 2002/58 viene corroborada por el hecho de que el apartado 1 *bis* se añadió al artículo 15 de dicha Directiva cuando se adoptó la Directiva 2006/24, invalidada por la sentencia DRI. En virtud de dicho argumento, esa incompatibilidad fue la que llevó al legislador de la Unión a declarar que el artículo 15, apartado 1, de la Directiva 2002/58 no es aplicable al régimen general de conservación establecido en la Directiva 2006/24.

112. Considero que este argumento obedece a una deficiente comprensión del alcance del artículo 15, apartado 1 *bis*, de la Directiva 2002/58. Con arreglo a dicha disposición, «[el artículo 15, apartado 1, de la Directiva 2002/58] no se aplicará a los datos que deben conservarse específicamente de conformidad con la Directiva [2006/24] para los fines recogidos en el artículo 1, apartado 1, de dicha Directiva».

113. La lectura que hago de dicha disposición es la siguiente. Por lo que se refiere a los datos cuya conservación venía exigida por la Directiva 2006/24, y a efectos establecidos por ésta, los Estados miembros perdían la facultad contemplada en el artículo 15, apartado 1, de la Directiva 2002/58 de limitar aún más el contenido de los derechos y de las obligaciones contemplados en dicha disposición, en particular, a través de obligaciones complementarias en materia de conservación de datos. En otros términos, el artículo 15, apartado 1 *bis*, contemplaba una armonización exhaustiva en lo relativo a los datos cuya conservación venía exigida por la Directiva 2006/24, y a los efectos establecidos por ésta.

114. A mi juicio, confirma esta interpretación el considerando 12 de la Directiva 2006/24, a cuyo tenor, «el artículo 15, apartado 1, de la Directiva [2002/58] *sigue aplicándose* a los datos, incluidos los datos relativos a las llamadas telefónicas infructuosas, cuya conservación no se prescribe específicamente en la presente Directiva y *que, por consiguiente, quedan fuera del ámbito de aplicación de la misma*, así como la conservación a efectos, incluidos judiciales, *diferentes de los contemplados en la presente Directiva*» (el subrayado es mío).

115. De esta manera, la inserción del artículo 15, apartado 1 *bis*, de la Directiva 2002/58 no demuestra la incompatibilidad de una obligación general de conservar datos con el régimen establecido por dicha Directiva, sino la voluntad del legislador de la Unión de proceder a una armonización exhaustiva al adoptar a la Directiva 2006/24.

116. A la vista de lo anterior, estimo que una obligación general de conservar datos es compatible con el régimen establecido por la Directiva 2002/58 y, por lo tanto, que un Estado miembro puede hacer uso de la facultad ofrecida por el artículo 15, apartado 1, de dicha Directiva con el fin de imponer una obligación de esta índole. (20) El recurso a esa facultad está, no obstante, supeditado a que se cumplan estrictamente los requisitos establecidos no sólo en dicha disposición, sino también de las disposiciones pertinentes de la Carta leídas a la luz de la sentencia DRI, que serán analizadas en un apartado

posterior. (21)

C – *Sobre la aplicabilidad de la Carta a una obligación general de conservar datos*

117. Antes de examinar el contenido de los requisitos impuestos por la Carta, juntamente con el artículo 15, apartado 1, de la Directiva 2002/58, cuando un Estado decide establecer una obligación general de conservar datos, es preciso comprobar si la Carta es efectivamente aplicable a tal obligación.

118. La aplicabilidad de la Carta a una obligación general de conservar datos depende fundamentalmente de la aplicabilidad de la Directiva 2002/58 a tal obligación.

119. En efecto, según su artículo 51, apartado 1, primera frase, «las disposiciones de la Carta […] se dirigen a los Estados miembros únicamente cuando apliquen el Derecho de la Unión». Las explicaciones relativas al artículo 51 de la Carta se remiten, en este punto, a la jurisprudencia del Tribunal de Justicia según la cual la obligación de respetar los derechos fundamentales definidos en el marco de la Unión sólo se impone a los Estados miembros cuando actúan en el ámbito de aplicación del Derecho de la Unión. (22)

120. Los Gobiernos checo, francés, polaco y del Reino Unido, que niegan que la Directiva 2002/58 sea aplicable a una obligación general de conservar datos,(23) también han sostenido que la Carta no era aplicable a una obligación de ese tipo.

121. Ya he expuesto los motivos por los que considero que una obligación general de conservar datos constituye una aplicación de la facultad contemplada en el artículo 15, apartado 1, de la Directiva 2002/58. (24)

122. En consecuencia, considero que las disposiciones de la Carta son aplicables a las medidas nacionales que establecen tal obligación, con arreglo al artículo 51, apartado 1, de la Carta, como han alegado el Sr Watson, los Sres. Brice y Lewis, Open Rights Group y Privacy International, los Gobiernos danés, alemán, finlandés, así como la Comisión (25).

123. Esta conclusión no se ve desmentida por el hecho de que el ámbito de aplicación de la Carta no abarque las disposiciones nacionales que regulan el acceso a los datos conservados.

124. Ciertamente, en la medida en que afecten a «actividades del Estado en materia penal», las disposiciones nacionales que regulan el acceso a los datos conservados por las autoridades policiales o judiciales para luchar contra infracciones graves están, en mi opinión, comprendidas en la exclusión establecida en el artículo 1, apartado 3, de la Directiva 2002/58. (26) Por consiguiente, tales disposiciones nacionales no ejecutan el Derecho de la Unión, de manera que la Carta no les resulta aplicable.

125. No obstante, la razón de ser de una obligación de conservación de datos es permitir a las autoridades encargadas de combatir la delincuencia acceder a los datos conservados, de manera que los problemas que se refieren a la conservación y al acceso no pueden separarse totalmente. Como ha subrayado con razón la Comisión, las disposiciones que regulan el acceso revisten una importancia determinante para juzgar la compatibilidad con la Carta de las disposiciones que crean una obligación general de conservar datos, las cuales ejecutan el artículo 15, apartado 1, de la Directiva 2002/58. Más precisamente, las disposiciones que regulan el acceso han de ser tenidas en cuenta a la hora de apreciar la necesidad y la proporcionalidad de tal obligación. (27)

D – *Sobre la compatibilidad de una obligación general de conservar datos con los requisitos establecidos por el artículo 15, apartado 1, de la Directiva 2002/58, así como por los artículos 7, 8 y 52, apartado 1, de la Carta*

126. Me queda ahora por abordar la difícil cuestión de la compatibilidad de una obligación general de conservar datos con los requisitos establecidos por el artículo 15, apartado 1, de la Directiva 2002/58, así como por los artículos 7, 8 y 52, apartado 1, de la Carta leídos a la luz de la sentencia DRI. Esta cuestión afecta, de forma más general, a la necesaria adaptación del marco legal que regula las

facultades de vigilancia de los Estados, multiplicadas a causa de los recientes progresos tecnológicos. (28)

127. La primera etapa de cualquier análisis en este ámbito consiste en comprobar si existe una injerencia en los derechos consagrados en la Directiva 2002/58 y en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta.

128. En efecto, dicha obligación constituye una injerencia grave en el derecho al respeto de la vida privada, consagrado en el artículo 7 de la Carta, y en el derecho a la protección de datos de carácter personal, garantizado por el artículo 8 de la Carta. No considero útil insistir en esta injerencia declarada, expuesta con claridad por el Tribunal de Justicia en los apartados 32 a 37 de la sentencia DRI. (29) De igual manera, una obligación general de conservar datos constituye una injerencia en varios derechos consagrados por la Directiva 2002/58. (30)

129. La segunda etapa del análisis consiste en determinar si dicha injerencia grave en los derechos consagrados por la Directiva 2002/58, así como en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta puede estar justificada y, en su caso, con qué requisitos.

130. Existen dos disposiciones que establecen los requisitos que deben cumplirse para que esta doble injerencia esté justificada: el artículo 15, apartado 1, de la Directiva 2002/58, que delimita la facultad de los Estados miembros de limitar el alcance de ciertos derechos establecidos por dicha Directiva, y el artículo 52, apartado 1, de la Carta, leído a la luz de la sentencia DRI, que delimita cualquier limitación del ejercicio de los derechos reconocidos por la Carta.

131. Deseo subrayar que estas exigencias son *acumulativas*. En efecto, el cumplimiento de los requisitos fijados en el artículo 15, apartado 1, de la Directiva 2002/58 no supone de por sí que las exigencias establecidas en el artículo 52, apartado 1, de la Carta se cumplan, y viceversa. (31) Por consiguiente, sólo podrá considerarse que una obligación general de conservar datos es compatible con el Derecho de la Unión si cumple a la vez los requisitos establecidos en el artículo 15, apartado 1, de la Directiva 2002/58 y los que se prevén en el artículo 52, apartado 1, de la Carta, como ha subrayado la Law Society of England and Wales. (32)

132. Entre las dos disposiciones se establecen seis requisitos que han de ser cumplidos para que pueda justificarse la injerencia generada por una obligación general de conservar datos:

– la obligación de conservación debe tener una base legal;

– debe respetar el contenido esencial de los derechos consagrados por la Carta;

– debe perseguir un objetivo de interés general;

– debe ser apropiada para la consecución de dicho objetivo;

– debe ser necesaria para la consecución de dicho objetivo, y

– debe ser proporcionada, en una sociedad democrática, para la consecución de ese mismo objetivo.

133. Varios de esos requisitos ya fueron evocados por el Tribunal de Justicia en la sentencia DRI. Sin embargo, con ánimo clarificador, y habida cuenta las particularidades de los presentes asuntos en relación con el asunto DRI, deseo volver sobre cada uno de ellos, examinando con mayor detalle los requisitos referidos a la base legal, al carácter necesario y al carácter proporcionado, dentro de una sociedad democrática, de una obligación general de conservar datos.

1. Sobre el requisito de tener una base legal de Derecho nacional

134. Tanto el artículo 52, apartado 1, de la Carta como el artículo 15, apartado 1, de la Directiva 2002/58 establecen requisitos en relación con la base legal que debe utilizar un Estado miembro para imponer una obligación general de conservar datos.

135. En primer lugar, cualquier limitación al ejercicio de los derechos reconocidos por la Carta deberá ser «establecida por la ley», con arreglo a su artículo 52, apartado 1. Debo precisar que esta exigencia no fue examinada formalmente por el Tribunal de Justicia en la sentencia DRI, que se refería a una injerencia prevista por una Directiva.

136. Hasta la reciente sentencia WebMindLicenses, (33) el Tribunal de Justicia jamás se había pronunciado sobre el alcance exacto de dicho requisito, incluso cuando la declaraba expresamente cumplida (34) o vulnerada. (35) En el apartado 81 de dicha sentencia, la Sala Tercera del Tribunal de Justicia se pronunció en los siguientes términos:

«A este respecto, procede señalar que el requisito de que cualquier limitación del ejercicio de ese derecho debe establecerse por ley implica que la base jurídica que permita a la administración tributaria utilizar las pruebas mencionadas en el apartado anterior debe ser suficientemente clara y precisa, y que, al definir ella misma el alcance de la limitación del ejercicio del derecho garantizado por el artículo 7 de la Carta, ofrece una cierta protección contra posibles injerencias arbitrarias por parte de dicha administración (véanse TEDH, en particular, sentencias Malone c. Reino Unido de 2 de agosto de 1984, serie A n.º 82, § 67, y Gillan y Quinton c. Reino Unido de 12 de enero de 2010, n.º 4158/05, § 77, CEDH 2010)».

137. Invito a la Gran Sala del Tribunal de Justicia a que confirme esta interpretación en los presentes asuntos por las razones que expongo a continuación.

