Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
HENRIK SAUGMANDSGAARD ØE
apresentadas em 19 de julho de 2016[1]

Processos apensos C-203/15 e C-698/15

Tele2 Sverige AB
contra
Post- och telestyrelsen (C-203/15)
e
Secretary of State for the Home Department
contra
Tom Watson,
Peter Brice,
Geoffrey Lewis(C-698/15)
sendo intervenientes
Open Rights Group,
Privacy International,
Law Society of England and Wales

[pedidos de decisão prejudicial apresentados pelo Kammarrätten i Stockholm (Tribunal administrativo de recurso de Estocolmo, Suécia) e pela Court of Appeal (England & Wales) (Civil Division) (Tribunal de recurso) (Inglaterra e País de Gales) (Divisão Cível) (Reino Unido)]

«Reenvio prejudicial — Diretiva 2002/58/CE — Tratamento de dados pessoais e proteção da vida privada no setor das comunicações eletrónicas — Legislação nacional que prevê uma obrigação geral de conservação dos dados relativos às comunicações eletrónicas — Artigo 15.º, n.º 1 — Carta dos Direitos Fundamentais da União Europeia — Artigo 7.º — Direito ao respeito da vida privada — Artigo 8.º — Direito à proteção dos dados pessoais — Ingerência grave — Justificação — Artigo 52.º, n.º 1 — Requisitos — Objetivo legítimo de luta contra as infrações graves — Exigência de uma base legal no direito nacional — Exigência da estrita necessidade — Exigência de proporcionalidade numa sociedade democrática»

Índice

1 — Língua original: francês.

I – Introdução

1. Em 1788, James Madison, um dos autores da Constituição dos Estados Unidos, escreveu: «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. Os presentes processos colocam-nos no cerne da «grande dificuldade» identificada por Madison. Dizem respeito à compatibilidade com o direito da União de regimes nacionais que impõem, aos prestadores de um serviço de comunicações eletrónicas acessíveis ao público (a seguir «prestadores»), uma obrigação de conservação dos dados relativos às comunicações eletrónicas (a seguir «dados relativos às comunicações»), que incidem sobre todos os meios de comunicação e sobre todos os utilizadores (a seguir «obrigação geral de conservação de dados»).

3. Por um lado, a conservação dos dados relativos às comunicações confere poderes «ao governo para controlar os governados», oferecendo às autoridades competentes um meio de investigação que pode revestir uma certa utilidade na luta contra as infrações graves, nomeadamente na luta contra o terrorismo. Em substância, a conservação destes dados concede às autoridades uma capacidade limitada de «ler o passado», acedendo aos dados relativos às comunicações que uma pessoa efetuou inclusivamente antes de se suspeitar que esta pode estar associada a uma infração grave [3].

2 — «Se os homens fossem anjos, os governos não seriam necessários. Se os anjos governassem os homens, não seriam necessários controlos externos nem internos sobre o governo. Aquando da criação de um governo de homens que deverá governar homens, a grande dificuldade reside no seguinte: devemos, em primeiro lugar, conferir poderes ao governo para controlar os governados; em seguida, há que obrigá-lo a controlar-se a si próprio»: Madison, J., «Federalist N.º 51», in Hamilton, A., Madison, J. e Jay, J., ed. Genovese, M. A., *The Federalist Papers*, Palsgrave Macmillan, New York, 2009, p. 120 (tradução livre). Madison foi um dos principais autores e um dos 39 signatários da Constituição dos Estados Unidos (1787). Viria, posteriormente, a ser o quarto presidente dos Estados Unidos (entre 1809 e 1817).

3 — Esta capacidade limitada de «ler o passado» pode, nomeadamente, revelar grande utilidade para efeitos da identificação de eventuais cúmplices: v., n.os 178 a 184 das presentes conclusões.

4. Todavia, e por outro lado, é imperativo «obrigar o governo a controlar-se a si próprio» no que respeita tanto à conservação como ao acesso aos dados conservados, atendendo aos riscos graves que podem decorrer da existência de tais bases de dados que abrangem todas as comunicações realizadas no território nacional. Com efeito, estas bases de dados de dimensão considerável oferecem a qualquer pessoa que a elas aceda poder para catalogar instantaneamente toda a população relevante [4]. Há que proceder a um escrutínio escrupuloso destes riscos, nomeadamente através do exame do caráter da estrita necessidade e do caráter proporcionado de uma obrigação geral de conservação de dados, como as que estão em causa nos litígios nos processos principais.

5. Deste modo, no âmbito dos presentes processos, o Tribunal de Justiça e os órgãos jurisdicionais de reenvio são chamados a definir um ponto de equilíbrio entre a obrigação que incumbe aos Estados-Membros de garantirem a segurança dos indivíduos que se encontram no seu território e o respeito dos direitos fundamentais à vida privada e à proteção dos dados pessoais consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

6. Apreciarei as questões submetidas ao Tribunal de Justiça nos presentes processos à luz desta «grande dificuldade». Estas questões, dizem, mais especificamente, respeito à compatibilidade de regimes nacionais que estabelecem uma obrigação geral de conservação de dados com a Diretiva 2002/58/CE [5], bem como com os artigos 7.º e 8.º da Carta. Para responder a estas questões, o Tribunal de Justiça deverá nomeadamente precisar a interpretação que, num contexto nacional, deve ser dada ao acórdão Digital Rights Ireland e o. (a seguir «acórdão DRI») [6], no qual a Grande Secção do Tribunal de Justiça declarou a invalidade da Diretiva 2006/24 [7].

7. Pelos motivos que em seguida irei expor, penso que uma obrigação geral de conservação de dados imposta por um Estado-Membro pode ser compatível com os direitos fundamentais consagrados pelo direito da União desde que essa obrigação seja estritamente enquadrada por uma série de garantias que identificarei no decurso da minha exposição.

II – Quadro jurídico

A – Diretiva 2002/58

8. O artigo 1.º da Diretiva 2002/58, sob a epígrafe «Âmbito e objetivos», dispõe que:

«1. A presente diretiva prevê a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na [União Europeia].

2. Para os efeitos do n.º 1, as disposições da presente diretiva especificam e complementam a Diretiva [95/46]. Além disso, estas disposições asseguram a proteção dos legítimos interesses dos assinantes que são pessoas coletivas.

4 — V. n.os 252 a 261 das presentes conclusões.

5 — Diretiva do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 201, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO 2009, L 337, p. 11).

6 — Acórdão de 8 de abril de 2014 (C-293/12 e C-594/12, EU:C:2014:238).

7 — Diretiva do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO 2006, L 105, p. 54).

3. A presente diretiva não é aplicável a atividades fora do âmbito do [TFUE], tais como as abrangidas pelos títulos V e VI do [TUE], e em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em matéria de direito penal».

9. O artigo 15.º, n.º 1, da Diretiva 2002/58, sob a epígrafe «Aplicação de determinadas disposições da Diretiva [95/46]», tem a seguinte redação:

«Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva [95/46]. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.ºs 1 e 2 do artigo 6.º do [TUE]».

B – Direito sueco

10. A Diretiva 2006/24, atualmente invalidada, foi transposta para o direito sueco através das alterações introduzidas na lagen (2003:389) om elektronisk kommunikation (lei sueca 2003:389 relativa às comunicações eletrónicas, a seguir «LEK») e no förordningen (2003:396) om elektronisk kommunikation (regulamento 2003:396 relativo às comunicações eletrónicas, a seguir «FEK»), tendo estes diplomas entrado em vigor em 1 de maio de 2012.

1. Quanto ao âmbito da obrigação de conservação

11. Resulta das disposições do § 16 a) do capítulo 6 da LEK que os prestadores estão obrigados a conservar os dados relativos às comunicações necessários para identificar a fonte e o destino de uma comunicação, para determinar a respetiva data, hora, duração e natureza, para identificar o tipo de material utilizado, bem como para localizar o equipamento de comunicação móvel utilizado no início e no fim da comunicação. Os tipos de dados que devem ser conservados são objeto de disposições mais detalhadas nos §§ 38 a 43 do FEK.

12. Esta obrigação de conservação diz respeito aos dados tratados no âmbito de um serviço telefónico, de um serviço telefónico realizado através de uma ligação móvel, de um sistema de correio eletrónico, de um serviço de acesso à Internet, bem como de um serviço de oferta de capacidade de acesso à Internet.

13. Os dados a conservar incluem não apenas todos os dados que deviam ser conservados no âmbito da Diretiva 2006/24, mas também os dados relativos às comunicações falhadas, bem como os dados relativos à localização no momento em que termina uma comunicação realizada através de um sistema móvel. À semelhança do regime que se encontrava previsto nesta diretiva, os dados a conservar não incluem o conteúdo das comunicações.

2. Quanto ao acesso aos dados conservados

14. O acesso aos dados conservados é regulado por três diplomas, designadamente, a LEK, o rättegångsbalken (Código de Processo Civil, a seguir «RB») e a lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Lei sueca n.º 2012:278 sobre a comunicação de dados relativos a comunicações eletrónicas no âmbito das atividades de informação das autoridades repressivas).

a) LEK

15. De acordo com as disposições do § 22, primeiro parágrafo, 2º, do capítulo 6 da LEK, todos os prestadores devem transmitir os dados respeitantes a uma assinatura se um pedido for formulado nesse sentido pelo Ministério Público, pela Polícia, pelo Säkerhetspolisen (Serviço de Segurança sueco, a seguir «Säpo») ou por qualquer outra autoridade pública repressiva, se os referidos dados disserem respeito a uma infração presumida. De acordo com estas disposições, não é necessário que se trate de uma infração grave.

16. Por dados respeitantes a uma assinatura entende-se, essencialmente, os dados relativos ao nome, ao título, ao endereço, ao número de telefone e ao endereço IP do subscritor da assinatura.

17. Nos termos da LEK, a transmissão de dados respeitantes a uma assinatura não está subordinada a um controlo prévio, mas pode ser objeto de um controlo administrativo posterior. Além disso, o número de autoridades que pode ter acesso aos dados não é limitado.

b) RB

18. O RB regula a monitorização secreta de comunicações eletrónicas no âmbito de investigações preliminares.

19. No essencial, a monitorização secreta de comunicações eletrónicas só pode ser decretada quando haja motivos razoáveis de que uma determinada pessoa é suspeita de ser o autor de uma infração punida com pena de prisão de pelo menos seis meses ou de outras infrações especificamente enumeradas, se esta medida for especialmente necessária para a investigação.

20. Para além destas situações, a monitorização secreta de comunicações eletrónicas só pode ser realizada para investigar uma infração punida com pena de prisão de pelo menos dois anos para determinar quem poderá razoavelmente ser suspeito de ser autor dessa infração, se esta medida for especialmente necessária para a investigação.

21. Nos termos do § 21 do capítulo 27 do RB, o Ministério Público tem, em regra, de obter autorização judicial antes de dar execução às medidas de monitorização secreta de comunicações eletrónicas.

22. Não obstante, se o facto de submeter a questão ao juiz competente antes de proceder à monitorização secreta de comunicações eletrónicas, medida que reveste uma necessidade imperiosa para as necessidades do inquérito, for incompatível com a urgência da sua execução ou criasse obstáculos, a autorização da medida é concedida pelo Ministério Público na pendência da decisão do juiz competente. Este último deve ser imediatamente informado por escrito pelo Ministério Público. O juiz competente deve então analisar rapidamente se a medida é justificada.

c) Lei 2012:278

23. No âmbito da recolha de informações e em aplicação do § 1 da Lei 2012:278, a polícia nacional, a Säpo e a Tullverket (Serviços Aduaneiros suecos) podem, nas condições previstas nesta lei e sem conhecimento do prestador, proceder à recolha de dados relativos às comunicações.

24. Nos termos dos §§ 2 e 3 da Lei 2012:278, os dados podem ser recolhidos quando, em função das circunstâncias, a medida seja especialmente necessária para prevenir, impedir ou constatar atividades criminosas que envolvam uma ou várias infrações às quais é aplicável uma pena de pelo menos dois anos de prisão, ou um dos atos enumerados no § 3 (incluindo nomeadamente diferentes formas de sabotagem e de espionagem).

25. A decisão de proceder a tal medida é tomada pela chefia da autoridade relevante ou por qualquer funcionário em quem essa chefia delegue poderes para adotar essa decisão.

26. A decisão deve indicar a atividade criminosa, o período em causa, bem como o número de telefone, qualquer outro endereço, o equipamento de comunicação eletrónica ou a área geográfica por ela coberta. A duração da autorização não deve ser superior ao necessário e, relativamente ao período de tempo posterior à data da decisão de autorização, não pode ter uma duração superior a um mês.

27. Este tipo de medida não está sujeito a controlo prévia. No entanto, nos termos do § 6 da Lei 2012:278, a Säkerhets- och integritetsskyddsnämnden (Comissão de segurança e de proteção da integridade, Suécia) deve ser informada de todas as decisões de autorização de proceder à recolha de dados. Nos termos do § 1 da lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Lei 2007:980 relativa ao controlo de determinadas atividades repressivas), este organismo vigia a aplicação da lei pelas autoridades repressivas.

3. Quanto à duração da conservação dos dados

28. Resulta das disposições do § 16 d) do capítulo 6 da LEK que os dados visados no § 16 a) do mesmo capítulo devem ser conservados durante um período de seis meses contado a partir do dia em que cessou a comunicação. Em seguida, os dados devem ser imediatamente eliminados, exceto se o § 16 d), segundo parágrafo, (do capítulo 6) da LEK dispuser diversamente. De acordo com estas últimas disposições, os dados cuja comunicação foi solicitada antes de expirado o período de duração da conservação mas que ainda não tenham sido transmitidos devem ser eliminados imediatamente após essa transmissão.

4. Quanto à proteção e à segurança dos dados conservados

29. O § 20, primeiro parágrafo, do capítulo 6 da LEK proíbe a difusão ou a utilização não autorizada de dados relativos às comunicações.

30. Nos termos do § 3 a) do capítulo 6 da LEK, os prestadores devem adotar as medidas técnica e organizativa adequadas para assegurarem a proteção dos dados durante o seu tratamento. Resulta dos trabalhos preparatórios relativos a esta disposição que não é permitido determinar o nível de proteção com base numa ponderação entre as considerações de ordem técnica, dos custos, e dos riscos de pirataria e de violação da privacidade.

31. Outras prescrições sobre a proteção de dados constam do § 37 do FEK, bem como das instruções e das orientações da Post-och telestyrelsen (Autoridade sueca de vigilância dos correios e das telecomunicações, a seguir «PTS») sobre as medidas de proteção no âmbito da conservação e do tratamento de dados para efeitos de luta contra a criminalidade (PTSFS 2012:4), incluem outras disposições relativas à segurança dos dados. Destes textos resulta nomeadamente que os prestadores

devem adotar medidas para proteger os dados da destruição não intencional ou não autorizada, contra a conservação, o tratamento e o acesso não autorizados, bem como da divulgação não autorizada. Os prestadores devem também levar a cabo operações contínuas e sistemáticas de segurança dos dados, tomando em consideração os riscos concretos decorrentes da obrigação de conservação.

32. Não existem disposições no direito sueco que regulem o local no qual os dados devem ser conservados.

33. Nos termos do capítulo 7 da LEK, a autoridade reguladora tem poder, caso um prestador não cumpra as suas obrigações, para adotar as ordens e proibições, eventualmente acompanhadas de uma sanção pecuniária, assim como para ordenar uma cessão total ou parcial da atividade.

C – Direito do Reino Unido

34. As disposições que regulam a conservação dos dados figuram na Data Retention and Investigatory Powers Act 2014 (Lei de 2014 relativa à conservação dos dados e aos poderes de investigação, a seguir «DRIPA»), nos Data Retention Regulations 2014 (SI 2014/2042) (Regulamento de 2014 relativo à conservação dos dados, a seguir «Regulamento de 2014»), bem como no Retention of Communications Data Code of Practice (Código das boas práticas relativo à conservação dos dados).

35. As disposições que regulam o acesso aos dados figuram no capítulo 2 da parte 1 da Regulation of Investigatory Powers Act 2000 (Lei de 2000 que regula os poderes de investigação, a seguir «RIPA»), no Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480)] (Despacho de 2015 que regula os poderes de investigação em matéria de dados relativos às comunicações, conforme alterado pela Regulation of Investigatory Powers (Communications Data) (Amendement) Order 2015 (SI 2015/228)], assim como no Acquisition and Disclosure of Communications Data Code of Practice (Código das boas práticas relativo à obtenção e à divulgação dos dados relativos às comunicações, a seguir «Código relativo à obtenção dos dados»).