138. Como señaló acertadamente el Abogado General Cruz Villalón en las conclusiones que presentó en el asunto Scarlet Extended, (36) el TEDH ha elaborado un abundante corpus jurisprudencial en relación con este requisito en el contexto del CEDH, que se caracteriza por una acepción material y no formal del término «ley». (37)

139. Según dicha jurisprudencia, la expresión «prevista por la ley» implica que la base legal sea suficientemente accesible y previsible, es decir, que se enuncie con la suficiente precisión como para permitir al individuo, buscando si es preciso asesoramiento jurídico adecuado, que ajuste su conducta a Derecho. Dicha base legal debe asimismo proporcionar una protección adecuada frente a la arbitrariedad y, en consecuencia, definir con la suficiente nitidez la amplitud y los modos de ejercer la facultad conferida a las autoridades competentes (principio de la primacía del Derecho). (38)

140. Pues bien, considero necesario, por las razones que expondré seguidamente, que se atribuya a la expresión «prevista por la ley» utilizada en el artículo 52, apartado 1, de la Carta un alcance similar al que dicha expresión tiene en el contexto del CEDH.

141. Por una parte, en virtud del artículo 53 de la Carta y de las explicaciones relativas a ese artículo, el nivel de protección ofrecido por la Carta no puede ser jamás inferior al garantizado por el CEDH. Esta prohibición de traspasar el «umbral del CEDH» implica que la interpretación por el Tribunal de Justicia de la expresión «prevista por la ley» utilizada en el artículo 52, apartado 1, de la Carta debe ser al menos tan estricta como la del TEDH en el contexto del CEDH. (39)

142. Por otra parte, a la vista de la naturaleza horizontal de este requisito, que puede aplicarse a muchos tipos de injerencias, tanto en el contexto de la Carta como en el del CEDH, (40) no sería oportuno someter a los Estados miembros a criterios diferentes en función de si la injerencia se examina a la luz de uno u otro de esos dos instrumentos. (41)

143. Por lo tanto, considero que, como han alegado el Gobierno estonio y la Comisión, la expresión «prevista por la ley» que figura en el artículo 52, apartado 1, de la Carta ha de interpretarse a la luz de la jurisprudencia del TEDH, sintetizada en el punto 139 de las presentes conclusiones, en el sentido de que una obligación general de conservar datos, como las obligaciones de que se trata en los litigios principales, debe estar prevista en una base legal suficientemente accesible y previsible, por una parte, y que ofrezca una protección adecuada frente a la arbitrariedad, por otra parte.

144. En segundo lugar, procede determinar el contenido de los requisitos impuesto por el artículo 15, apartado 1, de la Directiva 2002/58 en relación con la base legal que debe utilizarse por un Estado miembro que desee utilizar la facultad que brinda esa disposición.

145. Sobre esta cuestión, tengo que señalar que existe una divergencia entre las versiones lingüísticas de la primera frase de dicha disposición.

146. En las versiones inglesa («legislative measures»), francesa («mesures législatives»), italiana («disposizioni legislative»), portuguesa («medidas legislativas»), rumana («măsuri legislative»), y sueca (« genom lagstiftning vidta åtgärder»), el artículo 15, apartado 1, primera frase de la Directiva 2002/58 impone, en mi opinión la adopción de medidas que emanen del poder legislativo.

147. En cambio, las versiones danesa («retsforskrifter»), alemana («Rechtsvorschriften»), neerlandesa («wettelijke maatregele») y española («medidas legales») de dicha frase pueden ser interpretadas en el sentido de que exigen que se adopten o bien medidas que emanen del poder legislativo, o bien medidas reglamentarias que emanen del poder ejecutivo.

148. Con arreglo a una jurisprudencia reiterada, la necesidad de una aplicación y, por ende, de una interpretación uniformes de un acto de la Unión excluye que éste sea considerado de manera aislada en una de sus versiones, exigiendo, por el contrario, que sea interpretado en función tanto de la voluntad real de su autor como del objetivo perseguido por éste a la luz, en particular, de las versiones adoptadas en todas las demás lenguas oficiales. En caso de divergencia entre las distintas versiones lingüísticas, la norma de que se trata debe interpretarse en función de la estructura general y de la finalidad de la normativa en que se integra. (42)

149. En el asunto que nos ocupa, el artículo 15, apartado 1, de la Directiva 2002/58 regula la facultad de los Estados miembros de establecer excepciones a los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, cuya protección del Directiva ejecuta. Estimo, por ello, oportuno interpretar la exigencia de una base legal impuesta por el artículo 15, apartado 1, de la Directiva 2002/58 a la luz de la Carta, y en particular de su artículo 52, apartado 1.

150. De esta manera, las «medidas» exigidas por el artículo 15, apartado 1, de la Directiva 2002/58 deben cumplir imperativamente las cualidades de accesibilidad, previsibilidad y protección adecuada frente a la arbitrariedad a las que me he referido en el punto 143 de las presentes conclusiones. De tales cualidades, en particular de la exigencia de una protección adecuada frente a la arbitrariedad, se desprende que dichas medidas han de ser *vinculantes* para las autoridades nacionales a las que se concede el poder de acceder a los datos conservados. Entre otras cosas, no sería suficiente que las garantías que rodean el acceso a dichos datos estén determinadas en códigos o directrices internas que no tengan tal carácter vinculante, como ha señalado con razón la Law Society of England and Wales.

151. Además, la expresión «los Estados miembros podrán adoptar medidas», común a todas las versiones lingüísticas del artículo 15, apartado 1, primera frase, de la Directiva 2002/58, parece excluir la posibilidad de que una jurisprudencia nacional, aunque sea reiterada, pueda constituir una base legal suficiente para ejecutar dicha disposición. Debo subrayar que, en ese aspecto, tal disposición va más allá de las exigencias impuestas por la jurisprudencia del TEDH. (43)

152. Debo añadir que me parece deseable, a la vista de la gravedad de las injerencias que implica una obligación general de conservar datos en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, se establezca el contenido esencial del régimen en cuestión, en particular el de las garantías que rodean tal obligación, en una medida adoptada por el poder legislativo, quedando el ejecutivo encargado de desarrollar la regulación de su aplicación.

153. A la vista de lo anterior, considero que el artículo 15, apartado 1, de la Directiva 2002/58 y el artículo 52, apartado 1, de la Carta han de interpretarse en el sentido de que el régimen que establezca una obligación general de conservar datos, como la que es objeto de los litigios principales, ha de fijarse mediante medidas legislativas o reglamentarias en que concurran las cualidades de accesibilidad, previsibilidad y protección adecuada frente a la arbitrariedad.

154. Corresponde a los órganos jurisdiccionales remitentes comprobar que se cumple este requisito habida cuenta de la posición privilegiada de que gozan en orden a valorar sus respectivos regímenes nacionales.

2. Sobre el respeto del contenido esencial de los derechos reconocidos por los artículos 7 y 8 de la

Carta

155. Con arreglo al artículo 52, apartado 1, de la Carta, toda limitación en el ejercicio de los derechos reconocidos por la Carta debe «respetar el contenido esencial de dichos derechos». (44) No me parece que este aspecto, examinado por el Tribunal de Justicia en los apartados 39 y 40 de la sentencia DRI en el contexto de la Directiva 2006/24, plantee problemas especiales en el marco de los presentes asuntos, como han subrayado los Gobiernos español e irlandés, así como la Comisión.

156. En el apartado 39 de la sentencia DRI, el Tribunal de Justicia declaró que dicha Directiva no vulneraba el contenido esencial del derecho fundamental al respeto de la vida privada y de los otros derechos reconocidos en el artículo 7 de la Carta al no permitir conocer el contenido de las comunicaciones electrónicas como tal.

157. Desde mi punto de vista, esta apreciación puede transponerse a los regímenes nacionales de que se trata en los asuntos principales dado que éstos tampoco permiten conocer el contenido, en cuanto tal, de las comunicaciones electrónicas. (45)

158. En el apartado 40 de la sentencia DRI, el Tribunal de Justicia consideró que la Directiva 2006/24 no vulneraba el contenido esencial del derecho fundamental a la protección de datos de carácter personal, reconocido en el artículo 8 de la Carta, a la vista de los principios de protección y de seguridad de los datos que deben respetar los proveedores en virtud del artículo 7 de dicha Directiva, debiendo los Estados miembros velar por que se adopten medidas técnicas y organizativas adecuadas contra la destrucción accidental o ilícita de los datos y su pérdida o alteración accidental.

159. Considero, una vez más, que esta apreciación puede transponerse a los regímenes nacionales de que se trata en los asuntos principales, dado que éstos parecen prever garantías comparables en cuanto a protección y seguridad de los datos conservados por proveedores, garantías que deben permitir proteger de manera eficaz los datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos. (46)

160. No obstante, corresponde a los órganos jurisdiccionales remitentes comprobar que los regímenes nacionales de que se trata en los litigios principales respetan de una manera efectiva el contenido esencial de los derechos reconocidos por los artículos 7 y 8 de la Carta, a la luz de las anteriores consideraciones.

3. Sobre la existencia de un objetivo de interés general reconocido por la Unión que puede de justificar una obligación general de conservar datos

161. Tanto el artículo 15, apartado 1, de la Directiva 2002/58 como el artículo 52, apartado 1, de la Carta exigen que cualquier injerencia en los derechos consagrados por dichos instrumentos persiga un objetivo de interés general.

162. En los apartados 41 a 44 de la sentencia DRI, el Tribunal de Justicia consideró, de una parte, que la obligación general de conservar datos impuesta por la Directiva 2006/24 contribuía a «lucha contra la delincuencia grave y, en definitiva, a la seguridad pública» y, de otra, que dicha lucha constituía un objetivo de interés general de la Unión.

163. En efecto, de la jurisprudencia del Tribunal de Justicia se desprende que la lucha contra el terrorismo internacional para el mantenimiento de la paz y la seguridad internacionales es un objetivo de interés general de la Unión. Lo mismo ocurre en lo que respecta a la lucha contra la delincuencia grave para garantizar la seguridad pública. Por otra parte, en relación con esta cuestión procede señalar que el artículo 6 de la Carta establece el derecho de toda persona no sólo a la libertad, sino también a la seguridad. (47)

164. Cabe transponer esta apreciación a las obligaciones generales de conservación de datos de que se trata en los litigios principales, que pueden estar justificadas por el objetivo de lucha contra los delitos graves.

165. No obstante, a la vista de algunos de los argumentos formulados ante el Tribunal de Justicia,

procede determinar si tal obligación puede justificarse por otro objetivo de interés general, distinto del de la lucha contra los delitos graves.

166. Sobre este particular, la redacción artículo 52, apartado 1, de la Carta alude, de manera general, a «objetivos de interés general reconocidos por la Unión» y a «la necesidad de protección de los derechos y libertades de los demás».

167. La redacción del artículo 15, apartado 1, de la Directiva 2002/58 es más precisa en relación con los objetivos que pueden justificar una injerencia en los derechos establecidos en esa Directiva. En efecto, según dicha disposición, las medidas en cuestión deben contribuir a «proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46».

168. Además, en la sentencia Promusicae, (48) el Tribunal de Justicia consideró que dicha disposición debía interpretarse a la luz artículo 13, apartado 1, de la Directiva 95/46, que autoriza las excepciones a los derechos previstos en la Directiva cuando estén justificadas por «la protección de los derechos y libertades de otras personas». En consecuencia el Tribunal de Justicia consideró que el artículo 15, apartado 1, de la Directiva 2002/58 brindaba a los Estados miembros la posibilidad de imponer a los proveedores el deber de divulgar datos de carácter personal para que, en un procedimiento civil, se determinara si había habido una infracción de los derechos de autor en relación con grabaciones musicales y audiovisuales.

169. El Gobierno del Reino Unido se ha apoyado en dicha sentencia para alegar que una obligación general de conservar datos puede estar justificada por cualquier objetivo de los mencionados, ya sea en el artículo 15, apartado 1, de la Directiva 2002/58, ya sea en el artículo 13, apartado 1, de la Directiva 95/46. Según dicho Gobierno, tal obligación podría estar justificada por la utilidad que presentan los datos conservados en la lucha contra delitos «simples» (como contrapuestos a «graves») o incluso en el contexto de procedimientos no penales en relación con los objetivos mencionados por dichas disposiciones.

170. Este argumento no llega a convencerme, por las siguientes razones.

171. En primer lugar, y como han señalado acertadamente el Sr. Watson, así como Open Rights Group y Privacy International, el enfoque adoptado por el Tribunal de Justicia en la sentencia Promusicae (49) no puede transponerse a los presentes asuntos, al referirse dicha sentencia a una solicitud formulada por una asociación de titulares de derechos de autor, de acceder a datos conservados *motu proprio* por un proveedor, concretamente, Telefónica de España. En otros términos, dicha sentencia no se refería a objetivos susceptibles de justificar las graves injerencias en los derechos fundamentales que implica una obligación general de conservar datos, como la que es objeto de los litigios principales.

172. En segundo lugar, estimo que la exigencia de proporcionalidad en una sociedad democrática excluye que la lucha contra delitos simples o el buen desarrollo de procedimientos no penales pueda justificar una obligación general de conservar datos. En efecto, los considerables riesgos que genera tal obligación se presentan como desmedidos en comparación con las ventajas que puede aportar en la lucha contra delitos simples o en el contexto de procedimientos no penales. (50)

173. A la vista de lo que antecede, considero que el artículo 15, apartado 1, de la Directiva 2002/58 y el artículo 52, apartado 1, de la Carta han de interpretarse en el sentido de que la lucha contra los delitos graves constituye un objetivo de interés general susceptible de justificar una obligación general de conservar datos, a diferencia de la lucha contra delitos simples o el buen desarrollo de procedimientos no penales.

174. En consecuencia, procede examinar si tal obligación reviste un carácter apropiado, necesario y proporcionado a la luz del objetivo de luchar contra delitos graves.

4. Sobre el carácter apropiado de una obligación general de conservar datos en relación con la lucha contra los delitos graves

175. Los requisitos relativos al carácter apropiado, necesario (51) y proporcionado (52) se derivan tanto del artículo 15, apartado 1, de la Directiva 2002/58 como del artículo 52, apartado 1, de la Carta.

176. En virtud del primero de esos requisitos, una obligación general de conservar datos como la que es objeto de los litigios principales debe contribuir al objetivo de interés general que se ha identificado más arriba, es decir, la lucha contra los delitos graves.

177. Esta exigencia no plantea especiales dificultades en el contexto de los presentes asuntos. Como señaló, en esencia, el Tribunal de Justicia, en el apartado 49 de la sentencia DRI, los datos conservados permiten a las autoridades nacionales competentes en materia penal disponer de un medio más de investigación para prevenir o esclarecer delitos graves. Por consiguiente, tal obligación contribuye a la lucha contra los delitos graves.

178. Sin embargo, tengo interés en aclarar la utilidad que puede presentar una obligación general de conservar datos en la lucha contra los delitos graves. Como ha alegado con razón el Gobierno francés, tal obligación permite, en cierta medida, a las autoridades encargadas de combatir la delincuencia «leer el pasado» consultando los datos conservados, a diferencia de lo que ocurre con las medidas de vigilancia dirigidas a un grupo o persona concretos.

179. Una medida de vigilancia dirigida a un grupo o personas concretos tiene por objeto personas previamente identificadas como posiblemente relacionadas, siquiera indirecta o remotamente, con un delito grave. Tales medidas dirigidas a un grupo o persona concretos permiten a las autoridades competentes tener acceso a los datos relativos a las comunicaciones mantenidas por dichas personas, incluso al contenido de dichas comunicaciones. Sin embargo, tal acceso sólo puede referirse a las comunicaciones mantenidas por tales personas *posteriormente* a su identificación.

180. En cambio, una obligación general de conservar datos abarca el conjunto de las comunicaciones mantenidas por el conjunto de los usuarios, sin que se exija ninguna relación con un delito grave. Tal obligación permite a las autoridades competentes tener acceso al historial de las comunicaciones realizadas por una persona antes de haber sido identificada como alguien que tiene tal relación. En este aspecto, dicha obligación otorga a las autoridades que encargadas de combatir la delincuencia una capacidad limitada de leer el pasado, ofreciéndoles un acceso a las comunicaciones realizadas por dichas personas *antes* de su identificación. (53)

181. En otros términos, la utilidad que presenta una obligación general de conservar datos para la lucha contra los delitos graves reside en esa capacidad limitada de leer el paso a través de los datos que trazan el historial de las comunicaciones mantenidas por una persona antes que se sospeche que tiene una relación con un delito. (54)

182. Al presentar la propuesta de Directiva que condujo a la adopción de la Directiva 2006/24, la Comisión ilustró esta utilidad valiéndose de varios ejemplos concretos de investigaciones relativas, en particular, a actos de terrorismo, homicidio, secuestro y pornografía infantil. (55)

183. En los presentes asuntos, se han expuesto ante el Tribunal de Justicia varios ejemplos similares, en particular, por parte del Gobierno francés, que ha subrayado la obligación positiva que incumbe a los Estados miembros de garantizar la seguridad de las personas que se encuentran en su territorio. Según dicho Gobierno, en el marco de las investigaciones relativas al desmantelamiento de las redes que organizan la salida de residentes franceses hacia zonas de conflicto en Irak o en Siria, el acceso a los datos conservados tiene un papel determinante a la hora de identificar las personas que han facilitado tal salida. Dicho Gobierno añade que el acceso a los datos relativos a comunicaciones de las personas implicadas en los recientes atentados terroristas de enero y de noviembre de 2015 en Francia han sido extremadamente útiles para los investigadores a la hora de descubrir a los cómplices de los autores de dichos atentados. De la misma forma, en el marco de la búsqueda de una persona desaparecida, los datos relativos a la localización de dicha persona obtenidos de las comunicaciones mantenidas antes de su desaparición pueden ser determinantes en la investigación.

184. A la vista de las consideraciones que anteceden, considero que una obligación general de conservar datos puede contribuir a luchar contra los delitos graves. Sin embargo, queda por comprobar si tal obligación es a la vez necesaria y proporcionada a dicho objetivo.

5. Sobre el carácter necesario de una obligación general de conservar datos en relación con la lucha contra los delitos graves

185. Según una reiterada jurisprudencia, una medida sólo puede considerarse necesaria si no existe ninguna otra medida que sea igual de apropiada y que, al mismo tiempo, sea menos restrictiva. (56)

186. El requisito del carácter apropiado implica evaluar la eficacia «absoluta» —con independencia de cualquier otra medida que pueda pensarse— de una obligación general de conservar datos en relación con la lucha contra delitos graves. El requisito de necesidad, conduce, por su parte, a valorar la eficiencia, o eficacia «relativa», es decir, en comparación con cualquier otra medida que pueda pensarse– de tal obligación. (57)

187. En el contexto de los presentes asuntos, el test de necesidad obliga a comprobar, por una parte, si otra medidas podrían ser igual de eficaces que una obligación general de conservar datos en la lucha contra los delitos graves y, por otra parte, si, en su caso, dichas medidas son menos lesivas para los derechos consagrados por la Directiva 2002/58 y por los artículos 7 y 8 de la Carta. (58)

188. Deseo, además, recordar la reiterada jurisprudencia, evocada en el apartado 52 de la sentencia DRI, según la cual la protección del derecho fundamental a la vida privada exige que las excepciones a la protección de los datos de carácter personal y las limitaciones de dicha protección deben establecerse sin sobrepasar los límites de lo «estrictamente necesario» . (59)

189. Las partes que han presentado observaciones ante el Tribunal de Justicia han debatido ampliamente dos problemáticas referidas a la exigencia de una estricta necesidad en el contexto de los presentes asuntos, problemáticas que concuerdan con las dos cuestiones planteadas por el órgano jurisdiccional remitente en el asunto C-203/15:

– por una parte, a la luz des apartados 56 a 59 de la sentencia DRI, ¿debe considerarse que una obligación general de conservar datos excede los límites de lo estrictamente necesario en relación con la lucha contra los delitos graves, y ello, con independencia de las garantías que pueda llevar aparejada tal obligación?

– Por otra parte, suponiendo que pueda considerarse que tal obligación excede, en sí misma, los límites de lo estrictamente necesario, ¿debe llevar aparejado el conjunto de garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI con el fin de limitar a lo estrictamente necesario el menoscabo a los derechos consagrados por la Directiva 2002/58 y por los artículos 7 y 8 de la Carta?

190. Antes de abordar esas cuestiones, considero oportuno apartar un argumento formulado por el Gobierno del Reino Unido en el sentido de que los criterios sentados en la sentencia DRI carecen de pertinencia en el contexto de los presentes asuntos por referirse dicha sentencia no a un régimen nacional sino a un régimen establecido por el legislador de la Unión.

191. A este propósito, debo subrayar que la sentencia DRI interpretó los artículos 7, 8 y 52, apartado 1, de la Carta y que dichas disposiciones también son objeto de las cuestiones planteadas en los litigios principales. Pues bien, en mi opinión, resulta imposible interpretar las disposiciones de la Carta de manera diferente en función de si el régimen de que se trata ha sido establecido a escala de la Unión o a escala nacional, como, con razón, han subrayado los Sres. Brice y Lewis, así como la Law Society of England and Wales. Cuando esté comprobado que la Carta resulta aplicable, como ocurre en los presentes asuntos, (60) ésta ha de aplicarse de igual forma, con independencia del régimen de que se trate. Por lo tanto, los criterios establecidos por el Tribunal de Justicia en la sentencia DRI son pertinentes a efectos de apreciar los regímenes nacionales de que se trata en los presentes asuntos, como han alegado, en particular, los Gobiernos danés e irlandés, así como la Comisión.

a) Sobre el carácter estrictamente necesario de una obligación general de conservar datos

192. Según un primer enfoque, sostenido por Tele2 Sverige, así como por Open Rights Group y Privacy International, después de la sentencia DRI, debe considerarse que una obligación general de

conservar datos excede, en sí misma, los límites de lo estrictamente necesario a efectos de la lucha contra los delitos graves, y ello, con independencia de las garantías que pueda llevar aparejadas esta obligación.

193. Según un segundo enfoque, sostenido por la mayoría de las demás partes que han presentado observaciones al Tribunal de Justicia, tal obligación no sobrepasa los límites de lo estrictamente necesario siempre que vaya lleve aparejadas ciertas garantías con respecto al acceso a los datos, al período de conservación, así como a la protección y la seguridad de los datos.

194. Éstas son las razones que me llevan a optar por este segundo enfoque.

195. En primer lugar, según la lectura que hago de la sentencia DRI, el Tribunal de Justicia consideró que una obligación general de conservar datos excede los límites de lo estrictamente necesario cuando *no lleve aparejadas* estrictas garantías en relación con el acceso a los datos, el período de conservación, así como la protección y la seguridad de los datos. En cambio, el Tribunal de Justicia no se pronunció sobre la compatibilidad con el Derecho de la Unión de una obligación general de conservar datos que estuviera *sí llevara aparejadas* tales garantías, por el motivo de que, en ese asunto, el objeto de las cuestiones planteadas al Tribunal de Justicia no era un régimen de tales características.

196. Sobre este extremo, debo subrayar que los apartados 56 a 59 de la sentencia DRI no recogen ninguna declaración del Tribunal de Justicia en el sentido de que una obligación general de conservar datos exceda, en sí misma, los límites de lo estrictamente necesario.

197. En los apartados 56 y 57 de dicha sentencia, el Tribunal de Justicia declara que la obligación de conservación establecida en la Directiva 2006/24 abarca el conjunto de medios de comunicación electrónica, el conjunto de los usuarios, así como el conjunto de los datos de tráfico, sin que se haga ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves.