1. Quanto ao âmbito da obrigação de conservação

36. Nos termos da section 1 da DRIPA, o Secretary of State for the Home Department (Ministro da Administração Interna, Reino Unido, a seguir «Ministro») pode impor aos prestadores a obrigação de conservarem todos os dados relativos às comunicações. Em substância, esta obrigação pode dizer respeito a todos os dados gerados numa comunicação encaminhada por um serviço postal ou por um sistema de telecomunicações, com exceção do conteúdo da comunicação. Estes dados incluem, nomeadamente, o local onde se encontra o utilizador do serviço, bem como os dados que permitem determinar o endereço IP (protocolo Internet) ou qualquer outro identificador que pertença ao remetente ou ao destinatário de uma comunicação.

37. Os objetivos que podem justificar a adoção de tal medida de conservação incluem os interesses da segurança nacional, a prevenção ou a deteção da criminalidade ou a prevenção da perturbação da ordem pública, os interesses do bem-estar económico do Reino Unido, desde que estes interesses também sejam relevantes para os interesses da segurança nacional, os interesses da segurança pública, a proteção da saúde pública, a liquidação ou a cobrança de taxas, impostos, direitos ou qualquer outra imposição, contribuição ou encargo devidos à administração pública, a prevenção de danos para a saúde física ou mental em casos de urgência, o auxílio às investigações de erros judiciários, a identificação de uma pessoa que faleceu ou que não está em condições de se identificar a si própria devido a um problema que não resulte de um crime ou delito (como uma catástrofe natural ou um acidente), o exercício de funções relacionadas com a regulamentação dos serviços e dos mercados financeiros ou com a estabilidade financeira, assim como qualquer outro objetivo previsto numa injunção adotada pelo Ministro nos termos da section 22(2) da DRIPA.

38. A legislação nacional não exige que a adoção de uma notificação que ordena a conservação esteja sujeita a uma autorização prévia judicial ou de uma entidade independente. O Ministro deve verificar que a obrigação de conservação é «necessária e proporcionada» para efeitos da prossecução de um ou vários dos objetivos para os quais os dados pertinentes relativos a comunicações podem ser conservados.

2. Quanto ao acesso aos dados conservados

39. Nos termos da section 22(4) da RIPA, as autoridades públicas podem, mediante notificação, exigir que os prestadores de serviços de comunicações lhes transmitam dados relativos a comunicações. A forma e o conteúdo dessas notificações são regulados pela section 23(2) da RIPA. Essa notificação tem uma duração que é limitada no tempo por disposições relativas à sua revogação e à sua renovação.

40. A obtenção dos dados relativos a comunicações deve ser necessária e proporcionada à prossecução de um ou de vários dos objetivos que figuram na section 22 da RIPA, que correspondem aos objetivos que podem justificar a conservação dos dados descritos no n.º 37 das presentes conclusões.

41. Resulta do Código relativo à obtenção dos dados que é necessária uma ordem judicial em caso de um pedido de acesso apresentado para identificação da fonte de jornalistas, bem como em caso de pedido de acesso formulado por autoridades locais.

42. Excetuadas estas hipóteses, o acesso das autoridades públicas está sujeito à obtenção de uma autorização concedida pelas pessoas designadas para este efeito na autoridade pública em causa. Uma pessoa designada para este efeito é uma pessoa que exerce determinadas funções ou detém um determinado cargo ou uma categoria definido na autoridade pública em causa e que foi designada para efeitos da obtenção de dados relativos às comunicações em conformidade com o Despacho de 2015 que regula os poderes de investigação em matéria de dados relativos às comunicações, conforme alterado.

43. Não é especificamente exigida uma autorização judicial ou de uma entidade independente para o acesso a dados relativos às comunicações protegidas por segredo profissional legal ou aos dados relativos às comunicações de médicos, de membros do Parlamento ou de ministros de cultos. O Código relativo à obtenção dos dados especifica apenas que deve ser concedida uma atenção especial quanto à necessidade e à proporcionalidade de um pedido de acesso a tais dados.

3. Quanto à duração da conservação dos dados

44. A section 1(5) da DRIPA e a disposição 4(2) do Regulamento de 2014 preveem uma duração máxima de conservação dos dados de doze meses. De acordo com o Código das boas práticas relativo à conservação dos dados, este período de tempo não deve ultrapassar o que for necessário e proporcionado. A disposição 6 do Regulamento de 2014 exige que o Ministro reveja as notificações que ordenam a conservação.

4. Quanto à proteção e à segurança dos dados conservados

45. Nos termos da section 1 da DRIPA, os prestadores estão proibidos de divulgar os dados conservados exceto se essa divulgação for conforme com o capítulo 2 da parte 1 da RIPA, com uma decisão judicial ou com qualquer outra autorização ou mandado judicial, ou ainda com um regulamento adotado pelo Ministro em aplicação da secção 1 da DRIPA.

46. Nos termos das disposições 7 e 8 do Regulamento de 2014, os prestadores devem garantir a integridade e a segurança dos dados conservados; protegê-los contra uma destruição acidental ou ilícita, uma perda ou uma alteração acidental, ou uma conservação, um tratamento, um acesso ou uma divulgação não autorizados ou ilícitos; destruir os dados de forma a impossibilitar o acesso a estes nos casos em que a sua conservação deixar de ser autorizada; e implementar sistemas de segurança. A disposição 9 do Regulamento de 2014 atribui ao Information Commissioner (Comissário responsável pela informação) o dever de fiscalizar que os prestadores cumprem estas obrigações.

47. As autoridades às quais os prestadores comunicam os dados relativos às comunicações devem tratar e conservar estes dados, assim como todas as suas cópias, todos os seus excertos e todos os seus resumos de forma segura. Em aplicação do Código relativo à obtenção dos dados, as exigências que figuram na lei relativa à proteção de dados (Data Proteção Act, a seguir «DPA»), que transpôs a Diretiva 95/46, devem ser respeitadas.

48. A RIPA instituiu a figura do Interception of Communications Commissioner (Comissário responsável pela interceção de comunicações, a seguir «Comissário responsável pela interceção de comunicações»), que é responsável pela supervisão independente do exercício e da execução dos poderes e deveres que figuram no capítulo II da parte I da RIPA. O Comissário responsável pela interceção de comunicações não supervisiona a aplicação da section 1 do DRIPA. Deve apresentar regularmente relatórios destinados ao público e ao Parlamento [section 57(2) e section 58 da RIPA] e informar sobre a conservação de registos e a apresentação de relatórios por autoridades públicas (Código relativo à obtenção de dados, pontos 6.1 a 6.8). Podem ser apresentadas queixas ao Investigatory Powers Tribunal (Tribunal responsável pelos poderes de investigação) se existirem suspeitas de que determinados dados foram obtidos de forma inapropriada (section 65 do RIPA).

49. Resulta do Código relativo à obtenção dos dados que o Comissário responsável pela interceção de comunicações não tem competência para remeter um caso àquele Tribunal. Só está autorizado a informar uma pessoa de que existe uma suspeita de um exercício ilícito de poderes no caso de se poder «provar que alguém foi prejudicado por um incumprimento intencional ou por negligência». Todavia, não pode proceder a esta divulgação se esta representar uma ameaça para a segurança nacional, ainda que considere que existiu uma falha intencional ou por negligência.

III – Litígios nos processos principais e questões prejudiciais

A – Processo C-203/15

50. Em 9 de abril de 2014, ou seja, no dia seguinte à prolação do acórdão DRI, a Tele2 Sverige comunicou à PTS a sua decisão de deixar de conservar os dados referidos no capítulo 6 da LEK. Além disso, a Tele2 Sverige ia igualmente eliminar os dados conservados até então ao abrigo deste capítulo. A Tele2 Sverige considerava que a legislação sueca que transpôs a Diretiva 2006/24 não era conforme com a Carta.

51. Em 15 de abril de 2014, a Rikspolisstyrelsen (Direcção-Geral da Polícia Nacional, Suécia, a seguir «RPS») apresentou uma queixa à PTS por a Tele2 Sverige ter deixado de comunicar aos seus serviços os dados relativos a determinadas comunicações eletrónicas. A RPS expôs, na sua queixa, que a recusa da Tele2 Sverige tinha consequências graves para as atividades repressivas da polícia.

52. Por decisão de 27 de junho de 2014, a PTS ordenou que, o mais tardar até 25 de julho de 2014, a Tele2 Sverige voltasse a proceder à conservação de dados, em conformidade com o disposto no § 16 a) do capítulo 6 da LEK e nos §§ 37 a 43 do FEK.

53. A Tele2 Sverige interpôs no Förvaltningsrätten i Stockholm (Tribunal administrativo de Estocolmo, Suécia) recurso da decisão da PTS. Por sentença de 13 de outubro de 2014, o Förvaltningsrätten i Stockholm negou provimento a este recurso.

54. A Tele2 Sverige interpôs recurso da sentença do Förvaltningsrätten i Stockholm no órgão jurisdicional de reenvio tendo pedido a anulação da decisão recorrida.

55. Constatando que existiam argumentos favoráveis e contrários ao facto de uma obrigação de conservação tão ampla como a prevista no § 16 a) do capítulo 6 da LEK ser compatível com as disposições do artigo 15.º, n.º 1, da Diretiva 2002/58, e com as obrigações constantes dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta, o Kammarrätten i Stockholm (Tribunal administrativo de recurso de Estocolmo, Suécia) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) É compatível com o artigo 15.º, n.º 1, da Diretiva 2002/58/CE, à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta [dos Direitos Fundamentais da União Europeia], uma obrigação geral de conservar dados de tráfego relativos a todas as pessoas, a todos os meios de comunicação eletrónica e a todos os dados de tráfego, sem quaisquer distinções, limitações ou exceções, para efeitos do objetivo de combate à criminalidade (conforme descrito [nos n.os 1 a 6 do despacho de reenvio])?

2) Em caso de resposta negativa à primeira questão, pode, não obstante, a conservação ser permitida quando:

   a) o acesso das autoridades nacionais aos dados conservados seja determinado conforme [descrito nos n.os 7 a 24 do despacho de reenvio], e

   b) [as exigências] de segurança sejam regulad[a]s conforme [descrito nos n.os 26 a 31 do despacho de reenvio], e

   c) todos os dados relevantes sejam conservados pelo período de seis meses, calculado a partir do dia em que cessa a comunicação, sendo subsequentemente apagados conforme [descrito no n.º 25 do despacho de reenvio]?»

B – Processo C-698/15

56. T. Watson, P. Brice e G. Lewis interpuseram, na High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) [Tribunal Supremo de Justiça (Inglaterra e País de Gales), Secção do Contencioso Administrativo)], recursos jurisdicionais de fiscalização de legalidade («judicial review») do regime de conservação de dados que figura na section 1 da DRIPA, que autoriza o Ministro a impor aos operadores de telecomunicações públicas a conservação de todos os dados relativos às comunicações por um período máximo de doze meses, estando excluída a conservação do conteúdo das comunicações em causa.

57. Foi admitida a intervenção da Open Rights Group, da Privacy Internacional e da Law Society of England and Wales em cada um destes recursos.

58. Por sentença de 17 de julho de 2015, este órgão jurisdicional constatou que o referido regime não era compatível com o direito da União na medida em que não respeita as exigências constantes do acórdão DRI, que considerou serem aplicáveis às regulamentações dos Estados-Membros em matéria de conservação dos dados relativos às comunicações eletrónicas e de acesso a tais dados. O Ministro interpôs recurso desta sentença no órgão jurisdicional de reenvio.

59. Por acórdão de 20 de novembro de 2015, a Court of Appeal (England & Wales) (Civil Division) [Tribunal de recurso (Inglaterra e País de Gales) (Divisão Cível), Reino Unido] considerou a título provisório que o acórdão DRI não estabelecia exigências imperativas no direito da União com as quais as legislações nacionais se tivessem de conformar, limitando-se aquele acórdão a identificar e a descrever formas de proteção que não figuravam no regime harmonizado da União.

60. Todavia, considerando que as respostas a estas questões do direito da União não eram claras e que eram necessárias para se poder pronunciar nesses processos, a Court of Appeal (England & Wales) (Civil Division) [Tribunal de recurso (Inglaterra e País de Gales) (Divisão Cível) (Reino Unido)] decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) O acórdão [DRI] (incluindo, em especial, os seus n.os 60 a 62) estabelece exigências imperativas de direito da União, aplicáveis ao regime interno de um Estado-Membro que regula o acesso a dados conservados em conformidade com a legislação nacional, a fim de dar cumprimento aos artigos 7.º e 8.º da [Carta]?

2) O acórdão do [DRI] alarga o âmbito de aplicação dos artigos 7.º e/ou 8.º da Carta para além do âmbito de aplicação do artigo 8.º da Convenção Europeia dos Direitos do Homem (a seguir 'CEDH'), tal como definido na jurisprudência do Tribunal Europeu dos Direitos do Homem (a seguir 'TEDH')?»

IV – Tramitação processual no Tribunal de Justiça

61. Os pedidos de decisão prejudicial foram registados na Secretaria do Tribunal de Justiça em 4 de maio de 2015 no processo C-203/15 e em 28 de dezembro de 2015 no processo C-698/15.

62. Por despacho de 1 de fevereiro de 2016, o Tribunal de Justiça decidiu submeter o processo C-698/15 à tramitação acelerada prevista no artigo 105.º, n.º 1, do Regulamento de Processo do Tribunal de Justiça.

63. No processo C-203/15, apresentaram observações escritas a Tele2 Sverige, os Governos belga, checo, dinamarquês, alemão, estónio, irlandês, espanhol, francês, húngaro, neerlandês, sueco e do Reino Unido, assim como a Comissão Europeia.

64. No processo C-698/15, apresentaram observações escritas T. Watson, P. Brice e G. Lewis, a Open Rights Group, a Privacy Internacional, a Law Society of England and Wales, os Governos checo, dinamarquês, alemão, estónio, irlandês, francês, cipriota, polaco, finlandês e do Reino Unido, assim como a Comissão.

65. Por decisão do Tribunal de Justiça de 10 de março de 2016, estes dois processos foram apensos para efeitos da fase oral e do acórdão.

66. Compareceram na audiência de 12 de abril de 2016 para apresentaram as suas observações os representantes da Tele2 Sverige, de T. Watson, de P. Brice e de G. Lewis, da Open Rights Group, da Privacy Internacional e da Law Society of England and Wales, dos Governos checo, dinamarquês, alemão, estónio, irlandês, espanhol, francês, finlandês, sueco e do Reino Unido, bem como da Comissão.

V – Análise das questões prejudiciais

67. Com a primeira questão colocada no processo C-203/15, o órgão jurisdicional de reenvio pergunta ao Tribunal de Justiça se, à luz do acórdão DRI, o artigo 15.º, n.º 1, da Diretiva 2002/58, bem como os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, devem ser interpretados no sentido de que se opõem a que um Estado-Membro imponha aos prestadores uma obrigação geral de conservação de dados, como as que estão em causa nos litígios nos processos principais, independentemente de eventuais garantias que acompanhem esta obrigação.

68. Na hipótese de a resposta a esta questão ser negativa, a segunda questão colocada no processo C-203/15 e a primeira questão colocada no processo C-698/15 visam determinar se estas disposições devem ser interpretadas no sentido de que se opõem a que um Estado-Membro imponha aos prestadores uma obrigação geral de conservação de dados quando esta obrigação não seja acompanhada de todas as garantias enunciadas pelo Tribunal de Justiça nos n.ºs 60 a 68 do acórdão DRI, respeitantes ao acesso aos dados, à duração da conservação, bem como à proteção e à segurança dos dados.

69. Na medida em que estas três questões estão intimamente ligadas, irei, em seguida, apreciá-las conjuntamente na minha exposição.

70. Em contrapartida, a segunda questão colocada no processo C-698/15 requer um tratamento autónomo. Com esta questão, o órgão jurisdicional de reenvio pergunta ao Tribunal de Justiça se o acórdão DRI alargou o âmbito de aplicação dos artigos 7.º e/ou 8.º da Carta para além do âmbito de aplicação do artigo 8.º da CEDH. Exporei, na secção seguinte, as razões pelas quais considero que esta questão deve ser julgada inadmissível.