198. En los apartados 58 y 59 de dicha sentencia, el Tribunal de Justicia expone con mayor detalle las implicaciones prácticas de esta falta de diferenciación. Por una parte, esta obligación de conservación afecta incluso a personas respecto de las cuales no existen indicios que sugieran que su comportamiento puede guardar relación, ni siquiera indirecta o remota, con delitos graves. Por otra parte, dicha Directiva no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública y, en particular, la conservación no se limita a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave.

199. Con ello, el Tribunal de Justicia pone de relieve que una obligación general de conservar datos se caracteriza por su falta de diferenciación en función del objetivo de lucha contra los delitos graves. Sin embargo, no ha considerado que esta falta de diferenciación signifique que dicha obligación exceda, en sí misma, los límites de lo estrictamente necesario.

200. En realidad, hasta que no finaliza su examen del régimen establecido por la Directiva 2006/24, y comprueba la falta de determinadas garantías, que a continuación examinaré, (61) el Tribunal de Justicia no concluye, en apartado 69 de la sentencia DRI que:

«Habida cuenta de todas las consideraciones anteriores, ha de considerarse que, al adoptar la Directiva 2006/24, el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los artículos 7, 8 y 52, apartado 1, de la Carta.» (El subrayado es mío).

201. Como han alegado los Gobiernos alemán y neerlandés, si la conservación generalizada de datos hubiera bastado, por sí sola, para invalidar la Directiva 2006/24, el Tribunal de Justicia no habría tenido necesidad de examinar, además detalladamente, la falta de las garantías enunciadas en los apartados 60 a 68 de dicha sentencia.

202. Por lo tanto, la obligación general de conservar datos prevista en la Directiva 2006/24 no excedía, en sí misma, los límites de lo estrictamente necesario. Dicha Directiva excedía los límites de lo

estrictamente necesario en razón del *efecto combinado* de la conservación generalizada de los datos y de la falta de garantías dirigidas a limitar a lo estrictamente necesario el menoscabo de los derechos consagrados en los artículos 7 y 8 de la Carta. En razón de ese efecto combinado, la Directiva debía declararse inválida en su integridad. (62)

203. En segundo lugar, encuentro una confirmación de esta interpretación en el apartado 93 de la sentencia Schrems, (63) que reproduzco a continuación:

«Pues bien, no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, *sin* establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y *sin* prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización [véase, en este sentido, por lo que se refiere a la Directiva 2006/24, la sentencia DRI, apartados 57 a 61]» (el subrayado es mío).

204. Nuevamente, el Tribunal de Justicia no consideró que el régimen en cuestión en dicho asunto excediera los límites de lo estrictamente necesario sólo por autorizar una conservación generalizada de datos de carácter personal. En ese supuesto, los límites de lo estrictamente necesario se sobrepasaban debido al efecto combinado de la posibilidad de tal conservación generalizada y de la falta de garantías respecto al acceso con vistas a reducir la injerencia a lo estrictamente necesario.

205. De lo anterior deduzco que no siempre debe considerarse que una obligación general de conservar datos excede, por sí misma, los límites de lo que es estrictamente necesario para la lucha contra los delitos graves. En cambio, tal obligación siempre excede los límites de lo estrictamente necesario cuando no lleva aparejadas garantías relativas al acceso a los datos, al período de conservación, así como a la protección y seguridad de los datos.

206. En tercer lugar, mi impresión sobre esta cuestión se ve confirmada por la necesidad de comprobar de manera concreta el cumplimiento del requisito de la estricta necesidad en el contexto de los regímenes nacionales de que se trata en los litigios principales.

207. Como he mencionado en el punto 187 de las presentes conclusiones, el requisito de estricta necesidad requiere examinar si otras medidas podrían ser igual de eficaces que una obligación general de conservar datos en la lucha contra los delitos graves y, al mismo tiempo, menos lesivas para los derechos reconocidos por la Directiva 2002/58 y por los artículos 7 y 8 de la Carta.

208. Pues bien, tal apreciación ha de llevarse a cabo en el contexto específico de cada régimen nacional que establezca una obligación general de conservar datos. Por una parte, esta apreciación requiere comparar la eficacia de esta obligación con la de cualquier otra medida que pueda preverse en el contexto nacional, teniendo en cuenta el hecho de que dicha obligación ofrece a las autoridades competentes una capacidad limitada para leer el pasado a través de los datos conservados. (64)

209. A la vista de la exigencia de estricta necesidad, resulta obligado que dichos órganos jurisdiccionales no se contenten con comprobar simplemente la utilidad de una obligación general de conservar datos, sino que comprueben estrictamente que ninguna otra medida o combinación de medidas, en particular, una obligación de conservar determinados datos relativos a grupos o personas concretos, acompañada de otras herramientas de investigación pueda ofrecer la misma eficacia en la lucha contra los delitos graves. Debo subrayar, a este respecto, que varios estudios presentados al Tribunal de Justicia cuestionan la necesidad de este tipo de obligación a efectos de la lucha contra los delitos graves. (65)

210. Por otra parte, suponiendo que otras medidas puedan ser tan eficaces en la lucha contra los delitos graves, también corresponde a los órganos jurisdiccionales remitentes determinar si esas otras medidas son menos lesivas para los derechos fundamentales de que se trata que una obligación general de conservar datos, con arreglo a la reiterada jurisprudencia que se ha recordado en el punto 185 de las presentes conclusiones.

211. A la luz del apartado 59 de la sentencia DRI, corresponderá a los órganos jurisdiccionales nacionales interrogarse, en particular, acerca de la posibilidad de limitar la extensión material de la obligación de conservación, salvaguardando, al tiempo, la eficacia de esa medida en la lucha contra los delitos graves. (66) En efecto, tales obligaciones pueden tener una amplitud material más o menos grande, en función de los usuarios, de las zonas geográficas y de los medios de comunicación de que se trate. (67)

212. Considero, entre otras cosas, que sería deseable, si la tecnología lo permite, excluir de la obligación de conservación los datos particularmente sensibles con respecto a los derechos fundamentales de que se trata en los presentes asuntos, como los datos amparados por el secreto profesional o los datos que permiten identificar las fuentes de los periodistas.

213. No obstante ha de tenerse presente que existe el riesgo de que una limitación sustancial de la extensión de la obligación general de conservar datos reduzca considerablemente la utilidad que presenta tal régimen en la lucha contra los delitos graves. Por otra parte, varios Gobiernos han subrayado la dificultad, incluso la imposibilidad, de determinar de antemano los datos que pueden presentar una relación con un delito grave. Por lo tanto, esta limitación puede excluir la conservación de datos que podrían resultar ser pertinentes en la luchas contra los delitos graves.

214. Por otra parte, como alega el Gobierno estonio, la criminalidad grave es un fenómeno dinámico, capaz de adaptarse a los instrumentos de investigación de que disponen las autoridades que actúan contra la delincuencia. De esta manera, una limitación a una zona geográfica o a un medio de comunicación determinados podría provocar el riesgo de un desplazamiento de las actividades relacionadas con los delitos graves hacia una zona geográfica o un medio de comunicación no cubiertos por ese régimen.

215. Al requerir una evaluación compleja de los regímenes nacionales de que se trata en los litigios principales, considero que esta apreciación ha de realizarse por los órganos jurisdiccionales nacionales, como han subrayado los Gobiernos checo, estonio, irlandés, francés, neerlandés, y la Comisión.

b) Sobre el carácter imperativo de las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI en relación con el requisito de estricta necesidad

216. Dando por supuesto que una obligación general de conservar datos pueda considerarse estrictamente necesaria en el contexto del régimen nacional de que se trata, extremo cuya apreciación corresponde al juez nacional, quedaría por determinar si tal obligación debe llevar aparejado el conjunto de garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI de manera que se limite a lo estrictamente necesario la lesión a los derechos consagrados por la Directiva 2002/58 y por los artículos 7 y 8 de la Carta.

217. Estas garantías se refieren a las normas que regulan el acceso y el uso de los datos conservados por las autoridades competentes (apartados 60 a 62 de la sentencia DRI), el período de conservación de los datos (apartados 63 y 64 de dicha sentencia), así como la seguridad y la protección de los datos conservados por los proveedores (apartados 66 a 68 de dicha sentencia).

218. Dos han sido las tesis que se han enfrentado, a través de las observaciones presentadas al Tribunal de Justicia, con respecto a la naturaleza de dichas garantías.

219. Según una primera tesis, sostenida por el Sr. Watson, los Sres. Brice y Lewis, así como Open Rights Group y Privacy International, las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI son de obligado cumplimiento. Según esta tesis, el Tribunal de Justicia ha fijado unas garantías mínimas *todas las cuales* deben ser adoptadas por el régimen nacional de que se trata para que el menoscabo a los derechos fundamentales no rebase el límite de lo estrictamente necesario.

220. Según una segunda tesis sostenida por los Gobiernos alemán, estonio, irlandés, francés y del Reino Unido, las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI son meramente indicativas. Consideran que el Tribunal de Justicia procedió a una «apreciación de conjunto» de las garantías que faltaban en el régimen previsto por la Directiva

2006/24, sin que ninguna de ellas pueda considerarse aisladamente imperativa en relación con el requisito de la estricta necesidad. Para ilustrar esta tesis, el Gobierno alemán ha evocado la imagen de los «vasos comunicantes» según la cual un enfoque más flexible de uno de los tres aspectos identificados por el Tribunal de Justicia (por ejemplo, el acceso a los datos conservados) podría compensarse con un enfoque más estricto en relación con los otros dos aspectos (el período de conservación, así como la seguridad y la protección de los datos).

221. Tengo la convicción de que esta tesis de los «vasos comunicantes» ha de rechazarse y de que *todas* las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI han de considerarse de obligado cumplimiento, y ello por las siguientes razones.

222. En primer lugar, el lenguaje utilizado por el Tribunal de Justicia al examinar la estricta necesidad del régimen establecido por la Directiva 2006/24 no se presta a tal interpretación. En particular, el Tribunal de Justicia no alude en ningún lugar, a lo largo de los apartados 60 a 68 de dicha sentencia, a posibilidad alguna de «compensar» un enfoque más flexible en uno de los tres aspectos identificados por el Tribunal de Justicia con un enfoque más estricto con respecto a los otros aspectos.

223. En realidad, la tesis de los «vasos comunicantes» parece proceder de una confusión entre el requisito de necesidad y el de proporcionalidad *stricto sensu,* que no fue examinado por el Tribunal de Justicia en la sentencia DRI. En efecto, como he indicado en el punto 186 de las presentes conclusiones, el requisito de necesidad consiste en rechazar cualquier medida ineficiente. En ese contexto, no puede estarse a una «apreciación de conjunto», a una «compensación» o a una «ponderación», prácticas que sólo entran en juego en la fase de la apreciación de la proporcionalidad *stricto sensu.* (68)

224. En segundo lugar, esta tesis de los «vasos comunicantes» anula el efecto útil de las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI, de tal manera que las personas cuyos datos hubiesen sido conservados dejarían de disponer de garantías suficientes que permitan proteger con eficacia sus datos de carácter personal contra los riesgos de abuso, así como contra cualquier acceso y utilización ilícitas de dichos datos, como exige el apartado 54 de dicha sentencia.

225. El efecto destructivo de esta tesis puede ilustrarse con facilidad con la ayuda de los siguientes ejemplos. Un régimen nacional que restringiera estrictamente el acceso, limitándolo a los fines de lucha contra el terrorismo y limitara el período de conservación a tres meses (enfoque estricto con respecto al acceso y al período de conservación), pero que no obligue a los proveedores a conservar los datos en su territorio nacional y en un formato encriptado (enfoque flexible en cuanto a la seguridad), expondría al conjunto de su población a un elevado riesgo de acceso ilegal a los datos conservados. Del mismo modo, un régimen nacional que previera una duración de conservación de tres meses, así como una conservación de datos en su territorio nacional y en un formato encriptado (enfoques estrictos en cuanto a la duración y a la seguridad), pero que permitiera a todos los funcionarios públicos acceder a los datos conservados (enfoque flexible en cuanto al acceso), expondría al conjunto de su población a un elevado riesgo de abuso por parte de las autoridades nacionales.