71. Antes de iniciar a apreciação destas questões, creio que é útil recordar o tipo de dados visados pelas obrigações de conservação em causa nos litígios nos processos principais. De acordo com as constatações efetuadas pelos órgãos jurisdicionais de reenvio, o alcance destas obrigações é, no essencial, equivalente ao da obrigação que estava prevista no artigo 5.º da Diretiva 2006/24[8]. De forma esquemática, os dados relativos às comunicações que constituem o objeto destas obrigações de conservação podem ser organizados em quatro categorias[9]:

— os dados que permitem identificar tanto a fonte como o destino da comunicação;

— os dados que permitem localizar tanto a fonte como o destino da comunicação;

— os dados relativos à data, à hora e à duração da comunicação, e

— os dados que permitem determinar o tipo de comunicação e o tipo de material utilizado.

72. O conteúdo das comunicações está excluído das obrigações gerais de conservação de dados em causa nos processos principais, à imagem do que o artigo 5.º, n.º 2, da Diretiva 2006/24 previa.

A – Quanto à admissibilidade da segunda questão colocada no processo C-698/15

73. A segunda questão colocada no processo C-698/15 convida o Tribunal de Justiça a precisar se o acórdão DRI alarga o âmbito de aplicação dos artigos 7.º e/ou 8.º da Carta para além do âmbito de aplicação do artigo 8.º da CEDH conforme interpretado pelo Tribunal EDH.

8 — Esta equivalência é compreensível uma vez que esses regimes nacionais visavam transpor esta diretiva que foi julgada inválida.

9 — V. a descrição dos regimes nacionais em causa nos litígios processos principais nos n.ºs 11 a 13 e 36 das presentes conclusões.

74. Esta questão reflete nomeadamente um argumento invocado pelo Ministro perante o órgão jurisdicional de reenvio, segundo o qual a jurisprudência do Tribunal EDH não exige, por um lado, que o acesso aos dados seja subordinado à autorização prévia de um órgão independente nem, por outro, que a conservação e o acesso a estes dados estejam limitados à luta contra as infrações graves.

75. Considero que esta questão deve ser julgada inadmissível pelos seguintes motivos. É evidente que os fundamentos e a solução adotados pelo Tribunal de Justiça no acórdão DRI revestem uma importância determinante para decidir os litígios nos processos principais. No entanto, o facto de este acórdão ter eventualmente alargado o âmbito de aplicação dos artigos 7.º e/ou 8.º da Carta para além do âmbito de aplicação do artigo 8.º da CEDH não é, por si só, relevante para decidir estes litígios.

76. A este respeito, importa recordar que, em conformidade com o artigo 6.º, n.º 3, TUE, os direitos fundamentais, conforme garantidos pela CEDH, fazem parte do direito da União enquanto princípios gerais. Todavia, não tendo a União aderido a tal Convenção, esta não constitui um instrumento jurídico formalmente integrado na ordem jurídica da União [10].

77. É certo que o primeiro período do artigo 52.º, n.º 3, da Carta estabelece uma regra de interpretação segundo a qual, na medida em que a Carta contém direitos que correspondem a direitos garantidos pela CEDH, «o sentido e o âmbito desses direitos são iguais aos conferidos por essa Convenção».

78. Todavia, de acordo com o segundo período do artigo 52.º, n.º 3, da Carta, «[e]sta disposição não obsta a que o direito da União confira uma proteção mais ampla». Em meu entender, resulta deste período que o Tribunal de Justiça pode, se o considerar necessário no contexto do direito da União, alargar o âmbito de aplicação das disposições da Carta para além do âmbito de aplicação das disposições correspondentes da CEDH.

79. Acrescento, a título subsidiário, que o artigo 8.º da Carta, interpretado pelo Tribunal de Justiça no acórdão DRI, consagra um direito que não corresponde a nenhum direito garantido pela CEDH, ou seja, um direito à proteção dos dados pessoais, o que, de resto, é confirmado pelas explicações relativas ao artigo 52.º da Carta [11]. Por conseguinte, a regra de interpretação consagrada no artigo 52.º, n.º 3, primeiro período, da Carta não é, em caso nenhum, aplicável à interpretação do artigo 8.º da Carta, conforme foi observado por P. Brice e G. Lewis, pela Open Rights Group e pela Privacy Internacional, pela Law Society of England and Wales, bem como pelos Governos checo, irlandês e finlandês.

80. Decorre do que precede que o direito da União não se opõe a que os artigos 7.º e 8.º da Carta concedam uma proteção mais ampla do que a prevista na CEDH. Por conseguinte, o facto de o acórdão DRI ter eventualmente alargado o âmbito de aplicação destas disposições da Carta para além do âmbito de aplicação do artigo 8.º da CEDH não é, por si só, relevante para decidir os litígios nos processos principais. A solução a dar a estes litígios depende essencialmente dos requisitos segundo os quais uma obrigação geral de conservação de dados pode ser considerada compatível com o artigo 15.º, n.º 1, da Diretiva 2002/58 bem como com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, interpretados à luz do acórdão DRI, questão que constitui precisamente o objeto das três outras questões colocadas nos presentes processos.

10 — Parecer 2/13, de 18 de dezembro de 2014 (EU:C:2014:2454, n.º 179), e acórdão de 15 de fevereiro de 2016, N. (C-601/15 PPU, EU:C:2016:84, n.º 45 e jurisprudência referida).

11 — Em conformidade com o artigo 6.º, n.º 1, terceiro parágrafo, TUE e com o artigo 52.º, n.º 7, da Carta, as explicações relativas à Carta devem ser tidas em consideração para efeitos da sua interpretação (v. acórdãos de 26 de fevereiro de 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, n.º 20, e de 15 de fevereiro de 2016, N., C-601/15 PPU, EU:C:2016:84, n.º 47). De acordo com estas explicações, o artigo 7.º da Carta corresponde ao artigo 8.º da CEDH, ao passo que o artigo 8.º da Carta não corresponde a nenhum direito da CEDH.

81. Segundo jurisprudência constante, o indeferimento de um pedido apresentado por um órgão jurisdicional nacional só é possível se resultar de forma manifesta que a interpretação solicitada do direito da União não tem nenhuma relação com a realidade ou com o objeto do litígio no processo principal, ou ainda quando o problema é de natureza hipotética ou o Tribunal de Justiça não disponha dos elementos de facto e de direito necessários para responder utilmente às questões que lhe são submetidas [12].

82. No presente caso, e pelos motivos expostos anteriormente, a segunda questão colocada no processo C-698/15 reveste, em minha opinião, um interesse meramente teórico, uma vez que uma eventual resposta a esta questão não permite deduzir elementos de interpretação do direito da União que o órgão jurisdicional de reenvio pudesse aplicar utilmente para resolver, em função deste direito, o litígio que lhe foi submetido [13].

83. Nestas condições, considero que a referida questão deve ser julgada inadmissível, como alegam corretamente T. Watson, a Law Society of England and Wales e o Governo checo.

B – Quanto à compatibilidade de uma obrigação geral de conservação de dados com o regime estabelecido pela Diretiva 2002/58

84. A presente secção diz respeito à possibilidade de os Estados-Membros utilizarem a faculdade prevista no artigo 15.º, n.º 1, da Diretiva 2002/58 para imporem uma obrigação geral de conservação de dados. Em contrapartida, não examina as exigências específicas que devem ser respeitadas pelos Estados-Membros que pretendam utilizar esta faculdade, que serão amplamente analisadas noutra secção [14].

85. Com efeito, a Open Rights Group e a Privacy Internacional alegaram que tal obrigação é incompatível com o regime harmonizado estabelecido pela Diretiva 2002/58, independentemente do respeito das exigências que decorrem do artigo 15.º, n.º 1, da Diretiva 2002/58, por reduzir a nada a essência dos direitos e do regime estabelecidos nesta diretiva.

86. Antes de examinar este argumento, importa verificar se uma obrigação geral de conservação de dados está abrangida pelo âmbito de aplicação desta diretiva.

1. Quanto à inclusão de uma obrigação geral de conservação de dados no âmbito de aplicação da Diretiva 2002/58

87. Nenhuma das partes que apresentou observações ao Tribunal de Justiça contestou que uma obrigação geral de conservação de dados, como as que estão em causa nos litígios nos processos principais, está abrangida pelo conceito de «tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na [União]» na aceção do artigo 3.º da Diretiva 2002/58.

88. Todavia, os Governos checo, francês, polaco e do Reino Unido alegaram que uma obrigação geral de conservação de dados está abrangida pela exclusão prevista no artigo 1.º, n.º 3, da Diretiva 2002/58. Por um lado, as disposições nacionais que regulam o acesso aos dados e a exploração destes pelas autoridades policiais ou judiciárias dos Estados-Membros dizem respeito à segurança pública, à defesa

12 — V. nomeadamente acórdãos de 9 de novembro de 2010, Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662, n.º 40 e jurisprudência referida), assim como de 24 de abril de 2012, Kamberaj (C-571/10, EU:C:2012:233, n.º 42 e jurisprudência referida).

13 — V. nomeadamente acórdão de 16 de setembro de 1982, Vlaeminck (132/81, EU:C:1982:294, n.º 13); despacho de 24 de março de 2011, Abt e o. (C-194/10, EU:C:2011:182, n.ºs 36 e 37 e jurisprudência referida), e acórdão de 24 de outubro de 2013, Stoilov i Ko (C-180/12, EU:C:2013:693, n.º 46 e jurisprudência referida).

14 — V. n.ºs 126 a 262 das presentes conclusões.

ou à segurança do Estado ou estão, pelo menos, estão relacionadas com o direito penal. Por outro, a conservação dos dados tem como único objetivo permitir que estas autoridades policiais ou judiciárias acedam a tais dados e os explorem. Por conseguinte, uma obrigação de conservação dos dados está excluída do âmbito de aplicação desta diretiva, em aplicação da disposição acima referida.

89. Este raciocínio não me convence pelos seguintes motivos.

90. Em primeiro lugar, a redação do artigo 15.º, n.º 1, da Diretiva 2002/58 confirma que as obrigações de conservação impostas pelos Estados-Membros estão abrangidas pelo âmbito de aplicação desta diretiva. Com efeito, nos termos desta disposição «[o]s Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número». Parece-me que é, no mínimo, difícil afirmar que as obrigações de conservação estão excluídas do âmbito de aplicação desta diretiva uma vez que o artigo 15.º, n.º 1, da referida diretiva regula a faculdade de adotar tais obrigações.

91. Na realidade, como alegam T. Watson, P. Brice e G. Lewis, os Governos belga, dinamarquês, alemão, finlandês, bem como a Comissão, uma obrigação geral de conservação de dados, como as que estão em causa nos litígios nos processos principais, constitui uma implementação do artigo 15.º, n.º 1, da Diretiva 2002/58.

92. Em segundo lugar, a circunstância de as disposições que regulam o acesso poderem estar abrangidas pela exclusão constante do artigo 1.º, n.º 3, da Diretiva 2002/58 [15] não implica que a obrigação de conservação também esteja abrangida e que fique, assim, fora do âmbito de aplicação desta diretiva.

93. A este respeito, o Tribunal de Justiça já teve oportunidade de precisar que as atividades mencionadas no artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46/CE [16], cuja redação tem um alcance equivalente ao alcance do artigo 1.º, n.º 3, da Diretiva 2002/58, eram atividades próprias dos Estados ou das autoridades estatais e alheias aos domínios de atividade dos particulares [17].

94. Ora, as obrigações de conservação em causa nos litígios nos processos principais são impostas a operadores privados no âmbito de atividades privadas de prestações de serviços de comunicações eletrónicas, conforme a Comissão salientou. Além disso, estas obrigações impõem-se independentemente de qualquer pedido de acesso por parte das autoridades policiais ou judiciárias, assim como, de forma mais genérica, de qualquer ato das autoridades estatais relativo à segurança pública, à defesa, à segurança do Estado ou ao direito penal.

95. Em terceiro lugar, a solução adotada pelo Tribunal de Justiça no acórdão Irlanda/Parlamento e Conselho confirma que uma obrigação geral de conservação de dados não está abrangida pelo domínio penal [18]. Com efeito, o Tribunal de Justiça declarou que a Diretiva 2006/24, que previa tal obrigação, não estava abrangida pelo domínio penal mas sim pelo funcionamento do mercado interno, pelo que o artigo 95.º CE (atual artigo 114.º TFUE) constituía a base jurídica adequada para a adoção desta diretiva.

15 — V. n.os 123 a 125 das presentes conclusões.

16 — Diretiva do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31).

17 — Acórdão de 6 de novembro de 2003, Lindqvist (C-101/01, EU:C:2003:596, n.os 43 e 44).

18 — Acórdão de 10 de fevereiro de 2009 (C-301/06, EU:C:2009:68).

96. Para chegar a esta conclusão, o Tribunal de Justiça constatou, nomeadamente, que as disposições desta diretiva estavam essencialmente limitadas às atividades dos prestadores e não regulamentavam o acesso aos dados nem a exploração destes pelas autoridades policiais ou judiciárias dos Estados-Membros [19]. Daqui deduzo que disposições de direito nacional que estabelecem uma obrigação de conservação semelhante à prevista na Diretiva 2006/24 também não estão abrangidas pelo domínio penal.

97. Atendendo ao que precede, entendo que uma obrigação geral de conservação de dados não está abrangida pela exclusão estabelecida no artigo 1.º, n.º 3, da Diretiva 2002/58 pelo que, por conseguinte, se inclui no âmbito de aplicação desta diretiva.

2. Quanto à possibilidade de derrogar o regime estabelecido pela Diretiva 2002/58 através do estabelecimento de uma obrigação geral de conservação de dados

98. Importa agora determinar se uma obrigação geral de conservação de dados é compatível com o regime estabelecido na Diretiva 2002/58.

99. A questão que se coloca a este respeito é a de saber se um Estado-Membro pode utilizar a faculdade conferida pelo artigo 15.º, n.º 1, da Diretiva 2002/58 para impor tal obrigação.

100. Foram apresentados quatro argumentos contra tal possibilidade, nomeadamente pela Open Rights Group e pela Privacy Internacional.

101. De acordo com um primeiro argumento, conceder aos Estados-Membros poder para adotar uma obrigação geral de conservação de dados poria em causa o objetivo de harmonização que constitui a razão de ser da Diretiva 2002/58. Com efeito, nos termos do seu artigo 1.º, n.º 1, esta diretiva prevê a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e para garantir a livre circulação desses dados e dos equipamentos e serviços de comunicações eletrónicas na União.

102. Deste modo, o artigo 15.º, n.º 1, da Diretiva 2002/58 não pode ser interpretado no sentido de que confere aos Estados-Membros poderes para adotarem uma exceção ao regime estabelecido por esta diretiva de tal modo ampla que este esforço de harmonização ficaria privado de qualquer efeito útil.

103. De acordo com um segundo argumento, a redação do artigo 15.º, n.º 1, da Diretiva 2002/58 também se opõe a uma interpretação assim tão ampla do poder de os Estados-Membros consagrarem uma exceção ao regime previsto nesta diretiva. Com efeito, nos termos desta disposição «os Estados-Membros podem adotar medidas legislativas para *restringir o âmbito* dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1 a 4 do artigo 8.º e no artigo 9.º [desta] diretiva» (o sublinhado é nosso).

104. Ora, uma obrigação geral de conservação de dados não se limita a «restringir o âmbito» dos direitos e das obrigações referidos nesta disposição, mas reduziria a zero esses direitos e obrigações. Assim sucederia quanto:

— à obrigação de garantir a confidencialidade dos dados relativos ao tráfego e à obrigação de sujeitar o armazenamento de informações ao consentimento do utilizador, previstas respetivamente no artigo 5.º, n.ºs 1 e 3, da Diretiva 2002/58;

19 — Acórdão de 10 de fevereiro de 2009, Irlanda/Parlamento e Conselho (C-301/06, EU:C:2009:68, n.º 80).