226. Considero que estos ejemplos muestran que la necesidad de preservar el efecto útil de las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI exige considerar obligatoria *cada una* de ellas. El TEDH también ha subrayado la importancia fundamental de dichas garantías en su reciente sentencia Szabó y Vissy c. Hungría, refiriéndose expresamente a la sentencia DRI. (69)

227. En tercer lugar, la ejecución de tales garantías, por parte de los Estados miembros que desean imponer una obligación general de conservar datos, no parece plantear mayores dificultades en la práctica. En realidad, dichas garantías me parecen en muchos aspectos «mínimas», como ha alegado el Sr. Watson.

228. Se han discutido ante el Tribunal de Justicia varias de esas garantías, en razón de su posible ausencia en los regímenes nacionales de que se trata en los procedimientos principales.

229. Primeramente, se desprende de los apartados 61 y 62 de la sentencia DRI que el acceso y la

utilización posterior de los datos conservados deberán limitarse estrictamente a fines de prevención y detección de delitos graves delimitados de forma precisa o al enjuiciamiento de tales delitos.

230. Según Tele2 Sverige y la Comisión, esta exigencia no se cumple en el régimen sueco controvertido en el asunto C-203/15, que permite el acceso a los datos conservados a efectos de lucha contra delitos simples. Parecida crítica emiten los Sres. Brice y Lewis, así como el Sr. Watson contra el régimen del Reino Unido controvertido en el asunto C-698/15, que autoriza el acceso a efectos de la lucha contra delitos simples e incluso aunque no exista delito.

231. Si bien es cierto que no compete al Tribunal de Justicia pronunciarse sobre el contenido de dichos regímenes nacionales, sí le corresponde identificar los objetivos de interés general que pueden justificar una injerencia grave en los derechos consagrados por la Directiva y por los artículos 7 y 8 de la Carta. Ya he expuesto, en este asunto, las razones por las que considero que *únicamente* la lucha contra los delitos graves puede justificar tal injerencia. (70)

232. En segundo lugar, según el apartado 62 de la sentencia DRI, el acceso a los datos conservados debe supeditarse a un control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo, cuya decisión tenga por objeto limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo perseguido. Además, este control previo ha de llevarse a cabo a raíz de una solicitud motivada de dichas autoridades presentada en el marco de procedimientos de prevención, detección o enjuiciamiento de delitos.

233. Según las observaciones de Tele2 Sverige y de la Comisión, esta garantía de un control independiente y previo al acceso está parcialmente ausente en el régimen sueco de que se trata en el asunto C-203/15. Lo mismo dicen los Sres. Brice y Lewis, el Sr. Watson, así como Open Rights Group y Privacy International en relación con el régimen del Reino Unido de que se trata en el asunto C-698/15, sin que el Gobierno del Reino Unido haya cuestionado la veracidad de su afirmación.

234. No veo ningún motivo para flexibilizar esta exigencia de control previo por parte de una entidad independiente, exigencia que se desprende sin género de dudas del lenguaje utilizado por el Tribunal de Justicia en el apartado 62 de la sentencia DRI. (71) En primer lugar, esta exigencia viene dictada por la gravedad de la injerencia y los riesgos generados por la creación de bases de datos que abarcan prácticamente la totalidad de la población afectada. (72) Debo señalar que varios expertos en materia de protección de los derechos humanos en la lucha antiterrorista han criticado la actual tendencia que consiste en sustituir los tradicionales procedimientos de autorización independiente y seguimiento efectivo por sistemas de «auto-autorización» por los que los servicios de información y policía acceden a los datos. (73)

235. Se exige, además, un control independiente y previo al acceso a los datos para permitir un tratamiento caso a caso de los datos particularmente sensibles en relación con los derechos fundamentales de los que se trata en los presentes asuntos, teles como los datos amparados por el secreto profesional o aquéllos que permiten identificar las fuentes de los periodistas, como han subrayado la Law Society of England and Wales, así como los Gobiernos francés y alemán. Este control previo es tanto más necesario en aquellos supuestos en los que, técnicamente, resulta difícil excluir el conjunto de dichos datos en la fase de conservación. (74)

236. Por último, añadiré que, desde un punto de vista práctico, ninguna de las tres partes afectadas por una solicitud de acceso tiene posibilidad de ejercer un control efectivo en cuanto al acceso a los datos conservados. Las autoridades competentes en materia represiva tienen el mayor interés en solicitar un acceso de lo más amplio posible a tales datos. Los proveedores, que no conocen el expediente de investigación, no pueden comprobar si la solicitud de acceso se limita a lo estrictamente necesario. En cuanto a las personas cuyos datos se consultan, no tienen ningún medio para averiguar que son objeto de tal medida de investigación, ni siquiera en caso de utilización abusiva o ilícita, como han subrayado el Sr. Watson, así como los Sres. Brice y Lewis. Esta configuración de los intereses en juego requiere, en mi opinión, la intervención de una entidad independiente antes de que se consulten datos conservados, con el fin de proteger a las personas cuyos datos se conservan de cualquier acceso abusivo por parte de las autoridades competentes.

237. Dicho esto, me parece razonable considerar que situaciones puntuales de extrema urgencia, invocadas por el Gobierno del Reino Unido, pueden justificar un acceso inmediato a los datos conservados por las autoridades que actúan contra la delincuencia, sin previo control, con vistas a prevenir la comisión de delitos graves o a perseguir a los autores de tales delitos. (75) Se impone, en cuanto sea posible, mantener la exigencia de una autorización previa instaurando, en la entidad independiente, un procedimiento de urgencia para tramitar este tipo de solicitud de acceso. No obstante, aunque el mero hecho de dirigir a esa entidad una solicitud de acceso parece incompatible con la extrema urgencia de la situación, el acceso y la utilización de los datos habrán de ser objeto de un control *a posteriori* por parte de dicha entidad, control que deberá realizarse a la mayor brevedad.

238. En tercer lugar, el apartado 68 de la sentencia DRI impone a los proveedores la obligación de conservar los datos en el territorio de la Unión, para garantizar el control por una autoridad independiente, como se exige en el artículo 8, apartado 3, de la Carta, del cumplimiento de los requisitos de protección y seguridad enunciados en los apartados 66 y 67 de dicha sentencia.

239. Tele2 Sverige y la Comisión han alegado que el régimen sueco de que se trata en el asunto C-203/15 no garantiza la conservación de los datos en el territorio nacional. Esta misma crítica es la que hacen los Sres. Brice y Lewis, así como el Sr. Watson contra el régimen del Reino Unido de que se trata en el asunto C-698/15.

240. A este respecto, por una parte, no veo razón alguna para disminuir este requisito, fijado en el apartado 68 de la sentencia DRI, por cuanto una conservación de los datos fuera del territorio de la Unión no permitiría garantizar a las personas cuyos datos se conservan en el nivel de protección que ofrecen la Directiva 2002/58 y los artículos 7, 8 y 52, apartado 1, de la Carta. (76)

241. Por otra parte, considero razonable adaptar este requisito, mencionado por el Tribunal de Justicia en el contexto de la Directiva 2006/24, al contexto de regímenes nacionales, previendo que se conserven los datos en el territorio nacional, como han alegado los Gobiernos alemán y francés, así como la Comisión. En efecto, en virtud del artículo 8, apartado 3, de la Carta, incumbe a cada Estado miembro garantizar el control, por una autoridad independiente, del cumplimiento de los requisitos de protección y seguridad por parte de los proveedores contemplados por su régimen nacional. Pues bien, en ausencia de coordinación a escala de la Unión, tal autoridad nacional podría encontrarse en la imposibilidad de llevar a buen puerto sus funciones de control en el territorio de otros Estado miembro.

242. En cuarto lugar, por lo que se refiere al período de conservación, los órganos jurisdiccionales remitentes deberán aplicar los criterios definidos por el Tribunal de Justicia en los apartados 63 y 64 de la sentencia DRI. Por una parte, estos órganos jurisdiccionales deben determinar si los datos conservados pueden diferenciarse en función de su utilidad y, en su caso, si se ha adaptado el período de conservación en función de dicho criterio. Por otra parte, dichos órganos jurisdiccionales deben comprobar si la determinación del período de conservación se basa en criterios objetivos que permitan garantizar que ésta se limita a lo estrictamente necesario.

243. Debo subrayar que, en su reciente sentencia Roman Zakharov c. Rusia, el TEDH ha considerado razonable un período máximo de conservación de seis meses, al tiempo que ha lamentado la ausencia de una obligación de destruir inmediatamente los datos que no guarden relación con la finalidad para la cual se recogen. (77) Añadiré, a este respecto, que los regímenes nacionales de los que se trata en los litigios principales deben prever una obligación de destruir definitivamente cualquier dato cuando ya no sea estrictamente necesario para la lucha contra delitos graves. Esta obligación ha de ser respetada no sólo por los proveedores que llevan a cabo la conservación de datos, sino también por las autoridades que hayan tenido acceso a datos conservados.

244. A la vista de las consideraciones que anteceden, estimo que todas las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI presentan un carácter imperativo y deben, por consiguiente, ir aparejadas a una obligación general de conservar datos para limitar a lo estrictamente necesario el menoscabo a los derechos consagrados por la Directiva 2002/58 y por los artículos 7 y 8 de la Carta.

245. Corresponde a los órganos jurisdiccionales remitentes verificar si los regímenes nacionales de los

que se trata en los litigios principales incluyen cada una de estas garantías.

6. Sobre el carácter proporcionado, en una sociedad democrática, de una obligación general de conservar datos en relación con el objetivo de lucha contra los delitos graves

246. Después de haber comprobado el carácter necesario de los regímenes nacionales de los que se trata en los asuntos principales, también corresponderá a los órganos jurisdiccionales remitentes comprobar su carácter proporcionado, en una sociedad democrática, en relación con el objetivo de lucha contra los delitos graves. Este aspecto no fue examinado por el Tribunal de Justicia en la sentencia DRI dado que el régimen establecido por la Directiva 2006/24 sí rebasaba los límites de lo estrictamente necesario a los efectos de la lucha contra los delitos graves.

247. Esta exigencia de proporcionalidad en una sociedad democrática —o proporcionalidad «*stricto sensu*»— se deriva a la vez del artículo 15, apartado 1, de la Directiva 2002/58, del artículo 52, apartado 1, de la Carta y de una reiterada jurisprudencia. Según esta reiterada jurisprudencia, una medida que menoscabe derechos fundamentales sólo puede considerarse proporcionada si las desventajas ocasionadas no son desproporcionadas con respecto a los objetivos perseguidos. (78)

248. A diferencia de los requisitos relativos al carácter apropiado y necesario de la medida de que se trate, que sirven para valorar su eficacia en relación con el objetivo perseguido, la exigencia de proporcionalidad *stricto sensu* consiste en ponderar, por una parte, las ventajas que resultan de esta medida en relación con el objetivo legítimo perseguido, y, por otra parte, las desventajas que se derivan de la misma en relación con derechos fundamentales consagrados en una sociedad democrática. (79) Esta exigencia abre así un debate sobre los valores que deben prevalecer en una sociedad democrática y, en definitiva, sobre el tipo de sociedad en el que deseamos vivir. (80)

249. Por consiguiente, y como he señalado en el punto 223 de las presentes conclusiones, será en la fase de examen de la proporcionalidad en sentido estricto cuando habrá de procederse a una apreciación de conjunto del régimen en cuestión, y no, como han alegado los partidarios de la tesis de los «vasos comunicantes» en la fase de examen de la necesidad. (81)

250. Con arreglo a la jurisprudencia recordada en el punto 247 de las presentes conclusiones, hay que ponderar las ventajas y desventajas, en una sociedad democrática, de una obligación general de conservar datos. Estas ventajas y estos inconvenientes están íntimamente vinculados a la característica esencial de tal obligación, cuya cara y cruz representan, de alguna manera, a saber, el hecho de que abarca el conjunto de las comunicaciones realizadas por el conjunto de los usuarios sin que se exija ninguna clase de vínculo con un delito grave.