— à obrigação de eliminar ou de tornar anónimos os dados relativos ao tráfego, inscrita no artigo 6.º, n.º 1, desta diretiva, e

— à obrigação de tornar anónimos os dados de localização ou de obter o consentimento do utilizador para tratar estes dados, imposta pelo artigo 9.º, n.º 1, da referida diretiva.

105. Sou da opinião de que estes dois primeiros argumentos devem ser rejeitados pelos seguintes motivos.

106. Por um lado, a redação do artigo 15.º, n.º 1, da Diretiva 2002/58 prevê a possibilidade de os Estados-Membros adotarem «medidas legislativas prevendo que os dados sejam conservados durante um período limitado». Esta referência explícita às obrigações de conservação de dados confirma que tais obrigações não são, por si só, incompatíveis com o regime estabelecido pela Diretiva 2002/58. Embora esta formulação não preveja expressamente a possibilidade de adotar uma obrigação *geral* de conservação de dados, há que constatar que também não se opõe a tal obrigação.

107. Por outro lado, o considerando 11 da Diretiva 2002/58 precisa que esta não altera «o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.º 1 do artigo 15.º [desta] diretiva, necessários para a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal». Por conseguinte, «[a referida] diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a [CEDH]».

108. Em meu entender, resulta deste considerando 11 que o legislador da União não tinha intenção de afetar a faculdade de os Estados-Membros adotarem as medidas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58, mas sim sujeitar esta faculdade a algumas exigências respeitantes, nomeadamente, às finalidades prosseguidas e à proporcionalidade destas medidas. Por outras palavras, uma obrigação geral de conservação de dados não é, em minha opinião, incompatível com o regime estabelecido por esta diretiva, desde que cumpra determinados requisitos.

109. De acordo com um terceiro argumento, o artigo 15.º, n.º 1, da Diretiva 2002/58 deve, enquanto exceção ao regime estabelecido por esta diretiva, ser objeto de uma interpretação estrita, ao abrigo de uma regra de interpretação que resulta de jurisprudência constante do Tribunal de Justiça. Esta regra de interpretação estrita proíbe que tal disposição seja interpretada no sentido de que oferece a faculdade de impor uma obrigação geral de conservação de dados.

110. A este respeito, sou da opinião que a faculdade prevista no artigo 15.º, n.º 1, da Diretiva 2002/58 não pode ser qualificada de exceção e, consequentemente, não pode ser interpretada de forma estrita, como a Comissão alega acertadamente. Com efeito, parece-me difícil qualificar esta faculdade de exceção à luz do considerando 11 acima referido, segundo o qual esta diretiva não afeta a faculdade de os Estados-Membros adotarem as medidas enunciadas nesta disposição. Além disso, observo que o artigo 15.º da referida diretiva tem por epígrafe «Aplicação de determinadas disposições da Diretiva 95/46», ao passo que o artigo 10.º desta mesma diretiva tem explicitamente por epígrafe «Exceções». Estas epígrafes confortam a minha opinião de que a faculdade prevista no referido artigo 15.º não pode ser qualificada de «exceção».

111. Em conformidade com um quarto e último argumento, a incompatibilidade de uma obrigação geral de conservação de dados com o regime estabelecido na Diretiva 2002/58 é corroborada pelo facto de lhe ter sido aditado o artigo 15.º, n.º 1-A desta diretiva por ocasião da adoção da Diretiva 2006/24, invalidada pelo acórdão DRI. Segundo este argumento, foi esta incompatibilidade que conduziu o legislador da União a declarar o artigo 15.º, n.º 1, da Diretiva 2002/58 inaplicável ao regime de conservação geral previsto na Diretiva 2006/24.

112. Parece-me que este argumento decorre de uma compreensão errada do âmbito do artigo 15.º, n.º 1-A, da Diretiva 2002/58. Nos termos desta disposição, «[o artigo 15.º, n.º 1, da Diretiva 2002/58] não é aplicável aos dados cuja conservação seja especificamente exigida pela Diretiva [2006/24], para os fins mencionados no n.º 1 do artigo 1.º [desta] diretiva».

113. A minha leitura desta disposição é a seguinte. No que respeita aos dados cuja conservação era exigida pela Diretiva 2006/24 e para os efeitos estabelecidos por esta, os Estados-Membros perdiam a faculdade, prevista no artigo 15.º, n.º 1, da Diretiva 2002/58, de limitar ainda mais o âmbito dos direitos e das obrigações visados por esta disposição, nomeadamente através de obrigações complementares de conservação de dados. Por outras palavras, o artigo 15.º, n.º 1-A previa uma harmonização exaustiva no que respeita os dados cuja conservação era exigida pela Diretiva 2006/24 e para os efeitos estabelecidos por esta.

114. Esta interpretação é confirmada pelo considerando 12 da Diretiva 2006/24, segundo o qual «o n.º 1 do artigo 15.º da Diretiva [2002/58] *continua a ser aplicável* aos dados, incluindo os relativos a chamadas telefónicas falhadas, cuja conservação não seja especificamente exigida pela presente diretiva e *que, por conseguinte, não são abrangidos pelo seu âmbito de aplicação*, bem como à conservação *para efeitos não contemplados pela presente diretiva*, incluindo fins judiciais» (o sublinhado é nosso).

115. Deste modo, a inserção do artigo 15.º, n.º 1-A, da Diretiva 2002/58 não confirma a incompatibilidade de uma obrigação geral de conservação de dados com o regime estabelecido por esta diretiva, mas sim a vontade de o legislador da União proceder a uma harmonização exaustiva aquando da adoção da Diretiva 2006/24.

116. Atendendo ao que precede, considero que uma obrigação geral de conservação de dados é compatível com o regime estabelecido pela Diretiva 2002/58 e que, por conseguinte, um Estado-Membro pode utilizar a faculdade conferida pelo artigo 15.º, n.º 1, desta diretiva para impor tal obrigação [20]. O recurso a esta faculdade está, no entanto, sujeito ao respeito de exigências estritas, que decorrem não apenas desta disposição, mas também das disposições relevantes da Carta lidas à luz do acórdão DRI, que serão analisadas noutra secção [21].

C – Quanto à aplicabilidade da Carta a uma obrigação geral de conservação de dados

117. Antes de apreciar o teor das exigências que são impostas pela Carta, em conjugação com o artigo 15.º, n.º 1, da Diretiva 2002/58, quando um Estado opta por instaurar uma obrigação geral de conservação de dados, há que verificar se a Carta é efetivamente aplicável a esta obrigação.

118. A aplicabilidade da Carta a uma obrigação geral de conservação de dados depende essencialmente da aplicabilidade da Diretiva 2002/58 a tal obrigação.

20 — Uma vez que a Diretiva 2002/58 pode ser qualificada de «lex specialis» em relação à Diretiva 95/46 (v., a este respeito, artigo 1.º, n.º 2, da Diretiva 2002/58), penso que não é necessário verificar a compatibilidade de uma obrigação geral de conservação de dados com o regime estabelecido pela Diretiva 95/46, que, de resto, não é objeto das questões colocadas ao Tribunal de Justiça. Para ser rigoroso, quero, não obstante, precisar que a redação do artigo 13.º, n.º 1, da Diretiva 95/46 oferece uma maior margem de discricionariedade aos Estados-Membros do que a que é oferecida pelo artigo 15.º, n.º 1, da Diretiva 2002/58, que precisa o respetivo âmbito no quadro da prestação de serviços de comunicações eletrónicas acessíveis ao público. Na medida em que a faculdade prevista no artigo 15.º, n.º 1, da Diretiva 2002/58 permite a adoção, por um Estado-Membro, de uma obrigação geral de conservação de dados, daqui deduzo que o artigo 13.º, n.º 1, da Diretiva 95/46 também o permite.

21 — V. n.os 126 a 262 das presentes conclusões.

119. Com efeito, nos termos do seu artigo 51.º, n.º 1, primeiro período, «as disposições da presente Carta tem por destinatários [...] os Estados-Membros apenas [...] quando apliquem o direito da União». As explicações relativas ao artigo 51.º da Carta remetem, a este respeito, para a jurisprudência do Tribunal de Justiça segundo a qual a obrigação de respeitar os direitos fundamentais definidos no quadro da União só se impõe aos Estados-Membros quando estes agem dentro do âmbito de aplicação do direito da União [22].

120. Os Governos checo, francês, polaco e do Reino Unido, que contestaram a aplicabilidade da Diretiva 2002/58 a uma obrigação geral de conservação de dados [23], alegaram igualmente que a Carta não é aplicável a tal obrigação.

121. Já apresentei as razões pelas quais considero que uma obrigação geral de conservação de dados constitui uma aplicação da faculdade prevista no artigo 15.º, n.º 1, da Diretiva 2002/58 [24].

122. Por conseguinte, considero que as disposições da Carta são aplicáveis às medidas nacionais que instauram tal obrigação, em aplicação do artigo 51.º, n.º 1, da Carta, conforme alegam T. Watson, P. Brice e G. Lewis, a Open Rights Group e a Privacy Internacional, os Governos dinamarquês, alemão, finlandês, bem como a Comissão [25].

123. Esta conclusão não é posta em causa pelo facto de as disposições nacionais que regulam o acesso aos dados conservados não estarem abrangidas, enquanto tais, pelo âmbito de aplicação da Carta.

124. É certo que na medida em que dizem respeito às «atividades do Estado em matéria de direito penal», as disposições nacionais que regulam o acesso aos dados conservados pelas autoridades policiais ou judiciárias para lutar contra as infrações graves estão abrangidas, em meu entender, pela exclusão prevista no artigo 1.º, n.º 3, da Diretiva 2002/58 [26]. Por conseguinte, uma vez que tais disposições nacionais não aplicam o direito da União, a Carta não lhes é aplicável.

125. Não obstante, uma obrigação de conservação de dados tem por razão de ser permitir que as autoridades repressivas acedam aos dados conservados, pelo que as problemáticas da conservação e do acesso dela não podem ser completamente dissociadas. Como a Comissão sublinhou acertadamente, as disposições que regulam o acesso revestem uma importância determinante para apreciar a compatibilidade com a Carta das disposições que instauram uma obrigação geral de conservação de dados, as quais implementam o artigo 15.º, n.º 1, da Diretiva 2002/58. Mais precisamente, as disposições que regulam o acesso devem ser tidas em conta na apreciação da necessidade e da proporcionalidade de tal obrigação [27].

22 — Com efeito, resulta de jurisprudência constante do Tribunal de Justiça que os direitos fundamentais garantidos pela ordem jurídica da União são aplicáveis a todas as situações reguladas pelo direito da União, mas não fora dessas situações. É nesta medida que o Tribunal de Justiça já recordou que não pode apreciar, à luz da Carta, uma regulamentação nacional que não se enquadra no âmbito do direito da União. Em contrapartida, quando uma regulamentação nacional se enquadra no âmbito de aplicação deste direito, o Tribunal de Justiça, chamado a pronunciar-se sobre uma questão prejudicial, deve fornecer todos os elementos de interpretação necessários à apreciação, pelo órgão jurisdicional nacional, da conformidade desta regulamentação com os direitos fundamentais cujo respeito assegura (v. acórdão de 26 de fevereiro de 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, n.º 19 e jurisprudência referida).

23 — V. n.º 88 das presentes conclusões.

24 — V. n.os 90 a 97 das presentes conclusões.

25 — De forma mais precisa, o artigo 51.º, n.º 1, segundo período, da Carta dispõe que os Estados-Membros devem respeitar os direitos garantidos por esta quando aplicam o direito da União.

26 — Quanto ao âmbito desta exclusão, v. n.os 90 a 97 das presentes conclusões.

27 — V. n.os 185 a 262 das presentes conclusões.

D – Quanto à compatibilidade de uma obrigação geral de conservação de dados com as exigências estabelecidas no artigo 15.º, n.º 1, da Diretiva 2002/58, bem como nos artigos 7.º, 8.º e 52.º, n.º 1, da Carta

126. Resta-me, agora, abordar a difícil questão da compatibilidade de uma obrigação geral de conservação de dados com as exigências estabelecidas no artigo 15.º, n.º 1, da Diretiva 2002/58 e nos artigos 7.º, 8.º e 52.º, n.º 1, da Carta, lidos à luz do acórdão DRI. Esta questão diz respeito, de forma mais geral, à necessária adaptação do quadro legal que regula as capacidades de vigilância dos Estados, que se multiplicaram com os recentes progressos tecnológicos [28].

127. Neste contexto, a primeira etapa de qualquer análise reside na constatação de ingerências nos direitos consagrados pela Diretiva 2002/58 e nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta.

128. Com efeito, tal obrigação constitui uma ingerência grave no direito ao respeito pela vida privada, consagrado no artigo 7.º da Carta, e no direito à proteção dos dados pessoais, garantido pelo artigo 8.º da Carta. Não creio que seja útil lamentar-me sobre esta constatação de ingerência, que foi claramente abordada pelo Tribunal de Justiça nos n.os 32 a 37 do acórdão DRI [29]. Do mesmo modo, uma obrigação geral de conservação de dados constitui uma ingerência em vários direitos consagrados na Diretiva 2002/58 [30].

129. A segunda etapa da análise consiste em determinar se, e em que condições, esta ingerência grave nos direitos consagrados na Diretiva 2002/58, assim como nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, pode ser justificada.

130. Duas disposições preveem os requisitos que devem ser preenchidos para que esta dupla ingerência seja justificada: o artigo 15.º, n.º 1, da Diretiva 2002/58, que enquadra a faculdade de os Estados-Membros restringirem o âmbito de certos direitos estabelecidos nesta diretiva, e o artigo 52.º, n.º 1, da Carta, lido à luz do acórdão DRI, que enquadra toda as restrições ao exercício dos direitos consagrados na Carta.

131. Importa sublinhar que estas exigências são *cumulativas*. Com efeito, o respeito das exigências estabelecidas no artigo 15.º, n.º 1, da Diretiva 2002/58 não implica, por si só, que as exigências previstas no artigo 52.º, n.º 1, da Carta estejam satisfeitas, e inversamente [31]. Por conseguinte, uma obrigação geral de conservação de dados só pode ser considerada compatível com o direito da União se respeitar simultaneamente as exigências estabelecidas no artigo 15.º, n.º 1, da Diretiva 2002/58 e as exigências previstas no artigo 52.º, n.º 1, da Carta, conforme sublinhou a Law Society of England and Wales [32].

28 — V. nomeadamente Conselho dos Direitos do Homem das Nações Unidas, relatório do relator especial sobre a promoção e a proteção do direito à liberdade de opinião e de expressão, 17 de abril de 2013, A/HRC/23/40, n.º 33: «Os progressos tecnológicos permitem ao Estado exercer atividades de vigilância que já não são limitadas por critérios relativos à escala ou à duração. […] Por conseguinte, o Estado dispõe atualmente e mais do que nunca de meios acrescidos para levar a cabo atividades de vigilância simultâneas, atentatórias da vida privada, direcionadas e em grande escala. […]». V., igualmente n.º 50: «De forma geral, a legislação não seguiu o ritmo das alterações tecnológicas. Na maioria dos Estados, as normas jurídicas são inexistentes ou inadequadas para fazer face às condições modernas de vigilância das comunicações. […]».

29 — Não obstante, retornarei em seguida nas presentes conclusões aos riscos específicos que decorrem da constituição de bases de dados de tal âmbito no quadro da exigência de proporcionalidade, numa sociedade democrática, de uma obrigação geral de conservação de dados como os que estão em causa nos litígios nos processos principais: V. n.os 252 a 261 das presentes conclusões.

30 — V., a este respeito, o argumento invocado pela Open Rights Group e pela Privacy International, resumido no n.º 104 das presentes conclusões.

31 — Esta natureza cumulativa encontra-se confirmada no último período do artigo 15.º, n.º 1, da Diretiva 2002/58, segundo o qual «[t]odas as medidas referidas por [este] número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do TUE». Nos termos do artigo 6.º, n.º 1, TUE, «[a] União reconhece os direitos, as liberdades e os princípios enunciados na [Carta], e que têm o mesmo valor jurídico que os Tratados».

32 — É lógico que resulta desta natureza cumulativa que, na medida em que as exigências estabelecidas por estas duas disposições se sobrepõem, há que aplicar a exigência mais estrita ou, por outras palavras, a exigência mais protetora dos direitos em causa.

132. Em conjunto, estas duas disposições estabelecem seis exigências que devem ser preenchidas para que seja justificada a ingerência originada por uma obrigação geral de conservação de dados:

— a obrigação de conservação deve ter uma base legal;

— deve respeitar o conteúdo essencial dos direitos consagrados na Carta;

— deve prosseguir um objetivo de interesse geral;

— deve ser adequada à prossecução deste objetivo;

— deve ser necessária à prossecução do referido objetivo, e

— deve ser proporcionada, numa sociedade democrática, à prossecução deste mesmo objetivo.

133. No acórdão DRI, o Tribunal de Justiça evocou vários destes requisitos. Por motivos de clareza e tendo em conta as particularidades dos presentes processos face ao processo DRI, pretendo, não obstante, debruçar-me sobre cada um deles, examinando de forma mais detalhada as exigências relativas à base legal, ao caráter necessário, assim como ao caráter proporcionado numa sociedade democrática de uma obrigação geral de conservação de dados.

1. Quanto à exigência de uma base legal no direito nacional

134. Tanto o artigo 52.º, n.º 1, da Carta como o artigo 15.º, n.º 1, da Diretiva 2002/58 estabelecem exigências quanto à base legal que deve ser utilizada por um Estado-Membro para impor uma obrigação geral de conservação de dados.

135. Em primeiro lugar, qualquer restrição ao exercício dos direitos reconhecidos pela Carta deve ser «prevista por lei» nos termos do seu artigo 52.º, n.º 1. Preciso que esta exigência não foi formalmente examinada pelo Tribunal de Justiça no acórdão DRI, que dizia respeito a uma ingerência prevista numa diretiva.

136. Até ao recente acórdão WebMindLicenses [33], o Tribunal de Justiça nunca se tinha pronunciado sobre o âmbito exato de tal exigência, embora tenha constatado expressamente se esta exigência estava [34] ou não estava [35] preenchida. No n.º 81 deste acórdão, a Terceira Secção do Tribunal de Justiça pronunciou-se nos seguintes termos:

«A este respeito, há que sublinhar que o requisito de que qualquer restrição ao exercício deste direito deve ser prevista por lei implica que a base legal que permite a utilização, pela Administração Fiscal, das provas mencionadas no número anterior deve ser suficientemente clara e precisa e que, ao definir ela mesma o alcance da restrição ao exercício do direito garantido pelo artigo 7.º da Carta, oferece uma certa proteção contra eventuais violações arbitrárias desta Administração (v., designadamente, TEDH, Malone c. Reino Unido, de 2 de agosto de 1984, série A, n.º 82, § 67, e Gillan e Quinton c. Reino Unido, de 12 de janeiro de 2010, n.º 4158/05, § 77, TEDH 2010)».

33 — Acórdão de 17 de dezembro de 2015 (C-419/14, EU:C:2015:832).

34 — V., nomeadamente, acórdãos de 17 de outubro de 2013, Schwarz (C-291/12, EU:C:2013:670, n.º 35) (ingerência prevista num regulamento europeu); de 27 de maio de 2014, Spasic (C-129/14 PPU, EU:C:2014:586, n.º 57) (ingerência prevista na Convenção de aplicação do Acordo de Schengen, de 14 de junho de 1985, entre os Governos dos Estados da União Económica Benelux, da República Federal da Alemanha e da República Francesa relativo à supressão gradual dos controlos nas fronteiras comuns, assinada em Schengen em 19 de junho de 1990 e entrada em vigor em 26 de março de 1995); de 6 de outubro de 2015, Delvigne (C-650/13, EU:C:2015:648, n.º 47) (ingerência prevista no Código Eleitoral e no Código Penal francês); e de 17 de dezembro de 2015, Neptune Distribution (C-157/14, EU:C:2015:823, n.º 69) (ingerência prevista num regulamento e numa diretiva europeus).

35 — Acórdão de 1 de julho de 2010, Knauf Gips/Comissão (C-407/08 P, EU:C:2010:389, n.ºs 87 a 92) (ingerência desprovida de base legal).

137. Convido a Grande Secção do Tribunal de Justiça a confirmar esta interpretação nos presentes processos pelos seguintes motivos.

138. Conforme o advogado-geral P. Cruz Villalón afirmou acertadamente nas suas conclusões no processo Scarlet Extended [36], existe no Tribunal EDH abundante jurisprudência relativa a esta exigência no contexto da CEDH, que se caracteriza por uma aceção material e não formal do termo «lei» [37].

139. Segundo esta jurisprudência, a expressão «prevista por lei» implica que a base legal seja suficientemente acessível e previsível, ou seja, formulada com precisão suficiente para permitir que o indivíduo, se necessário através de assessoria jurídica adequada, ajuste a sua conduta. Esta base legal deve fornecer igualmente uma proteção adequada contra o livre arbítrio e, consequentemente, definir com suficiente nitidez a amplitude e as modalidades do exercício do poder conferido às autoridades competentes (princípio do primado do direito) [38].

140. Ora, pelas razões que a seguir apresento, considero que é necessário atribuir à expressão «prevista por lei» utilizada no artigo 52.º, n.º 1, da Carta um alcance semelhante ao que esta expressão reveste no âmbito da CEDH.

141. Por um lado, nos termos do artigo 53.º da Carta e das explicações relativas a este artigo, o nível de proteção oferecido pela Carta nunca pode ser inferior ao que é garantido pela CEDH. Esta proibição de ultrapassar o «limiar CEDH» implica que a interpretação adotada pelo Tribunal de Justiça da expressão «prevista por lei» utilizada no artigo 52.º, n.º 1, da Carta deve ser pelo menos tão estrita como a do Tribunal EDH no âmbito da CEDH [39].

142. Por outro lado, atendendo à natureza horizontal desta exigência, que pode ser aplicada a vários tipos de ingerências tanto no contexto da Carta como no contexto da CEDH [40], não é oportuno sujeitar os Estados-Membros a critérios diferentes consoante a ingerência seja examinada à luz de um ou outro destes instrumentos [41].

143. Por conseguinte, considero, como o Governo estónio e a Comissão alegam, que a expressão «prevista por lei» que consta do artigo 52.º, n.º 1, da Carta deve ser interpretada, à luz da jurisprudência do Tribunal EDH resumida no n.º 139 das presentes conclusões, no sentido de que uma obrigação geral de conservação de dados, como as que estão em causa nos litígios nos processos principais, deve ser prevista numa base legal suficientemente acessível e previsível, por um lado, e que conceda uma proteção adequada contra o livre arbítrio, por outro.

36 — C-70/10, EU:C:2011:255 (n.ºs 94 a 100).

37 — V., nomeadamente, Tribunal EDH, 14 de setembro de 2010, Sanoma Uitgevers B.V. c. Países Baixos, CE:ECHR:2010:0914JUD003822403, § 83.

38 — V., nomeadamente, Tribunal EDH, 26 de março de 1987, Leander c. Suécia, CE:ECHR:1987:0326JUD000924881, §§ 50-51; Tribunal EDH, 26 de outubro de 2000, Hassan e Tchaouch c. Bulgária, CE:ECHR:2000:1026JUD003098596, § 84; Tribunal EDH, 4 de dezembro de 2008, S. e Marper c. Reino Unido, CE:ECHR:2008:1204JUD003056204, § 95; Tribunal EDH, 14 de setembro de 2010, Sanoma Uitgevers B.V. c. Países Baixos, CE:ECHR:2010:0914JUD003822403, § 81-83; Tribunal EDH, 31 de março de 2016, Stoyanov e o. c. Bulgária, CE:ECHR:2016:0331JUD005538810, § 124-126.

39 — Para ser mais preciso, o Tribunal de Justiça não pode, em meu entender, adotar uma interpretação deste requisito mais permissiva do que a do Tribunal EDH, uma vez que tal teria como consequência permitir um número de ingerências mais elevado do que aquele que resultaria da interpretação deste requisito pelo Tribunal EDH.

40 — Esta expressão, «prevista por lei», é utilizada no artigo 8.º, n.º 2 (direito ao respeito pela vida privada e familiar), no artigo 9.º, n.º 2 (liberdade de pensamento, de consciência e de religião), no artigo 10.º, n.º 2 (liberdade de expressão), e no artigo 11.º, n.º 2 (liberdade de reunião e de associação), da CEDH. Neste contexto da Carta, o artigo 52.º, n.º 1, aplica-se a qualquer limitação ao exercício dos direitos consagrados por esta, desde que tal limitação seja permitida.

41 — V., neste sentido, Peers, S., «Article 52 — Scope of guaranteed rights», in Peers, S., e al., *The EU Charter of Fundamental Rights: a Commentary*, Oxford, OUP, 2014, n.º 52.39.

144. Em segundo lugar, importa determinar o teor das exigências impostas no artigo 15.º, n.º 1, da Diretiva 2002/58 no que respeita à base legal que deve ser utilizada por um Estado-Membro que pretenda usar a faculdade conferida por esta disposição.

145. A este respeito, quero sublinhar que existe uma divergência entre as versões linguísticas do primeiro período desta disposição.

146. Nas versões inglesa («*legislative measures*»), francesa («*mesures législatives*»), italiana («*disposizioni legislative*»), portuguesa («*medidas legislativas*»), romena («*măsuri legislative*») e sueca («*genom lagstiftning vidta åtgärder*»), o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 impõe, em meu entender, a adoção de medidas que emanam do poder legislativo.

147. Em contrapartida, as versões dinamarquesa («*retsforskrifter*»), alemã («*Rechtsvorschriften*»), neerlandesa («*wettelijke maatregele*») e espanhola («*medidas legales*») deste período podem ser interpretadas no sentido de que exigem a adoção tanto de medidas que emanam do poder legislativo, como de medidas regulamentares que emanam do poder executivo.

148. Em conformidade com jurisprudência constante, a necessidade de uma aplicação e, por conseguinte, de uma interpretação uniformes de um ato da União exclui a possibilidade de esse ato ser considerado isoladamente numa das suas versões, antes exigindo que seja interpretado em função tanto da vontade efetiva do seu autor como do fim por ele prosseguido, à luz, nomeadamente, das versões em todas as línguas oficiais. Em caso de divergência entre estas, a disposição em causa deve ser interpretada em função da economia geral e da finalidade da regulamentação de que constitui um elemento [42].

149. No caso em apreço, o artigo 15.º, n.º 1, da Diretiva 2002/58 regula a faculdade de os Estados-Membros derrogarem os direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, cuja proteção é instituída por esta diretiva. Por conseguinte, considero que é oportuno interpretar a exigência de uma base legal imposta pelo artigo 15.º, n.º 1, da Diretiva 2002/58 à luz da Carta, e, em particular, do artigo 52.º, n.º 1, desta.

150. Deste modo, as «medidas» exigidas no artigo 15.º, n.º 1, da Diretiva 2002/58 devem imperativamente possuir as qualidades de acessibilidade, de previsibilidade e de proteção adequada contra o livre arbítrio, evocadas no n.º 143 das presentes conclusões. Decorre, designadamente, destas qualidades, em particular da exigência de proteção adequada contra o livre arbítrio, que estas medidas devem ser *vinculativas* para as autoridades nacionais às quais é concedido poder para aceder aos dados conservados. Nomeadamente, não basta que as garantias que envolvem o acesso a estes dados estejam previstas em códigos ou em orientações internas que não possuem tal caráter vinculativo, conforme a Law Society of England and Wales sublinhou acertadamente.

151. Além disso, parece-me que a expressão «[o]s Estados-Membros podem adotar medidas», comum a todas as versões linguísticas do artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58, exclui a possibilidade de que uma jurisprudência nacional, mesmo que constante, possa constituir uma base legal suficiente para implementar esta disposição. Sublinho que, nesta medida, a referida disposição excede as exigências que resultam da jurisprudência do Tribunal EDH [43].

42 — V., nomeadamente, acórdão de 30 de maio de 2013, Asbeek Brusse e de Man Garabito (C-488/11, EU:C:2013:341, n.º 26); de 24 de junho de 2015, Hotel Sava Rogaška (C-207/14, EU:C:2015:414, n.º 26), e de 26 de fevereiro de 2015, Christie's France (C-41/14, EU:C:2015:119, n.º 26).

43 — V., nomeadamente, Tribunal EDH, 14 de setembro de 2010, Sanoma Uitgevers B.V. c. Países Baixos, CE:ECHR:2010:0914JUD003822403, § 83: «[o termo 'lei' que figura nos artigos 8.º a 11.º da CEDH inclui] simultaneamente o 'direito escrito', incluindo tanto os textos de nível infralegislativo como os atos regulamentares adotados por uma ordem profissional, por delegação do legislador, no âmbito do seu poder normativo autónomo, e o 'direito não escrito'. A 'lei' deve ser entendida no sentido de que abrange o texto escrito e o 'direito elaborado' pelos tribunais».

152. Atendendo à gravidade das ingerências que resultam para os direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta de uma obrigação geral de conservação de dados, acrescento que me parece desejável que o conteúdo essencial do regime em causa, nomeadamente o das garantias que envolvem esta obrigação, seja estabelecido numa medida adotada pelo poder legislativo, cabendo ao poder executivo precisar as respetivas modalidades de aplicação.

153. Atendendo ao que precede, considero que o artigo 15.º, n.º 1, da Diretiva 2002/58 e o artigo 52.º, n.º 1, da Carta devem ser interpretados no sentido de que o regime que estabelece uma obrigação geral de conservação de dados, como as que estão em causa nos litígios nos processos principais, deve ser estabelecido através de medidas legislativas ou regulamentares que possuam qualidades de acessibilidade, de previsibilidade e de proteção adequada contra o livre arbítrio.

154. Cabe aos órgãos jurisdicionais de reenvio verificar o respeito desta exigência, atendendo à posição privilegiada que ocupam para avaliar os seus respetivos regimes nacionais.

2. Quanto ao respeito do conteúdo essencial dos direitos reconhecidos nos artigos 7.º e 8.º da Carta

155. Nos termos do seu artigo 52.º, n.º 1, qualquer restrição do exercício dos direitos reconhecidos pela Carta deve «respeitar o conteúdo essencial desses direitos» [44]. Não me parece que este aspeto, que foi examinado pelo Tribunal de Justiça nos n.os 39 e 40 do acórdão DRI no contexto da Diretiva 2006/24, cause problemas especiais no âmbito dos presentes processos, conforme observaram os Governos espanhol e irlandês, bem como a Comissão.

156. No n.º 39 do acórdão DRI, o Tribunal de Justiça declarou que esta diretiva não afetava o conteúdo essencial do direito ao respeito da vida privada e dos outros direitos consagrados no artigo 7.º da Carta, uma vez que não permitia tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal.

157. Esta apreciação é, em meu entender, transponível para os regimes nacionais em causa nos processos principais, uma vez que estes também não permitem tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal [45].

158. No n.º 40 do acórdão DRI, o Tribunal de Justiça considerou que a Diretiva 2006/24 não afetava o conteúdo essencial do direito fundamental à proteção dos dados pessoais, consagrado no artigo 8.º da Carta, atendendo aos princípios de proteção e de segurança dos dados que devem ser respeitados pelos prestadores nos termos do artigo 7.º desta diretiva, cabendo aos Estados-Membros assegurar a adoção de medidas técnicas e organizacionais contra a eliminação acidental ou ilícita, a perda ou a alteração acidental dos dados.

159. Considero, uma vez mais, que esta apreciação é transponível para os regimes nacionais em causa nos processos principais, uma vez que estes preveem, em minha opinião, garantias comparáveis no que respeita à proteção e à segurança dos dados conservados pelos prestadores, devendo estas garantias permitir proteger eficazmente os dados pessoais contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícitos destes dados [46].

44 — Tal exigência não resulta da redação do artigo 15.º, n.º 1, da Diretiva 2002/58, nem da sistematização desta diretiva pelas razões expostas nos n.os 99 a 116 das presentes conclusões.

45 — V. a descrição dos regimes nacionais em causa nos litígios nos processos principais, nomeadamente nos n.os 13 e 36 das presentes conclusões.

46 — Acórdão DRI, n.º 54. V., descrição dos regimes nacionais em causa nos processos principais nos n.os 29 a 33, assim como 45 e 46 das presentes conclusões.

160. Não obstante, cabe aos órgãos jurisdicionais de reenvio verificar se os regimes nacionais em causa nos litígios nos processos principais respeitam efetivamente o conteúdo essencial dos direitos reconhecidos pelos artigos 7.º e 8.º da Carta, à luz das considerações que precedem.