251. Por otra parte, ya he expuesto en los puntos 178 a 183 de las presentes conclusiones las ventajas que representa, para la lucha contra los delitos graves, la conservación de los datos relativos al conjunto de las comunicaciones realizadas en el territorio nacional.

252. Por otra parte, los inconvenientes de una obligación general de conservar datos se derivan del hecho de que la inmensa mayoría de los datos conservados se refieren a personas que jamás tendrán vínculo alguno con un delito grave. Es importante, a este respecto, precisar la naturaleza de los inconvenientes que afectarán a esas personas. Pues bien, esos inconvenientes son de naturaleza diferente dependiendo del nivel de injerencia en sus derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal.

253. En el marco de una injerencia «individual», que afecte a un determinado individuo, los inconvenientes que resultan de una obligación general de conservar datos han sido descritos con gran agudeza por el Abogado General Cruz Villalón en los puntos 72 a 74 de las conclusiones que presentó en el asunto DRI. (82) Recogiendo los términos utilizados por éste, la explotación de estos datos hace posible «determinar de manera tan fiel como exhaustiva una parte importante de los comportamientos de una persona pertenecientes estrictamente a su vida privada, o incluso [obtener] un retrato completo y preciso de su identidad privada».

254. En otros términos, en un contexto individual, una obligación general de conservar datos permite injerencias tan graves como las de las medidas de vigilancia dirigidas a grupos o personas

determinados, incluida la interceptación del contenido de las comunicaciones realizadas.

255. Aunque no pueda subestimarse la gravedad de tales injerencias individuales, considero, sin embargo, que los riesgos específicos generados por una obligación general de conservar datos son patentes en el contexto de injerencias «en masa».

256. En efecto, a diferencia de las medidas de vigilancia dirigidas a un grupo o persona concretos, tal obligación puede facilitar considerablemente las injerencias en masa, es decir las injerencias que afectan a una parte sustancial o incluso al conjunto de la población pertinente, lo que puede ilustrarse con la ayuda de los siguientes ejemplos.

257. Supongamos, en primer lugar, que una persona que tenga acceso a los datos conservados tenga la intención de identificar, dentro de la población del Estado miembro, a todos los individuos que padezcan alguna alteración de orden psicológico. El análisis, con este fin, del contenido del conjunto de las comunicaciones realizadas en el territorio nacional exigiría considerables recursos. En cambio, la explotación de bases de datos relativas a comunicaciones permitiría identificar en un instante todos los individuos que se hayan puesto en contacto con un psicólogo a lo largo del período de conservación de los datos. (83) Añadiré que esta técnica podría extenderse a cada una de las especialidades médicas registradas en un Estado miembro. (84)

258. Supongamos, en segundo lugar, que esa misma persona desea identificar a los individuos contrarios a la política del Gobierno que esté en el poder, Nuevamente, el análisis, con este fin, del contenido de las comunicaciones exigiría recursos considerables. En cambio, la explotación de los datos relativos a las comunicaciones permitiría identificar a todos los individuos cuyo nombre figura en listas de distribución de correos electrónicos críticos con la política del Gobierno. Además, estos datos permitirían también identificar a los individuos que participan en cualquier manifestación pública de oposición al Gobierno. (85)

259. Deseo poner de relieve que los riesgos vinculados al acceso a los datos relativos a las comunicaciones (o «metadatos») pueden ser parecidos, o incluso superiores, a los que resultan del acceso al contenido de dichas comunicaciones, como han subrayado Open Rights Group y Privacy International, la Law Society of England and Wales, así como un reciente informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (86) En particular, y como demuestran los anteriores ejemplos, los «metadatos» permiten catalogar de manera prácticamente instantánea a la totalidad de una población, cosa que el contenido de las comunicaciones no permite.

260. Debo añadir que los riesgos de acceso abusivo o ilegal a los datos conservados no tienen nada de teórico. Por una parte, el riesgo de acceso abusivo por parte de las autoridades ha de ponerse en relación con la cantidad elevadísima de solicitudes, puesta de manifiesto en las observaciones presentadas ante el Tribunal de Justicia. En el contexto del régimen sueco, Tele2 Sverige ha señalado que recibía unas 10 000 solicitudes de acceso al mes, cifra que no incluye las solicitudes recibidas por otros proveedores que operan en el territorio sueco. En cuanto al régimen del Reino Unido, el Sr. Watson ha reproducido las cifras extraídas de un informe oficial que da cuenta de 517 236 autorizaciones y de 55 346 autorizaciones verbales urgentes, sólo en 2014. Por otra parte, el riesgo de acceso ilegal, por cualquier persona, es consustancial a la propia existencia de bases de datos conservadas en soporte informático. (87)

261. Considero que corresponde a los órganos jurisdiccionales remitentes apreciar si las desventajas causadas por las obligaciones generales de conservación de datos de las que se trata en los litigios principales son desproporcionadas, en una sociedad democrática, en relación con los objetivos que se pretenden alcanzar, con arreglo a la jurisprudencia citada en el apartado 247 de las presentes conclusiones. En el marco de esta apreciación, los órganos jurisdiccionales deberán ponderar los riesgos y las ventajas vinculados a tal obligación, a saber:

– por una parte, las ventajas relacionadas con la concesión de una capacidad limitada de leer el pasado a las autoridades encargadas de la lucha contra los delitos graves (88) y,

– por otra parte, los graves riesgos que entrañan, en una sociedad democrática, el poder de retratar la vida privada de un individuo y el poder de catalogar a una población en su totalidad.

262. Esta apreciación ha de realizarse en relación con todas las características pertinentes de los regímenes nacionales de los que se trata en los litigios principales. Debo subrayar, a este respecto, que las garantías imperativas enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia DRI no constituyen sino garantías mínimas dirigidas a limitar a lo estrictamente necesario la lesión a los derechos consagrados por la Directiva 2002/58 y por los artículos 7 y 8 de la Carta. Por lo tanto, no se excluye que un régimen nacional que incluya el conjunto de estas garantías deba, sin embargo, considerarse desproporcionado dentro de una sociedad democrática, en razón de la desproporción entre los graves riesgos generados por esta obligación en una sociedad democrática y las ventajas que reporta en relación con la lucha contra los delitos graves.

V – Conclusión

263. A la vista de cuanto antecede, propongo al Tribunal de Justicia que responda en el siguiente sentido a las cuestiones prejudiciales del Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo, Suecia) y de la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil) (Reino Unido)]:

El artículo 15, apartado 1, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, así como los artículos 7, 8 y 52, apartado 1, de la Carta de Derechos Fundamentales, deben interpretarse en el sentido de que no se oponen a que un Estado miembro imponga a los proveedores de servicios de comunicación electrónica una obligación de conservar el conjunto de los datos relativos a las comunicaciones mantenidas por los usuarios de sus servicios cuando se cumplan todos los requisitos siguientes, extremo que corresponde comprobar a los órganos jurisdiccionales remitentes, a la luz de todas las características pertinentes de los regímenes nacionales de los que se trata en los litigios principales:

– Esta obligación y las garantías que lleve aparejadas deben establecerse mediante medidas legislativas o reglamentarias en las que concurran las cualidades de accesibilidad, previsibilidad y protección adecuada frente a la arbitrariedad;

– esta obligación y las garantías que lleve aparejadas deben respetar el contenido esencial de los derechos reconocidos por los artículos 7 y 8 de la Carta;

– esta obligación debe ser estrictamente necesaria para la lucha contra los delitos graves, lo cual implica que ninguna otra medida o combinación de medidas pueda ser igual de eficaz en la lucha contra los delitos graves y, al mismo tiempo, menos lesiva para los derechos consagrados por la Directiva 2002/58 y por los artículos 7 y 8 de la Carta;

– esta obligación debe llevar aparejadas todas las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238) en relación con el acceso a los datos, el período de conservación, así como la protección y la seguridad de los datos, con el fin de limitar a lo estrictamente necesario el menoscabo a los derechos reconocidos por la Directiva 2002/58 y por los artículos 7 y 8 de la Carta, y

– esta obligación debe ser proporcionada, en una sociedad democrática, al objetivo de lucha contra los delitos graves, lo cual implica que los graves riesgos generados por tal obligación en una sociedad democrática no deben ser desproporcionados en relación con las ventajas que lleva consigo en relación con la lucha contra los delitos graves.

---

1 Lengua original: francés.

---

2 «Si los hombres fueran como ángeles, no sería necesario gobierno alguno. Si los ángeles gobernaran a los hombres, no sería necesario ningún control externo o interno sobre el gobierno. Al organizar un gobierno

de hombres para hombres, la gran dificultad estriba en esto: primero hay que capacitar al gobierno para que controle a los gobernados; luego hay que obligarle a que se controle a sí mismo»: Madison, J., «Federalist No. 51», in Hamilton, A., Madison, J. y Jay, J., ed. Genovese, M. A., *The Federalist Papers*, Palsgrave Macmillan, Nueva York, 2009, p. 120, traducción libre. Madison fue uno de los principales autores y uno de los 39 signatarios de la Constitución de los Estados Unidos (1787). Fue el cuarto presidente de Estados Unidos (de 1809 a 1817).

---

3 Esta capacidad limitada de «leer el pasado» puede, en particular, resultar de gran utilidad a efectos de identificar posibles cómplices: véanse los puntos 178 a 184 de las presentes conclusiones.

---

4 Véanse los puntos 252 a 261 de las presentes conclusiones.

---

5 Directiva 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 2002, L 201, p. 37), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (DO 2009, L 337, p. 11).

---

6 Sentencia de 8 de abril de 2014 (C-293/12 y C-594/12, EU:C:2014:238).

---

7 Directiva 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 2006, L 105, p. 54).

---

8 Este parecido es comprensible habida cuenta de que dichos regímenes nacionales iban dirigidos a transponer esa Directiva, que en la actualidad ya no es válida.

---

9 Véase la descripción de los regímenes nacionales de los que se trata en los litigios principales en los puntos 11 a 13 y 36 de las presentes conclusiones.

---

10 Dictamen 2/13, de 18 de diciembre de 2014 (EU:C:2014:2454), apartado 179, y sentencia de 15 de febrero de 2016, N. (C-601/15 PPU, EU:C:2016:84), apartado 45 y jurisprudencia citada.

---

11 Con arreglo al artículo 6 TUE, apartado 1, párrafo tercero, y al artículo 52, apartado 7, de la Carta, las explicaciones relativas a la Carta deben tenerse en cuenta a efectos de su interpretación (véanse las sentencias de 26 de febrero de 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, apartado 20, y de 15 de febrero de 2016, N., C-601/15 PPU, EU:C:2016:84, apartado 47). Según dichas explicaciones, el artículo 7 de la Carta se corresponde al artículo 8 del CEDH, mientras que el artículo 8 de la Carta no se corresponde con ningún derecho del CEDH.

---

12 Véanse, en particular, las sentencias de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert (C-92/09 y C-93/09, EU:C:2010:662), apartado 40 y jurisprudencia citada, así como de 24 de abril de 2012, Kamberaj (C-571/10, EU:C:2012:233), apartado 42 y jurisprudencia citada.

---

13 Véanse, en particular, la sentencias de 16 de septiembre de 1982, Vlaeminck (132/81,

EU:C:1982:294), apartado 13; el auto de 24 de marzo de 2011, Abt y otros (C-194/10, EU:C:2011:182), apartados 36 y 37, así como la jurisprudencia citada, y la sentencia de 24 de octubre de 2013, Stoilov i Ko (C-180/12, EU:C:2013:693), apartado 46, y jurisprudencia citada.