3. Quanto à existência de um objetivo de interesse geral reconhecido pela União suscetível de justificar uma obrigação geral de conservação de dados

161. Tanto o artigo 15.º, n.º 1, da Diretiva 2002/58 como o artigo 52.º, n.º 1, da Carta exigem que qualquer ingerência nos direitos consagrados por estes instrumentos prossiga um objetivo de interesse geral.

162. Nos n.ºs 41 a 44 do acórdão DRI, o Tribunal de Justiça declarou, por um lado, que a obrigação geral de conservação de dados imposta pela Diretiva 2006/24 contribui para «a luta contra a criminalidade grave e, assim, em última análise, para a segurança pública» e, por outro, que esta luta constitui um objetivo de interesse geral da União.

163. Com efeito, resulta da jurisprudência do Tribunal de Justiça que a luta contra o terrorismo internacional, com vista à manutenção da paz e da segurança internacionais, constitui um objetivo de interesse geral da União. O mesmo acontece com a luta contra a criminalidade grave, com o objetivo de garantir a segurança pública. Além disso, importa salientar, a este respeito, que o artigo 6.º da Carta enuncia o direito das pessoas não só à liberdade, mas também à segurança [47].

164. Esta apreciação é transponível para as obrigações gerais de conservação de dados em causa nos litígios nos processos principais, que podem ser justificadas pelo objetivo de luta contra as infrações graves.

165. Não obstante, atendendo a alguns dos argumentos apresentados ao Tribunal de Justiça, importa determinar se tal obrigação pode ser justificada por um objetivo de interesse geral diferente do objetivo da luta contra as infrações graves.

166. A este respeito, a redação do artigo 52.º, n.º 1, da Carta evoca, de forma geral, os «objetivos de interesse geral reconhecidos pela União» e a «necessidade de proteção dos direitos e liberdades de terceiros».

167. A redação do artigo 15.º, n.º 1, da Diretiva 2002/58 é mais precisa quanto aos objetivos suscetíveis de justificar uma ingerência aos direitos estabelecidos por esta diretiva. Com efeito, segundo esta disposição, as medidas em questão devem contribuir para «salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva 95/46».

168. Por outro lado, no acórdão Promusicae [48], o Tribunal de Justiça declarou que esta disposição deve ser interpretada à luz do artigo 13.º, n.º 1, da Diretiva 95/46, que autoriza as exceções aos direitos previstos nesta diretiva quando sejam justificadas pela «proteção dos direitos e liberdades de outrem». Por conseguinte, o Tribunal de Justiça declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58 oferecia aos Estados-Membros a faculdade de preverem a obrigação de um prestador divulgar dados pessoais para efeitos da determinação, no âmbito de um processo cível, da existência de uma afetação dos direitos de autor relativos aos registos musicais e audiovisuais.

47 — Acórdão DRI, n.º 42 e jurisprudência referida.

48 — Acórdão de 29 de janeiro de 2008 (C-275/06, EU:C:2008:54, n.ºs 50 a 54).

169. Baseando-se neste acórdão, o Governo do Reino Unido argumentou que uma obrigação geral de conservação de dados pode ser justificada por qualquer objetivo referido no artigo 15.º, n.º 1, da Diretiva 2002/58 ou no artigo 13.º, n.º 1, da Diretiva 95/46. De acordo com este Governo, tal obrigação pode ser justificada pela utilidade que apresentam os dados conservados para lutar contra infrações «simples» (por oposição às «graves»), ou inclusivamente no contexto de processos não penais relacionados com os objetivos mencionados nestas disposições.

170. Este argumento não me convence pelos seguintes motivos.

171. Em primeiro lugar, como sublinharam acertadamente T. Watson, bem como a Open Rights Group e a Privacy Internacional, a abordagem adotada pelo Tribunal de Justiça no acórdão Promusicae [49] não é transponível para os presentes processos, uma vez que este acórdão dizia respeito a um pedido de acesso, por parte de uma associação de titulares de direitos de autor, a dados conservados espontaneamente por um prestador, a saber, a Telefónica de España. Por outras palavras, este acórdão não dizia respeito aos objetivos suscetíveis de justificar as graves ingerências aos direitos fundamentais que uma obrigação geral de conservação de dados implica, como as que estão em causa nos litígios nos processos principais.

172. Em segundo lugar, considero que a exigência de proporcionalidade numa sociedade democrática exclui que a luta contra infrações simples ou o bom desenrolar de processos não penais possa justificar uma obrigação geral de conservação de dados. Com efeito, os riscos consideráveis que decorrem de tal obrigação são desmesurados face às vantagens que aquela proporciona na luta contra infrações simples ou no contexto de processos não penais [50].

173. Atendendo ao que precede, considero que o artigo 15.º, n.º 1, da Diretiva 2002/58 e o artigo 52.º, n.º 1, da Carta devem ser interpretados no sentido de que a luta contra as infrações graves constitui um objetivo de interesse geral suscetível de justificar uma obrigação geral de conservação de dados, ao contrário da luta contra as infrações simples ou do bom desenrolar de processos não penais.

174. Por conseguinte, há que examinar o caráter adequado, necessário e proporcionado de tal obrigação à luz do objetivo de luta contra as infrações graves.

4. Quanto ao caráter adequado de uma obrigação geral de conservação de dados no que respeita à luta contra as infrações graves

175. As exigências relativas ao caráter adequado, necessário [51] e proporcionado [52] decorrem tanto do artigo 15.º, n.º 1, da Diretiva 2002/58 como do artigo 52.º, n.º 1, da Carta.

176. Por força da primeira destas exigências, uma obrigação geral de conservação de dados como as que estão em causa nos litígios nos processos principais deve ser apta para contribuir para o objetivo de interesse geral acima identificado, a saber, a luta contra as infrações graves.

177. Esta exigência não coloca especiais dificuldades no contexto dos presentes processos. Como o Tribunal de Justiça salientou, em substância, no n.º 49 do acórdão DRI, os dados conservados permitem que as autoridades nacionais competentes em matéria penal disponham de um meio de investigação suplementar para prevenir ou elucidar as infrações graves. Por conseguinte, tal obrigação contribui para a luta contra as infrações graves.

49 — Acórdão de 29 de janeiro de 2008 (C-275/06, EU:C:2008:54).

50 — V. n.os 252 a 261 das presentes conclusões.

51 — Quanto ao caráter necessário, v., n.os 185 a 245 das presentes conclusões.

52 — Quanto ao caráter proporcionado *stricto sensu*, v., n.os 246 a 262 das presentes conclusões.

178. Não obstante, pretendo precisar a utilidade que uma obrigação geral de conservação de dados pode revestir na luta contra as infrações graves. Como o Governo francês alegou acertadamente, tal obrigação permite, em certa medida, que as autoridades repressivas possam «ler o passado» através da consulta dos dados conservados, ao contrário do que sucede com as medidas de vigilância direcionadas.

179. Uma medida de vigilância direcionada aplica-se a pessoas que tenham sido previamente identificadas como podendo estar relacionadas, ainda que indireta ou longínqua, a uma infração grave. Tais medidas direcionadas permitem que as autoridades competentes acedam aos dados relativos às comunicações realizadas por estas pessoas, ou inclusivamente ao conteúdo dessas comunicações. Todavia, este acesso só poderá visar as comunicações realizadas por essas pessoas *depois* de serem identificadas.

180. Em contrapartida, uma obrigação geral de conservação de dados visa todas as comunicações realizadas por todos os utilizadores, sem que se exija uma relação a uma infração grave. Tal obrigação permite que as autoridades competentes acedam ao histórico das comunicações realizadas por uma pessoa antes de esta ter sido identificada como alguém que tem esta relação. É neste sentido que tal obrigação concede às autoridades repressivas uma capacidade limitada de ler o passado, oferecendo-lhes um acesso às comunicações realizadas por essas pessoas *antes* de terem sido identificadas [53].

181. Por outras palavras, a utilidade que uma obrigação geral de conservação de dados assume para efeitos da luta contra as infrações graves reside nesta capacidade limitada de ler o passado através de dados que reconstituem o histórico das comunicações realizadas por uma pessoa inclusivamente antes de esta ser suspeita de ter uma relação a uma infração grave [54].

182. Aquando da apresentação da proposta de diretiva que conduziu à adoção da Diretiva 2006/24, a Comissão ilustrou esta utilidade através de vários exemplos concretos de investigações relativas, nomeadamente, a atos de terrorismo, de homicídio, de sequestro e de pornografia infantil [55].

183. Vários exemplos semelhantes foram expostos ao Tribunal de Justiça no âmbito dos presentes processos, nomeadamente pelo Governo francês, que sublinhou a obrigação positiva que incumbe aos Estados-Membros de garantirem a segurança das pessoas que se encontram no seu território. De acordo com este governo, no âmbito das investigações relativas ao desmantelamento das redes que organizam a partida de residentes franceses para zonas de conflito no Iraque ou na Síria, o acesso aos dados conservados desempenha um papel determinante para identificar as pessoas que facilitaram essas partidas. O referido Governo acrescenta que o acesso aos dados relativos às comunicações das pessoas envolvidas nos recentes atentados terroristas de janeiro e de novembro de 2015 em França foi de

53 — A Comissão também sublinhou que o valor acrescentado de uma obrigação geral de conservação de dados, em relação a uma conservação direcionada de dados, reside nesta capacidade limitada de ler o passado: v. Commission Staff Working Document apresentado em anexo à proposta de diretiva que conduziu à adoção da Diretiva 2006/24, SEC (2005) 1131, 21 de setembro de 2005, n.º 3.6, «Data Preservation versus Data Retention»: «[W]ith 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 — O Governo francês referiu, a este respeito, o relatório do Conseil d'État, *Le numérique et les droits fondamentaux*, 2014, pp. 209 e 210. O Conseil d'État (França) sublinha que um mecanismo de medidas de vigilância direcionadas «é significativamente menos eficaz do que a conservação sistemática do ponto de vista da segurança nacional e da procura dos autores da infração. Com efeito, não permite um acesso retrospetivo às trocas que tenham ocorrido antes de a autoridade ter identificado uma ameaça ou uma infração: o seu caráter operacional depende, assim, da capacidade de as autoridades anteciparem a identificação das pessoas cujos dados de conexão podem ser úteis, o que é impossível no quadro da polícia judiciária. Por exemplo, no que respeita a um crime, a autoridade judiciária não pode ter acesso às comunicações anteriores a este, dado que no entanto é precioso e, por vezes, até indispensável para a identificação do seu autor e dos seus cúmplices, como demonstraram alguns recentes casos de atentados terroristas. No domínio da prevenção dos ataques à segurança nacional, os novos programas técnicos assentam numa capacidade de deteção dos sinais fracos, incompatível com a ideia do pré-identificação das pessoas perigosas».

55 — Commission Staff Working Document apresentado em anexo à proposta de diretiva que conduziu à adoção da Diretiva 2006/24, SEC (2005) 1131, 21 de setembro de 2005, n.º 1.2, «The importance of traffic data for law enforcement».

extrema utilidade para os investigadores descobrirem os cúmplices dos autores destes atentados. De igual modo, no âmbito de buscas de uma pessoa desaparecida, os dados atinentes à localização desta pessoa aquando das comunicações efetuadas antes do seu desaparecimento podem desempenhar um papel determinante para efeitos da investigação.

184. Atendendo ao que precede, considero que uma obrigação geral de conservação de dados pode contribuir para lutar contra as infrações graves. No entanto, resta verificar se tal obrigação é simultaneamente necessária e proporcionada a este objetivo.

5. Quanto ao caráter necessário de uma obrigação geral de conservação de dados na luta contra as infrações graves

185. Segundo jurisprudência constante, uma medida só pode ser considerada necessária se não existir outra medida que sendo tão adequada seja, simultaneamente, menos vinculativa [56].

186. A exigência relativa ao caráter adequado equivale a avaliar a eficácia «absoluta» — independentemente de qualquer outra medida possível — de uma obrigação geral de conservação de dados na luta contra as infrações graves. A exigência de necessidade conduz, por seu turno, a apreciar a eficiência — ou eficácia «relativa», ou seja, por comparação com qualquer outra medida possível — de tal obrigação [57].

187. No contexto dos presentes processos, o teste da necessidade impõe que se verifique, por um lado, se outras medidas poderiam ser tão eficazes como uma obrigação geral de conservação de dados na luta contra as infrações graves e, por outro, se estas eventuais medidas são menos atentatórias dos direitos consagrados na Diretiva 2002/58 e nos artigos 7.º e 8.º da Carta [58].

188. Recordo ainda a jurisprudência constante, recordada no n.º 52 do acórdão DRI, segundo a qual a proteção do direito fundamental à vida privada exige que as exceções à proteção dos dados pessoais e as restrições a estas devem ocorrer na «estrita medida do necessário» [59].

189. No contexto dos presentes processos foram amplamente discutidas pelas partes que apresentaram observações no Tribunal de Justiça duas problemáticas relativas à exigência da estrita medida do necessário, as quais, em substância, correspondem às duas questões submetidas pelo órgão jurisdicional de reenvio no processo C-203/15:

— por um lado, à luz dos n.os 56 a 59 do acórdão DRI, deve considerar-se que uma obrigação geral de conservação de dados excede, por si só, os limites da estrita medida do necessário para efeitos da luta contra as infrações graves, independentemente de eventuais garantias que acompanhem esta obrigação?

56 — V., nomeadamente, acórdãos de 22 de janeiro de 2013, Sky Österreich (C-283/11, EU:C:2013:28, n.os 54 a 57); de 13 de novembro de 2014, Reindl (C-443/13, EU:C:2014:2370, n.º 39), e de 16 de julho de 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, n.os 120 a 122). Na doutrina, v., nomeadamente, 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 — V. 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 — Quanto à existência destes dois componentes no teste da necessidade, v. Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, pp. 323 a 331.

59 — V. nomeadamente, acórdãos de 9 de novembro de 2010, Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662, n.os 77 e 86), e de 7 de novembro de 2013, IPI (C-473/12, EU:C:2013:715, n.º 39).

— por outro lado, admitindo que é possível considerar que tal obrigação não excede, por si só, os limites da estrita medida do necessário, deve essa obrigação ser acompanhada de todas as garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI para limitar à estrita medida do necessário a afetação dos direitos consagrados na Diretiva 2002/58 e nos artigos 7.º e 8.º da Carta?

190. Antes de abordar estas questões, creio que é oportuno rejeitar um argumento invocado pelo Governo do Reino Unido, segundo o qual os critérios estabelecidos no acórdão DRI não são pertinentes no contexto dos presentes processos, uma vez que este acórdão não dizia respeito a um regime nacional mas a um regime estabelecido pelo legislador da União.

191. A este respeito, sublinho que o acórdão DRI interpretou os artigos 7.º, 8.º e 52.º, n.º 1, da Carta e que estas disposições constituem igualmente o objeto das questões colocadas nos litígios nos processos principais. Ora, em minha opinião, é impossível interpretar as disposições da Carta de modo distinto consoante o regime em causa tenha sido estabelecido a nível da União ou a nível nacional, conforme sublinharam acertadamente P. Brice e G. Lewis, bem como a Law Society of England and Wales. Nos casos em que seja constatado que a Carta é aplicável, como sucede nos presentes processos [60], esta deve ser aplicada da mesma forma independentemente do regime em causa. Por conseguinte, os critérios desenvolvidos pelo Tribunal de Justiça no acórdão DRI são relevantes para efeitos da apreciação dos regimes nacionais em causa nos presentes processos, conforme alegaram nomeadamente os Governos dinamarquês e irlandês, bem como a Comissão.

a) Quanto ao caráter estritamente necessário de uma obrigação geral de conservação de dados

192. De acordo com uma primeira abordagem, defendida pela Tele2 Sverige, bem como pela Open Rights Group e pela Privacy Internacional, deve considerar-se que uma obrigação geral de conservação de dados, na sequência do acórdão DRI, excede, por si só, os limites da estrita medida do necessário para efeitos da luta contra as infrações graves, independentemente de eventuais garantias que acompanhem esta obrigação.

193. De acordo com uma segunda abordagem, defendida pela maioria das outras partes que apresentaram observações ao Tribunal de Justiça, tal obrigação não excede os limites da estrita medida do necessário quando for acompanhada de certas garantias relativas ao acesso aos dados, à duração da conservação, bem como à proteção e à segurança dos dados.

194. Pelos motivos que em seguida irei expor, adoto esta segunda abordagem.

195. Em primeiro lugar, de acordo com a leitura que faço do acórdão DRI, o Tribunal de Justiça declarou que uma obrigação geral de conservação de dados excede os limites da estrita medida do necessário quando *não seja acompanhada* de garantias estritas relativas ao acesso aos dados, à duração da conservação, bem como à proteção e à segurança dos dados. Em contrapartida, o Tribunal de Justiça não se pronunciou sobre a compatibilidade com o direito da União de uma obrigação geral de conservação de dados que seja *acompanhada* dessas garantias, uma vez que tal regime não constituía o objeto das questões submetidas ao Tribunal de Justiça nesse processo.

196. A este respeito, sublinho que os n.os 56 a 59 do acórdão DRI não incluem uma declaração do Tribunal de Justiça no sentido de que uma obrigação geral de conservação de dados excede, por si só, os limites da estrita medida do necessário.

60 — V., n.os 117 a 125 das presentes conclusões.

197. Nos n.os 56 e 57 daquele acórdão, o Tribunal de Justiça constata que a obrigação de conservação prevista na Diretiva 2006/24 visa todos os meios de comunicação eletrónica, todos os utilizadores e todos os dados relativos ao tráfego, sem proceder a uma distinção, restrição ou exceção em função do objetivo de luta contra as infrações graves.

198. Nos n.os 58 e 59 do referido acórdão, o Tribunal de Justiça expõe de forma mais detalhada as consequências práticas dessa não distinção. Por um lado, esta obrigação de conservação abrange inclusivamente pessoas em relação às quais não haja indícios que deixem pensar que o seu comportamento pode estar associado, ainda que de forma indireta ou longínqua, a infrações graves. Por outro, esta diretiva não requer nenhuma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública e, designadamente, não se limita a uma conservação que incida sobre dados relativos a um período de tempo e/ou a uma determinada zona geográfica e/ou a um círculo de determinadas pessoas que possam estar envolvidas, de uma maneira ou de outra, numa infração grave.

199. Assim, o Tribunal de Justiça constata que uma obrigação geral de conservação de dados se caracteriza pela sua não distinção em função do objetivo de luta contra as infrações graves. Todavia, o Tribunal de Justiça não declarou que esta não distinção significava que tal obrigação excedia, por si só, os limites da estrita medida do necessário.

200. Na realidade, só no final do exame do regime previsto na Diretiva 2006/24, e depois de ter constatado a inexistência de determinadas garantias que em seguida apreciarei [61], é que o Tribunal de Justiça declara, no n.º 69 do acórdão DRI, que:

«*Face ao exposto*, há que considerar que, ao adotar a Diretiva 2006/24, o legislador da União *excedeu os limites* impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta» (o sublinhado é nosso).

201. Conforme os Governos alemão e neerlandês alegaram, se a mera conservação generalizada dos dados tivesse sido suficiente para conduzir à invalidade da Diretiva 2006/24, o Tribunal de Justiça não teria tido necessidade de examinar, e de forma detalhada, a inexistência das garantias enunciadas nos n.os 60 a 68 daquele acórdão.

202. Por conseguinte, a obrigação geral de conservação de dados prevista na Diretiva 2006/24 não excedia, em si mesma, os limites da estrita medida do necessário. Esta diretiva excedia os limites da estrita medida do necessário devido ao *efeito combinado* da conservação generalizada dos dados e à inexistência de garantias destinadas a limitar à estrita medida do necessário a afetação dos direitos consagrados nos artigos 7.º e 8.º da Carta. Devido a este efeito combinado, a diretiva devia ser declarada inválida na íntegra [62].

203. Em segundo lugar, encontro uma confirmação desta interpretação no n.º 93 do acórdão Schrems [63], que reproduzo em seguida:

«Assim, não é limitada ao estritamente necessário uma regulamentação que autoriza de modo generalizado a conservação da totalidade dos dados pessoais de todas as pessoas cujos dados foram transferidos da União para os Estados Unidos *sem* qualquer diferenciação, restrição ou exceção em função do objetivo prosseguido e *sem que* esteja previsto um critério objetivo que permita delimitar o

61 — V. n.os 216 a 245 das presentes conclusões.

62 — V. acórdão DRI, n.º 65: «Impõe-se pois concluir que esta diretiva comporta uma ingerência nestes direitos fundamentais, de grande amplitude e particular gravidade na ordem jurídica da União, *sem que* essa ingerência seja enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário» (o sublinhado é nosso).

63 — Acórdão de 6 de outubro de 2015, Schrems (C-362/14, EU:C:2015:650).

acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos, estritamente limitados e suscetíveis de justificar a ingerência que tanto o acesso como a utilização desses dados comportam [v., neste sentido, no que respeita à Diretiva 2006/24/CE, acórdão DRI, n.os 57 a 61]» (o sublinhado é nosso).

204. Uma vez mais, o Tribunal de Justiça não declarou que o regime em causa naquele processo excedia os limites do estritamente necessário apenas porque autorizava uma conservação generalizada de dados pessoais. Naquele caso, os limites do estritamente necessário eram ultrapassados devido ao efeito combinado da possibilidade de tal conservação generalizada e à inexistência de garantias relativas ao acesso para reduzir a ingerência à estrita medida do necessário.

205. Deduzo do que precede que nem sempre se deve considerar que uma obrigação geral de conservação de dados excede, em si mesma, os limites do estritamente necessário para efeitos da luta contra as infrações graves. Em contrapartida, tal obrigação excede sempre os limites do estritamente necessário quando não seja acompanhada de garantias relativas ao acesso aos dados, à duração da conservação, bem como à proteção e à segurança dos dados.

206. Em terceiro lugar, a minha opinião a este respeito é corroborada pela necessidade de verificar de forma concreta o respeito da exigência da estrita medida do necessário no contexto dos regimes nacionais em causa nos litígios nos processos principais.

207. Conforme referi no n.º 187 das presentes conclusões, a exigência da estrita medida do necessário impõe que se examine se outras medidas podem ser tão eficazes como uma obrigação geral de conservação de dados na luta contra as infrações graves, sendo, simultaneamente, menos atentatórias dos direitos consagrados na Diretiva 2002/58 e nos artigos 7.º e 8.º da Carta.

208. Ora, tal apreciação deve ser realizada no contexto específico de cada regime nacional que preveja uma obrigação geral de conservação de dados. Por um lado, esta apreciação requer que se compare a eficácia desta obrigação com a eficácia de qualquer outra medida no contexto nacional, tomando em consideração o facto de que a referida obrigação oferece às autoridades competentes uma capacidade limitada de ler o passado através dos dados conservados [64].

209. Atendendo à exigência da estrita medida do necessário, é imperativo que estes órgãos jurisdicionais não se limitem a verificar a simples utilidade de uma obrigação geral de conservação de dados, mas verifiquem de forma estrita que nenhuma outra medida ou combinação de medidas, nomeadamente uma obrigação direcionada de conservação de dados acompanhada de outros instrumentos de investigação, possa oferecer a mesma eficácia na luta contra as infrações graves. A este respeito, sublinho que vários estudos apresentados ao Tribunal de Justiça questionam a necessidade deste tipo de obrigação para efeitos da luta contra as infrações graves [65].

210. Por outro lado, admitindo que outras medidas também possam ser eficazes na luta contra as infrações graves, caberá ainda aos órgãos jurisdicionais de reenvio determinar se estas são menos atentatórias dos direitos fundamentais em causa do que uma obrigação geral de conservação de dados, em aplicação da jurisprudência constante recordada no n.º 185 das presentes conclusões.

64 — V. n.os 178 a 183 das presentes conclusões.

65 — V. comissário do Conselho da Europa para os Direitos Humanos, «Issue paper on the rule of law on the Internet and in the wider digital world», de dezembro de 2014, CommDH/IssuePaper (2014)1, p. 115; Conselho dos Direitos Humanos das Nações Unidas, relatório do Alto Comissariado das Nações Unidas para os Direitos Humanos sobre o direito à vida privada na era digital, 30 de junho de 2014, A/HRC/27/37, n.º 26; Assembleia-Geral das Nações Unidas, relatório do relator especial sobre a promoção e a proteção dos direitos do homem e das liberdades fundamentais na luta contra o terrorismo, 23 de setembro de 2014, A/69/397, n.os 18 e 19.

211. À luz do n.º 59 do acórdão DRI, incumbirá aos órgãos jurisdicionais nacionais questionar, nomeadamente, a possibilidade de limitar o alcance material da obrigação de conservação preservando em simultâneo a eficácia desta medida na luta contra as infrações graves [66]. Com efeito, essas obrigações podem ter um alcance material maior ou menor, em função dos utilizadores, das zonas geográficas e dos meios de comunicação visados [67].

212. Em minha opinião, seria desejável, se a tecnologia o permitir, excluir da obrigação de conservação os dados particularmente sensíveis relativos aos direitos fundamentais em causa nos presentes processos, como sejam os dados abrangidos pelo segredo profissional ou ainda os dados que permitem identificar as fontes dos jornalistas.

213. No entanto, importa ter presente que uma restrição substancial do alcance de uma obrigação geral de conservação de dados pode reduzir consideravelmente a utilidade que tal regime apresenta na luta contra as infrações graves. Por um lado, vários governos sublinharam a dificuldade, ou mesmo a impossibilidade, de determinar antecipadamente os dados que podem estar relacionados com uma infração grave. Por conseguinte, tal restrição é suscetível de excluir a conservação de dados que se possam revelar serem relevantes na luta contra as infrações graves.

214. Por outro lado, conforme o Governo estónio alegou, a criminalidade grave é um fenómeno dinâmico, capaz de se adaptar aos meios de investigação de que as autoridades de repressão dispõem. Deste modo, uma restrição a uma determinada zona geográfica ou a determinado meio de comunicação comporta o risco de provocar uma deslocação das atividades associadas às infrações graves para uma zona geográfica e/ou um meio de comunicação não abrangidos por este regime.

215. Uma vez que exige uma avaliação complexa dos regimes nacionais em causa nos litígios nos processos principais, considero que esta apreciação deve ser efetuada pelos órgãos jurisdicionais nacionais, conforme sublinharam os Governos checo, estónio, irlandês, francês, neerlandês, bem como a Comissão.

b) Quanto ao caráter imperativo das garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI à luz da exigência da estrita medida do necessário

216. Admitindo que uma obrigação geral de conservação de dados possa ser considerada como sendo estritamente necessária no contexto do regime nacional em causa, o que cabe ao órgão jurisdicional nacional apreciar, é ainda necessário determinar se tal obrigação deve ser acompanhada de todas as garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI para limitar à estrita medida do necessário a afetação dos direitos consagrados na Diretiva 2002/58 e nos artigos 7.º e 8.º da Carta.

217. Estas garantias dizem respeito às regras que regulam o acesso e a utilização dos dados conservados pelas autoridades competentes (n.os 60 a 62 do acórdão DRI), a duração da conservação dos dados (n.os 63 e 64 deste acórdão), bem como a segurança e a proteção dos dados conservados pelos prestadores (n.os 66 a 68 deste acórdão).

218. De entre as observações apresentadas no Tribunal de Justiça, duas teses opõem-se no que respeita à natureza destas garantias.

66 — Esta observação visa unicamente as obrigações gerais de conservação de dados (que são suscetíveis de visar qualquer pessoa independentemente de existir alguma ligação a uma infração grave) e não as medidas de vigilância direcionadas (que visam as pessoas que foram previamente identificadas como tendo uma ligação a uma infração grave): sobre esta distinção, v. n.os 178 a 183 das presentes conclusões.

67 — Nomeadamente, o Governo alemão precisou na audiência, que o Parlamento alemão exclui os correios eletrónicos da obrigação de conservação imposta pela legislação alemão, mas que este regime abrange todos os utilizadores e todo o território nacional.

219. De acordo com uma primeira tese defendida por T. Watson, P. Brice e G. Lewis, bem como pela Open Rights Group e pela Privacy Internacional, as garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI são imperativas. De acordo com esta tese, o Tribunal de Justiça estabeleceu garantias mínimas, devendo *todas* elas ser respeitadas pelo regime nacional em causa para limitar a afetação dos direitos fundamentais à estrita medida do necessário.

220. De acordo com uma segunda tese, defendida pelos Governos alemão, estónio, irlandês, francês e do Reino Unido, as garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI são apenas indicativas. O Tribunal de Justiça efetuou uma «apreciação de conjunto» das garantias inexistentes no regime previsto pela Diretiva 2006/24, não sendo possível que uma destas garantias possa, de forma isolada, ser considerada imperativa à luz da exigência da estrita medida do necessário. Para ilustrar esta tese, o Governo alemão evocou a imagem de «vasos comunicantes», segundo a qual uma abordagem mais flexível sobre um dos três aspetos identificados pelo Tribunal de Justiça (por exemplo, o acesso aos dados conservados) pode ser compensada por uma abordagem mais estrita no que se refere aos dois outros aspetos (a duração da conservação, bem como a segurança e a proteção dos dados).

221. Pelos motivos que a seguir apresento, sou da opinião de que esta tese dos «vasos comunicantes» deve ser rejeitada e, pelos seguintes motivos, de que *todas* as garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI devem ser consideradas imperativas.

222. Em primeiro lugar, a linguagem utilizada pelo Tribunal de Justiça no seu exame da estrita medida do necessário do regime estabelecido pela Diretiva 2006/24 não se presta a tal interpretação. Em particular, o Tribunal de Justiça não faz nenhuma alusão, nos n.os 60 a 68 do referido acórdão, a qualquer possibilidade de «compensar» uma abordagem mais flexível sobre um dos três aspetos identificados pelo Tribunal de Justiça com uma abordagem mais estrita no que respeita aos dois outros aspetos.

223. Na realidade, parece-me que a tese dos «vasos comunicantes» tem origem numa confusão entre a exigência de necessidade e a de proporcionalidade *stricto sensu*, a qual não foi examinada pelo Tribunal de Justiça no acórdão DRI. Com efeito, conforme indiquei no n.º 186 das presentes conclusões, a exigência de necessidade consiste em rejeitar todas as medidas que não sejam eficientes. Neste contexto, não está em causa a «apreciação de conjunto», a «compensação» ou a «ponderação», as quais só ocorrem na fase em que é apreciada a proporcionalidade *stricto sensu*[68].

224. Em segundo lugar, esta tese dos «vasos comunicantes» reduziria a zero o efeito útil das garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI, pelo que as pessoas cujos dados foram conservados deixariam de dispor de garantias suficientes que lhes permitissem proteger de forma eficaz os seus dados pessoais contra os riscos de abuso, bem como contra qualquer acesso e qualquer utilização ilícitos destes dados, conforme exige o n.º 54 deste acórdão.

225. O efeito destruidor desta tese pode ser facilmente ilustrado através dos seguintes exemplos. Um regime nacional que restringisse de forma estrita o acesso apenas para efeitos da luta contra o terrorismo e que limita a duração da conservação a três meses (abordagem estrita quanto ao acesso e à duração da conservação), mas que não obrigasse os prestadores a conservarem os dados no seu território nacional e num formato encriptado (abordagem flexível quanto à segurança), exporia toda a sua população a um risco elevado de acesso ilegal aos dados conservados. Do mesmo modo, um regime nacional que previsse uma duração da conservação de três meses e uma conservação dos dados no seu

68 — V., 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*» (o sublinhado é nosso).

território nacional e num formato encriptado (abordagens estritas quanto à duração e à segurança), mas que permitisse que todos os funcionários de todas as autoridades públicas acedessem aos dados conservados (abordagem flexível quanto ao acesso), exporia toda a sua população a um risco elevado de abuso por parte das autoridades nacionais.

226. Em meu entender, decorre destes exemplos que a preservação do efeito útil das garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI exige que se considere que *cada uma* destas garantidas é imperativa. O Tribunal EDH também sublinhou a importância fundamental destas garantias no recente acórdão Szabó e Vissy c. Hungria, referindo-se expressamente ao acórdão DRI [69].