---

14 Véanse los puntos 126 a 262 de las presentes conclusiones.

---

15 Véanse los puntos 123 a 125 de las presentes conclusiones.

---

16 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31).

---

17 Sentencia de 6 de noviembre de 2003, Lindqvist (C-101/01, EU:C:2003:596), apartados 43 y 44.

---

18 Sentencia de 10 de febrero de 2009 (C-301/06, EU:C:2009:68).

---

19 Sentencia de 10 de febrero de 2009, Irlanda/Parlamento y Consejo (C-301/06, EU:C:2009:68), apartado 80.

---

20 Dado que la Directiva 2002/58 puede calificarse de *«lex specialis»* en relación con la Directiva 95/46 (véase, a este respecto, el artículo 1, apartado 2, de la Directiva 2002/58), no creo necesario comprobar la compatibilidad de una obligación general de conservar datos con el régimen establecido por la Directiva 95/46, que, por otra parte, no es objeto de las cuestiones planteadas al Tribunal de Justicia. En aras de la exhaustividad, tengo interés, sin embargo, en aclarar que la redacción del artículo 13, apartado 1, de la Directiva 95/46 ofrece un abanico más amplio a los Estados miembros que el ofrecido por el artículo 15, apartado 1, de la Directiva 2002/58, que precisa su alcance en el marco de la prestación de servicios de comunicaciones electrónicas disponibles al público. Dado que la facultad contemplada en el artículo 15, apartado 1, de la Directiva 2002/58 permite que un Estado miembro establezca una obligación general de conservar datos, deduzco de ello que el artículo 13, apartado 1, de la Directiva 95/46 también lo permite.

---

21 Véanse los puntos 126 a 262 de las presentes conclusiones.

---

22 En efecto, conforme a reiterada jurisprudencia del Tribunal de Justicia, los derechos fundamentales garantizados en el ordenamiento jurídico de la Unión deben ser aplicados en todas las situaciones reguladas por el Derecho de la Unión, pero no fuera de ellas. El Tribunal de Justicia ya ha indicado que, por este motivo, no puede apreciar a la luz de la Carta una normativa nacional que no se inscriba en el marco del Derecho de la Unión. Por el contrario, cuando una normativa nacional está comprendida en el ámbito de aplicación del Derecho de la Unión, el Tribunal de Justicia debe proporcionar, en el marco de una remisión prejudicial, todos los elementos de interpretación necesarios para que el órgano jurisdiccional nacional pueda apreciar la conformidad de dicha normativa con los derechos fundamentales cuyo cumplimiento debe garantizar (véase la sentencia de 26 de febrero de 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105), apartado 19 y jurisprudencia citada).

---

23 Véase el punto 88 de las presentes conclusiones.

---

24 Véanse los puntos 90 a 97 de las presentes conclusiones.

25 Con mayor precisión, el artículo 51, apartado 1, segunda frase, de la Carta dispone que los Estados miembros respetarán los derechos garantizados por ésta cuando apliquen el Derecho de la Unión.

26 Sobre el alcance de dicha exclusión, véanse los puntos 90 a 97 de las presentes conclusiones.

27 Véanse los puntos 185 a 262 de las presentes conclusiones.

28 Véase, en particular, Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, 17 de abril de 2013, A/HRC/23/40, n.º 33: «Los adelantos tecnológicos determinan que la eficacia del Estado para llevar a cabo la vigilancia ya no se vea limitada en función de la escala o la duración. [...]En consecuencia, ahora el Estado tiene mayor capacidad que nunca para emprender una vigilancia simultánea, invasiva, selectiva y de escala amplia. [...]». Véase también el n.º 50: «En general, la legislación no ha seguido el ritmo de los cambios tecnológicos. En la mayoría de los Estados, las normas jurídicas o bien no existen o son insuficientes para responder al entorno moderno de vigilancia de las comunicaciones. [...]».

29 No obstante, volveré sobre los riesgos específicos planteados por la creación de bases de tal amplitud al tratar el requisito de proporcionalidad, en una sociedad democrática, de una obligación general de conservar datos como la que es objeto de los litigios principales: véanse los puntos 252 a 261 de las presentes conclusiones.

30 Véase, a este respecto, el argumento invocado por Open Rights Group y Privacy International, resumido en el punto 104 de las presentes conclusiones.

31 Encuentro la confirmación de este carácter acumulativo en la última frase del artículo 15, apartado 1, de la Directiva 2002/58, según la cual «todas las medidas contempladas en [dicho] apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del [TUE]». En virtud del artículo 6 TUE, apartado 1, «la Unión reconoce los derechos, libertades y principios enunciados en la [Carta], la cual tendrá el mismo valor jurídico que los Tratados».

32 Lógicamente, este carácter acumulativo conlleva que, en la medida en que los requisitos establecidos por ambas disposiciones se solapen, procede aplicar el requisito más exigente o, dicho en otros términos, el requisito que asegure una mayor protección para los derechos de que se trate.

33 Sentencia de 17 de diciembre de 2015 (C-419/14, EU:C:2015:832).

34 Véanse, en particular, las sentencias de 17 de octubre de 2013, Schwarz (C-291/12, EU:C:2013:670), apartado 35 (injerencia prevista en un reglamento europeo); de 27 de mayo de 2014, Spasic (C-129/14 PPU, EU:C:2014:586), apartado 57 (injerencia prevista por el Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990 y que entró en vigor el 26 de marzo de 1995); de 6 de octubre de 2015, Delvigne (C-650/13, EU:C:2015:648), apartado 47 (injerencia prevista por el Código electoral y el Código penal francés); y de 17 de diciembre de 2015, Neptune Distribution (C-157/14, EU:C:2015:823), apartado 69 (injerencia prevista por un reglamento y una directiva europeos).

35 Sentencia de 1 de julio de 2010, Knauf Gips/Comisión (C-407/08 P, EU:C:2010:389), apartados 87 a 92, (injerencia carente de base legal).

---

36 C-70/10, EU:C:2011:255, puntos 94 a 100.

---

37 Véase, en particular, TEDH, sentencia de 14 de septiembre de 2010, Sanoma Uitgevers B.V. c. Países Bajos, CE:ECHR:2010:0914JUD003822403, § 83.

---

38 Véanse, en particular TEDH, sentencia de 26 de marzo de 1987, Leander c. Suecia, CE:ECHR:1987:0326JUD000924881, § 50-51; TEDH, sentencia de 26 de octubre de 2000, Hassan y Tchaouch c. Bulgaria, CE:ECHR:2000:1026JUD003098596, § 84; TEDH, sentencia de 4 de diciembre de 2008, S. y Marper c. Reino Unido, CE:ECHR:2008:1204JUD003056204, § 95; TEDH, sentencia de 14 de septiembre de 2010, Sanoma Uitgevers B.V. c. Países Bajos, CE:ECHR:2010:0914JUD003822403, § 81-83; TEDH, sentencia de 31 de marzo 2016, Stoyanov y otros c. Bulgaria, CE:ECHR:2016:0331JUD005538810, § 124-126.

---

39 Para ser más preciso, el Tribunal de Justicia no puede, en mi opinión, adoptar una interpretación de dicho requisito que sea más permisiva que la del TEDH, lo cual traería consigo que se autorizara un mayor número de injerencias que el que resultaría de la interpretación de este requisito por el TEDH.

---

40 La expresión «prevista por la ley» se utiliza en el artículo 8, apartado 2 (derecho al respeto a la vida privada y familiar), en artículo 9, apartado 2 (libertad de pensamiento, de conciencia y de religión), en el artículo 10, apartado 2 (libertad de expresión), y en el artículo 11, apartado 2 (libertad de reunión de asociación), del CEDH. En el contexto de la Carta, el artículo 52, apartado 1, se aplica a cualquier limitación del ejercicio de los derechos reconocidos por la misma, suponiendo que tal limitación esté prevista.

---

41 Véase, en este sentido, Peers, S., «Article 52 – Scope of guaranteed rights», in Peers, S., et al, *The EU Cartar of Fundamental Rights: a Commentary,* Oxford, OUP, 2014, n.º 52.39.

---

42 Véanse, en particular, las sentencias de 30 de mayo de 2013, Asbeek Brusse y de Man Garabito (C-488/11, EU:C:2013:341), apartado 26; de 24 de junio de 2015, Hotel Sava Rogaška (C-207/14, EU:C:2015:414), apartado 26, y de 26 de febrero de 2015, Christie's France (C-41/14, EU:C:2015:119), apartado 26.

---

43 Véase, en particular, TEDH, sentencia de 14 de septiembre de 2010, Sanoma Uitgevers B.V. c. Países Bajos, CE:ECHR:2010:0914JUD003822403, § 83: «[el término "ley" que figura en los artículos 8 a 11 del CEDH incluye] al mismo tiempo el "derecho escrito", que abarca tanto los textos de rango inferior al rango legislativo, como actos reglamentarios adoptados por un colegio profesional, por delegación del legislador, en el marco de sus facultades normativas autónomas, y el "derecho no escrito". Ha de entenderse que la "ley" engloba tanto los textos escritos como el "derecho elaborado" por los jueces».

---

44 Este requisito no se deriva de la redacción del artículo 15, apartado 1, de la Directiva 2002/58, ni de la estructura de dicha Directiva, por las razones expuestas en los puntos 99 a 116 de las presentes conclusiones.

---

45 Véase la descripción de los regímenes nacionales de que se trata en los litios principales, en especial, en los puntos 13 y 36 de las presentes conclusiones.

46 Sentencia DRI, apartado 54. Véase la descripción de los regímenes nacionales de que se trata en los litigios principales en los puntos 29 a 33, así como 45 y 46 de las presentes conclusiones.

47 Sentencia DRI, apartado 42 y jurisprudencia citada.

48 Sentencia de 29 de enero de 2008 (C-275/06, EU:C:2008:54), apartados 50 a 54.

49 Sentencia de 29 de enero de 2008 (C-275/06, EU:C:2008:54).

50 Véanse los puntos 252 a 261 de las presentes conclusiones.

51 Sobre la necesariedad, véanse los puntos 185 a 245 de las presentes conclusiones.

52 Sur el carácter proporcionado stricto sensu, véanse los puntos 246 a 262 de las presentes conclusiones.

53 La Comisión también ha subrayado que el valor añadido de una obligación general de conservar datos, en relación con la obligación de conservar determinados datos concretos, reside en esa capacidad limitada de leer el pasado: véase Commission Staff Working Document, presentado como anexo a la propuesta de Directiva que condujo a la adopción de la Directiva 2006/24, SEC(2005) 1131, 21 de septiembre de 2005, n.º 3.6, «Data Preservation versus Data Retention»: «With only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects».

54 El Gobierno francés se refiere, en este punto, al Informe del Conseil d'État (Consejo de Estado, Francia), *Le numérique et les droits fondamentaux (Lo digital y los Derechos Fundamentales)*, 2014, pp. 209-10. El Conseil d'État subraya que un mecanismo de medidas de vigilancia dirigidas a un grupo o persona concretos «sería claramente menos eficaz que la conservación sistemática desde el punto de vista de la seguridad nacional y de la búsqueda de los autores de delitos. En efecto, no permitiría en modo alguno acceder retrospectivamente a las comunicaciones habidas antes de que la autoridad hubiera detectado una amenaza o una infracción: su operatividad dependería, por lo tanto, de la capacidad de las autoridades a anticiparse con respecto a la identidad de las personas cuyos datos de conexión podrían ser útiles, lo cual es imposible en el marco de la policía judicial. Por ejemplo, tratándose de un delito grave, la autoridad judicial no podría tener acceso a las comunicaciones anteriores a su comisión, pese a que el dato es precioso y a veces incluso indispensable para identificar al autor y su cómplice, como demostraron asuntos recientes de atentados terroristas. En el ámbito de la prevención de los ataques contra la seguridad nacional, los nuevos programas técnicos se basan en una capacidad de detección de indicios débiles, incompatible con la idea de la previa identificación de las persona peligrosas».

55 – Commission Staff Working Document presentado como anexo a la propuesta de Directiva que condujo a la adopción de la Directiva 2006/24, SEC(2005) 1131, 21 de septiembre de 2005, n.º 1.2, «The importance of traffic data for law enforcement».

56 – Véanse, en particular, las sentencias de 22 de enero de 2013, Sky Österreich (C-283/11, EU:C:2013:28), apartados 54 a 57; de 13 de noviembre de 2014, Reindl (C-443/13, EU:C:2014:2370), apartado 39, y de 16 de julio de 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480), apartados 120 a 122. Dentro de

la doctrina, véase, especialmente, Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, p. 29: «Under a necessity test, the adjudicator examines whether there exists an alternative measure which achieves the same degree of satisfaction for the first value while entailing a lower degree of non-satisfaction of the second value».

---

57 – Véase Rivers, J., «Proportionality and variable intensity of review», 65(1) *Cambridge Law Journal* (2006) 174, p. 198: «The test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person better off without making any one else worse off. Likewise an act is necessary if no alternative act could make the victim better off in terms of rights-enjoyment without reducing the level of realisation of some other constitutional interest».

---

58 – Sobre la existencia estos dos componentes en el test de necesidad, véase Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, pp. 323 a 331.

---

59 – Véanse, en particular, las sentencias de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert (C-92/09 y C-93/09, EU:C:2010:662), apartados 77 y 86, y de 7 de noviembre de 2013, IPI (C-473/12, EU:C:2013:715), apartado 39.

---

60 – Véanse los puntos 117 a 125 de las presentes conclusiones.

---

61 – Véanse los puntos 216 a 245 de las presentes conclusiones.

---

62 – Véase la sentencia DRI, apartado 65: «Por lo tanto, debe considerarse que esta Directiva constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, *sin que* esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario» (el subrayado es mío).

---

63 – Sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650).

---

64 – Véanse los puntos 178 a 183 de las presentes conclusiones.

---

65 – Véase Comisario de Derechos Humanos del Consejo de Europa, Issue paper on the rule of law on the Internet and in the wider digital world, diciembre de 2014, CommDH/IssuePaper(2014)1, p. 115; Consejo de Derechos Humanos de las Naciones Unidas, Informe de la Oficina del Alto Comisionado para los Derechos Humanos sobre el derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37, n.º 26; Asamblea General de las Naciones Unidas, Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, 23 de septiembre de 2014, A/69/397, n.º 18 y 19.

---

66 – Esta observación se refiere únicamente a las obligaciones generales de conservación de datos (que pueden ir referidas a cualquier persona, con independencia de si tiene un vínculo, del tipo que sea, con un delito grave) y no a las medidas de vigilancia dirigidas a un grupo o persona concretos (las cuales van dirigidas a personas previamente identificadas como relacionadas con un delito grave): acerca de esta distinción, véanse los puntos 178 a 183 de las presentes conclusiones.

---

67 – En particular, el Gobierno alemán aclaró durante la vista oral, que el Parlamento alemán había excluido los correos electrónicos de la obligación de conservación impuesta por la legislación alemana, pero que dicho régimen abarca al conjunto de usuarios y al conjunto del territorio nacional.

---

68 – Véase Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, p. 344: «The first three components of proportionality deal mainly with the relation between the limiting law's purpose and the means to fulfil that purpose. […] Accordingly, those tests are referred to as means-end analysis. *They are not based on balancing*. The test of proportionality *stricto sensu* is different. […] It focuses on the relation between the benefit in fulfilling the law's purpose and the harm caused by limiting the constitutional right. *It is based on balancing*» (el subrayado es mío).

---

69 – TEDH, sentencia de 12 de enero de 2016, Szabó y Vissy c. Hungría, CE:ECHR:2016:0112JUD003713814, §68: «Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information».

---

70 – Véanse los puntos 170 a 173 de las presentes conclusiones.

---

71 – No obstante, debo precisar que esta exigencia de control previo e independiente no puede, en mi opinión, basarse en el artículo 8, apartado 3, de la Carta, al no ser la Carta, en cuanto tal, aplicable a las disposiciones nacionales que regulan el acceso a los datos conservados: véanse los puntos 123 a 125 de las presentes conclusiones.

---

72 – Véanse los puntos 252 a 261 de las presentes conclusiones.

---

73 – Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, 28 de diciembre de 2009, A/HRC/13/37, n.º 62: «no debe haber ningún sistema secreto de vigilancia que no se encuentre sometido al examen de un órgano de supervisión efectivo y todas las injerencias deben ser autorizadas por un órgano independiente» (véase asimismo el n.º 51). Véase también Asamblea General de las Naciones Unidas, Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, 23 de septiembre de 2014, A/69/397, n.º 61.

---

74 – Véanse los puntos 212 de las presentes conclusiones. En cuanto a las fuentes periodísticas, el TEDH ha subrayado la necesidad de una autorización previa por parte de una entidad independiente, en la medida que el control a posteriori no permite restaurar la confidencialidad de tales fuentes: véase TEDH, sentencia de 22 de noviembre de 2012, Telegraaf Media Nederland Landelijke Media B.V. y otros c. Países Bajos, CE:ECHR:2012:1122JUD003931506, § 101 y TEDH, sentencia de 12 de enero de 2016, Szabó y Vissy c. Hungría, CE:ECHR:2016:0112JUD003713814, §77. En la sentencia Kopp c. Suiza, que trataba de la intervención de líneas telefónicas de un abogado, el TEDH censuró el hecho de que un funcionario perteneciente a la administración esté encargado, sin el control de un magistrado independiente, de filtrar las informaciones cubiertas por el secreto profesional: véase TEDH, sentencia de 25 de marzo de 1998, Kopp c. Suiza, CE:ECHR:1998:0325JUD002322494, § 74.

---

75 – Véase, a este respecto, el mecanismo descrito en el punto 22 de las presentes conclusiones. Debo señalar que esta problemática no ha sido abordada por el Tribunal de Justicia en la sentencia DRI.

---

76 – Véase, a este respecto, la sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650).

---

77 – Véase, sobre esta cuestión, TEDH, sentencia de 4 de diciembre de 2015, Roman Zakharov c. Rusia, CE:ECHR:2015:1204JUD004714306, § 254-255. Según el Derecho ruso, la destrucción de los elementos interceptados debía realizarse a los seis meses de su conservación si la persona afectada no había resultado imputada. El TEDH consideró razonable la duración máxima de conservación de seis meses, fijada por el Derecho ruso para tales datos. No obstante, deploró que no existiera una obligación de destruir inmediatamente los datos carentes de relación con la finalidad para la que fueron recogidos y aclaró que la conservación automática durante seis meses de datos manifiestamente carentes de interés no puede considerarse justificada a la luz del artículo 8 del CEDH.

---

78 – Véanse, en particular, las sentencias de 15 de febrero de 2016, N., C-601/15 PPU, EU:C:2016:84, apartado 54 (el carácter necesario se examina en los apartados 56 a 67, el carácter proporcionado, en los apartados 68 y 69); de 16 de julio de 2015, CHEZ Razpredelenie Bulgaria, C-83/14, EU:C:2015:480, apartado 123 (el carácter necesario se examina en los apartados 120 a 122, el carácter proporcionado en los apartados 123 a 127), y de 22 de enero de 2013, Sky Österreich, C-283/11, EU:C:2013:28, apartado 50 (el carácter necesario se examina en los apartados 54 a 57, el carácter proporcionado, en los apartados 58 a 67).

---

79 – Véase Rivers J., «Proportionality and variable intensity of review», 65(1) *Cambridge Law Journal* (2006) 174, p. 198: «It is vital to realise that the test of balance has a totally different function from the test of necessity. The test of necessity rules out inefficient human rights limitations. It filters out cases in which the same level of realisation of a legitimate aim could be achieved at less cost to rights. By contrast, the test of balance is strongly evaluative. It asks whether the combination of certain levels of rights-enjoyment combined with the achievement of other interests is good or acceptable».

---

80 – Véase Pirker B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, p. 30: «In its simple form, one could state that proportionality *stricto sensu* leads to a weighing between competing values to assess which value should prevail».

---

81 – La especificidad del requisito de proporcionalidad *stricto sensu*, en relación con requisitos de revestir un carácter apropiado y necesario, puede ilustrarse con el siguiente ejemplo. Imaginemos que un Estado miembro impone la implantación de un microchip de geo-localización a cualquier persona que resida en su territorio, al permitir el microchip a las autoridades recomponer las idas y venidas de su portador durante el año que ha transcurrido. Tal medida podría considerarse «necesaria» de no haber ninguna otra medida que permita alcanzar el mismo grado de eficacia en la lucha contra los delitos graves. Sin embargo, a mis ojos, tal medida resulta desproporcionada en una sociedad democrática, dado que las desventajas que resultan del menoscabo de los derechos a la integridad física, al respecto de la vida privada y a la protección de los datos de carácter personal serían desproporcionas en relación con las ventajas obtenidas en relación con la lucha contra los delitos graves.

---

82 – EU:C:2013:845. Véase también la sentencia DRI, apartados 27 y 37.

---

83 – Los datos conservados incluyen, en efecto, la identidad del origen y del destino de una comunicación, datos que bastaría con cruzar con la lista de los números de teléfono de los psicólogos que operan en el territorio nacional.

84 – Véase, a este respecto, Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, 28 de diciembre de 2009, A/HRC/13/37, n.º 42: «en Alemania las investigaciones demostraron que las políticas de conservación de datos tenían un efecto disuasorio: el 52 % de las personas entrevistadas dijo que probablemente no utilizaría las telecomunicaciones para entrar en contacto con asesores de drogadictos, psicoterapeutas o asesores matrimoniales debido a las leyes de conservación de datos».

85 – Dado que los datos conservados incluyen la localización del origen y del destinatario de una comunicación, cualquier persona que inicie o reciba una comunicación durante una manifestación podrá ser identificada con facilidad gracias a los datos conservados. A este respecto, Marc Goodman, experto ante el FBI e Interpol en el ámbito de los riesgos vinculados a las nuevas tecnologías relata que, en un pasado reciente, el Gobierno ucraniano procedió, durante una manifestación de la oposición, a identificar todos los teléfonos móviles localizados en las cercanías de los enfrentamientos callejeros entre las fuerzas del orden y personas contrarias al Gobierno. El conjunto de estos teléfonos recibió en ese momento un mensaje descrito por el autor como el más «orwelliano» jamás enviado por un gobierno: «Estimado abonado: está siendo grabado participando en una grave alteración del orden público» (Goodman, M., *Future Crimes*, Anchor Books, New York, 2016, p. 153, traducción libre). Véase también Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, 17 de abril de 2013, A/HRC/23/40, n.º 75, y Consejo de Derechos Humanos de las Naciones Unidas, Informe de la Oficina del Alto Comisionado para los Derechos Humanos sobre el derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37, n.º 3.

86 – Véase, a este respecto, Consejo de Derechos Humanos de las Naciones Unidas, Informe de la Oficina del Alto Comisionado para los Derechos Humanos sobre el derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37, n.º 19: «En la misma línea, se ha sugerido que la interceptación o la recopilación de datos acerca de una comunicación, en contraposición al contenido de la comunicación, no constituyen en sí mismas una injerencia en la vida privada. Desde el punto de vista del derecho a la privacidad, esa distinción no es convincente. La agregación de la información comúnmente conocida como "metadatos" puede incluso dar una *mejor idea* del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que *la información obtenida accediendo al contenido* de una comunicación privada» (el subrayado es mío). Véase también Asamblea General de las Naciones Unidas, Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, 23 de septiembre de 2014, A/69/397, n.º 53.

87 – Véase, en particular, Consejo de Derechos Humanos de Naciones Unidas, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, 17 de abril de 2013, A/HRC/23/40, n.º 67: «Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental».

88 – Véanse los puntos 178 a 183 de las presentes conclusiones.