227. Em terceiro lugar, a implementação destas garantias, pelos Estados-Membros que pretendam impor uma obrigação geral de conservação de dados, não parece colocar grandes dificuldades práticas. Na realidade, em muitos aspetos estas garantias afiguram-se efetivamente «mínimas», conforme T. Watson alega.

228. Várias destas garantias foram debatidas no Tribunal de Justiça por eventualmente não estarem consagradas nos regimes nacionais em causa nos processos principais.

229. Em primeiro lugar, resulta dos n.os 61 e 62 do acórdão DRI que o acesso e a utilização posterior dos dados conservados devem ser estritamente restringidos para efeitos de prevenção e de deteção de infrações graves delimitadas com precisão ou de ações penais contra as mesmas.

230. De acordo com a Tele2 Sverige e a Comissão, esta exigência não é respeitada pelo regime sueco em causa no processo C-203/15, que permite o acesso aos dados conservados para lutar contra infrações simples. Uma crítica semelhante foi efetuada por P. Brice, G. Lewis, e T. Watson contra o regime do Reino Unido em causa no processo C-698/15, que autoriza o acesso com vista à luta contra as infrações simples, inclusivamente quando não haja infração.

231. Embora não incumba ao Tribunal de Justiça pronunciar-se sobre o teor destes regimes nacionais, cabe-lhe identificar os objetivos de interesse geral suscetíveis de justificar uma ingerência grave nos direitos consagrados na diretiva e nos artigos 7.º e 8.º da Carta. Neste caso, já expus as razões pelas quais considero que *só* a luta contra as infrações graves é suscetível de justificar tal ingerência [70].

232. Em segundo lugar, nos termos do n.º 62 do acórdão DRI, o acesso aos dados conservados deve estar sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente cuja decisão vise limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido. Além disso, esse controlo prévio deve ocorrer na sequência de um pedido fundamentado destas autoridades, apresentado no âmbito de processos de prevenção, de deteção ou de uma ação penal.

233. De acordo com as observações da Tele2 Sverige e da Comissão, esta garantia de controlo independente e prévio ao acesso está parcialmente ausente no regime sueco em causa no processo C-203/15. A mesma constatação, cuja veracidade não é contestada pelo Governo do Reino Unido, é defendida por P. Brice, G. Lewis, e T. Watson, bem como pela Open Rights Group e pela Privacy Internacional relativamente ao regime do Reino Unido em causa no processo C-698/15.

69 — Tribunal EDH, 12 de janeiro de 2016, Szabó e Vissy c. Hungria, 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 — V. n.os 170 a 173 das presentes conclusões.

234. Não encontro motivos para atenuar esta exigência de controlo prévio por uma entidade independente, que resulta incontestavelmente da linguagem utilizada pelo Tribunal de Justiça no n.º 62 do acórdão DRI [71]. Antes de mais, esta exigência é ditada pela gravidade da ingerência e dos riscos que decorrem da criação de bases de dados que abrangem quase toda a população em causa [72]. Observo que vários especialistas em matéria de proteção dos direitos do homem na luta contra o terrorismo criticaram a tendência atual de substituir os tradicionais procedimentos de autorização independente e de acompanhamento efetivo por sistemas de «auto-autorização» de acesso aos dados pelos serviços de informação e de polícia [73].

235. Em seguida, é necessário um controlo independente e prévio ao acesso aos dados de modo a permitir um tratamento casuístico dos dados particularmente sensíveis no que respeita aos direitos fundamentais em causa nos presentes processos, tais como os dados abrangidos pelo segredo profissional ou ainda os dados que permitem identificar as fontes dos jornalistas, conforme sublinharam a Law Society of England and Wales, bem como os Governos francês e alemão. Este controlo prévio do acesso é ainda mais necessário na hipótese de ser tecnicamente difícil excluir todos estes dados na fase da conservação [74].

236. Por último, acrescento que, de um ponto de vista prático, nenhuma das três partes abrangidas por um pedido de acesso está em condições de exercer um controlo efetivo quanto ao acesso aos dados conservados. As autoridades competentes em matéria repressiva têm todo o interesse em pedir o acesso mais amplo possível a estes dados. Os prestadores, que desconhecem os elementos da investigação, não podem verificar se o pedido de acesso está limitado à estrita medida do necessário. Quanto às pessoas cujos dados são consultados, não têm forma de saber se são objeto de tal medida de investigação, inclusivamente em caso de utilização abusiva ou ilícita conforme sublinharam T. Watson, P. Brice e G. Lewis. Esta configuração dos interesses em causa exige, em meu entender, que haja uma intervenção de uma entidade independente antes de ser efetuada a consulta dos dados conservados, para proteger as pessoas cujos dados são conservados de qualquer acesso abusivo por parte das autoridades competentes.

237. Dito isto, parece-me que é razoável considerar que as situações pontuais de extrema urgência, evocadas pelo Governo do Reino Unido, podem justificar um acesso imediato aos dados conservados pelas autoridades repressivas, sem controlo prévio, para prevenir que sejam cometidas infrações graves ou para prosseguir os autores de tais infrações [75]. Tanto quanto possível, é imperativo manter a exigência de uma autorização prévia através da criação de um procedimento de urgência na entidade

71 — Não obstante, preciso que este requisito de fiscalização prévia e independente não pode, em meu entender, basear-se no artigo 8.º, n.º 3, da Carta, uma vez que esta não é aplicável, enquanto tal, às disposições nacionais que regulam o acesso aos dados conservados: v. n.os 123 a 125 das presentes conclusões.

72 — V. n.os 252 a 261 das presentes conclusões.

73 — Conselho dos Direitos do Homem das Nações Unidas, relatório do relator especial sobre a promoção e a proteção dos direitos do homem e das liberdades fundamentais na luta contra o terrorismo, 28 de dezembro de 2009, A/HRC/13/37, n.º 62: «[n]ão deve existir nenhum sistema secreto de vigilância que não esteja sob a supervisão de uma instância de controlo eficaz, nem nenhuma ingerência que não seja autorizada por intermediário de um organismo independente» (v., igualmente n.º 51). V. igualmente Assembleia-Geral das Nações Unidas, relatório do relator especial sobre a promoção e a proteção dos direitos do homem e das liberdades fundamentais na luta contra o terrorismo, 23 de setembro de 2014, A/69/397, n.º 61.

74 — V., n.os 212 das presentes conclusões. No que respeita às fontes dos jornalistas, o Tribunal EDH sublinhou a necessidade de uma autorização prévia por uma entidade independente, na medida em que uma fiscalização *a posteriori* não permite restaurar a confidencialidade de tais fontes: v. Tribunal EDH, 22 de novembro de 2012, Telegraaf Media Nederland Landelijke Media B.V. e o. c. Países Baixos, CE:ECHR:2012:1122JUD003931506, § 101 e Tribunal EDH, 12 de janeiro de 2016, Szabó e Vissy c. Hungria, CE:ECHR:2016:0112JUD003713814, §77. No acórdão Kopp c. Suíça, que dizia respeito à vigilância das linhas telefónicas de um advogado, o Tribunal EDH criticou o facto de um funcionário que pertence à Administração ser responsável, sem que haja fiscalização por parte de um magistrado independente, por filtrar as informações abrangidas pelo segredo profissional: v. Tribunal EDH, 25 de março de 1998, Kopp c. Suíça, CE:ECHR:1998:0325JUD002322494, § 74.

75 — V., a este respeito, o mecanismo descrito no n.º 22 das presentes conclusões. Sublinho que esta problemática não foi abordada pelo Tribunal de Justiça no acórdão DRI.

independente com vista ao processamento deste tipo de pedidos de acesso. Não obstante, embora o simples facto de apresentar a esta entidade um pedido de acesso possa parecer incompatível com a extrema urgência da situação, o acesso e a utilização dos dados deverão ser objeto de um controlo *a posteriori* por esta entidade, devendo ser feito o mais rapidamente possível.

238. Em terceiro lugar, o n.º 68 do acórdão DRI estabelece uma obrigação, imposta aos prestadores, de conservar dados no território da União, para garantir o controlo por uma autoridade independente, exigido pelo artigo 8.º, n.º 3, da Carta, do respeito das exigências de proteção e de segurança enunciadas nos n.os 66 e 67 deste acórdão.

239. A Tele2 Sverige e a Comissão alegam que a conservação de dados no território nacional não é garantida no âmbito do regime sueco em causa no processo C-203/15. A mesma crítica é efetuada por P. Brice, G. Lewis e T. Watson contra o regime do Reino Unido em causa no processo C-698/15.

240. Relativamente a esta questão, por um lado, não vislumbro nenhuma razão para atenuar esta exigência estabelecida no n.º 68 do acórdão DRI, uma vez que a conservação de dados fora do território da União não permitiria garantir às pessoas cujos dados são conservados o nível de proteção conferido pela Diretiva 2002/58 e pelos artigos 7.º, 8.º e 52.º, n.º 1, da Carta [76].

241. Por outro lado, parece-me razoável que se adapte esta exigência, expressa pelo Tribunal de Justiça no contexto da Diretiva 2006/24, ao contexto de regimes nacionais, prevendo a conservação dos dados no território nacional, conforme alegaram os Governos alemão e francês, bem como a Comissão. Com efeito, nos termos do artigo 8.º, n.º 3, da Carta, incumbe a cada Estado-Membro garantir o controlo, por parte de uma autoridade independente, do respeito das exigências de proteção e de segurança por parte dos prestadores visados pelo seu regime nacional. Ora, não havendo coordenação a nível da União, tal autoridade nacional pode ficar impossibilitada de executar correctamente as suas missões de controlo no território de outro Estado-Membro.

242. Em quarto lugar, no que respeita à duração da conservação, os órgãos jurisdicionais de reenvio deverão aplicar os critérios definidos pelo Tribunal de Justiça nos n.os 63 e 64 do acórdão DRI. Por um lado, estes órgãos jurisdicionais devem determinar se os dados conservados podem ser distinguidos em função da sua utilidade e, eventualmente, se a duração da conservação foi adaptada em função deste critério. Por outro, os referidos órgãos jurisdicionais devem verificar se a duração da conservação assenta em critérios objetivos que permitem garantir que esta se limita à estrita medida do necessário.

243. Sublinho que o Tribunal EDH, no recente acórdão Roman Zakharov c. Rússia, declarou que é razoável uma duração máxima de conservação de seis meses, embora tenha deplorado a inexistência de obrigação de destruição dos dados que não estão relacionados com a finalidade para a qual foram recolhidos [77]. A este respeito, acrescento que os regimes nacionais em causa nos litígios nos processos principais devem prever a obrigação de destruição definitiva de todos os dados conservados a partir do momento em que já não sejam estritamente necessários na luta contra as infrações graves. Esta obrigação deve ser respeitada não apenas pelos prestadores que conservam os dados, mas também pelas autoridades que tiveram acesso aos dados conservados.

76 — V., a este respeito, acórdão de 6 de outubro de 2015, Schrems (C-362/14, EU:C:2015:650).

77 — V., a este respeito, Tribunal EDH, 4 de dezembro de 2015, Roman Zakharov c. Rússia, CE:ECHR:2015:1204JUD004714306, § 254-255. Segundo o direito russo, a destruição dos elementos intercetados devia ocorrer findo um prazo de seis meses de conservação se a pessoa em causa não tiver sido considerada culpada de uma infração penal. O Tribunal EDH declarou razoável a duração máxima de conservação, ou seja, seis meses, fixada pelo direito russo para tais dados. Todavia, lamentou a inexistência de obrigação de destruição dos dados que não estão relacionados com a finalidade para a qual foram recolhidos, precisando que a conservação automática, durante seis meses, de dados manifestamente desprovidos de interesse não pode ser considerada justificada à luz do artigo 8.º da CEDH.

244. Atendendo às considerações que precedem, considero que todas as garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI têm um caráter imperativo e devem, por conseguinte, acompanhar uma obrigação geral de conservação de dados para limitar ao estritamente necessário a afetação dos direitos consagrados na Diretiva 2002/58 e nos artigos 7.º e 8.º da Carta.

245. Cabe aos órgãos jurisdicionais de reenvio verificar se os regimes nacionais em causa nos litígios nos processos principais comportam cada uma destas garantias.

6. Quanto ao caráter proporcionado, numa sociedade democrática, de uma obrigação geral de conservação de dados à luz do objetivo de luta contra as infrações graves

246. Depois de ter verificado o caráter necessário dos regimes nacionais em causa nos processos principais, incumbirá ainda aos órgãos jurisdicionais de reenvio verificar o respeito do caráter proporcionado, numa sociedade democrática, à luz do objetivo de luta contra as infrações graves. Este aspeto não foi examinado pelo Tribunal de Justiça no acórdão DRI porque o regime estabelecido pela Diretiva 2006/24 excedia os limites da estrita medida do necessário para efeitos da luta contra as infrações graves.

247. Esta exigência de proporcionalidade numa sociedade democrática — ou proporcionalidade «*stricto sensu*» — decorre simultaneamente do artigo 15.º, n.º 1, da Diretiva 2002/58, do artigo 52.º, n.º 1, da Carta e de jurisprudência constante. De acordo com esta jurisprudência constante, uma medida que afeta direitos fundamentais só pode ser considerada proporcionada se os inconvenientes causados não forem desmesurados face aos objetivos prosseguidos [78].

248. Ao contrário das exigências relativas ao caráter adequado e necessário da medida em causa, as quais avaliam a sua eficácia à luz do objetivo prosseguido, a exigência de proporcionalidade *stricto sensu* consiste em ponderar, por um lado, as vantagens resultantes desta medida à luz do objetivo legítimo prosseguido e, por outro, os inconvenientes que daí decorrem para os direitos fundamentais consagrados numa sociedade democrática [79]. Assim, esta exigência dá origem a um debate sobre os valores que devem prevalecer numa sociedade democrática e, em definitivo, sobre o tipo de sociedade em que desejamos viver [80].

249. Por conseguinte, conforme já indiquei no n.º 223 das presentes conclusões, é na fase do exame da proporcionalidade em sentido estrito que deve ser efetuada uma apreciação de conjunto do regime em causa, e não na fase do exame da necessidade, conforme alegam os defensores da tese dos «vasos comunicantes» [81].

78 — V., nomeadamente, acórdãos de 15 de fevereiro de 2016, N. (C-601/15 PPU, EU:C:2016:84, n.º 54; o caráter necessário é examinado nos n.os 56 a 67, o caráter proporcionado nos n.os 68 e 69); de 16 de julho de 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, n.º 123, o caráter necessário é examinado nos n.os 120 a 122, o caráter proporcionado nos n.os 123 a 127), e de 22 de janeiro de 2013, Sky Österreich (C-283/11, EU:C:2013:28, n.º 50, o caráter necessário é examinado nos n.os 54 a 57, o caráter proporcionado nos n.os 58 a 67).

79 — V. 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 — V., 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 — A especificidade da exigência de proporcionalidade *stricto sensu*, face aos requisitos do caráter adequado e necessário, pode ser ilustrada pelo seguinte exemplo. Imaginemos que um Estado-Membro impõe a injeção de um chip eletrónico de geolocalização a qualquer pessoa que resida no seu território, permitindo este chip permite que as autoridades retracem os movimentos do seu portador no ano anterior. Tal medida pode ser considerada «necessária» se nenhuma outra medida permitir atingir o mesmo grau de eficácia na luta contra as infrações graves. Todavia, em meu entender, tal medida é desproporcionada numa sociedade democrática, uma vez que os inconvenientes que resultam da afetação dos direitos à integridade física, ao respeito da vida privada e à proteção dos dados pessoais são excessivos face às vantagens que daí decorrem para a luta contra as infrações graves.

250. Em aplicação da jurisprudência recordada no n.º 247 das presentes conclusões, há que ponderar as vantagens e os inconvenientes, numa sociedade democrática, de uma obrigação geral de conservação de dados. Estas vantagens e estes inconvenientes estão intimamente ligados à característica essencial de tal obrigação, de que representam respetivamente a luz e a sombra, a saber, o facto de que aquela visa todas as comunicações realizadas por todos os utilizadores sem que seja exigida uma relação a uma infração grave.

251. Por um lado, expus nos n.os 178 a 183 das presentes conclusões as vantagens que, na luta contra as infrações graves, decorrem da conservação dos dados relativos a todas as comunicações realizadas no território nacional.

252. Por outro lado, os inconvenientes de uma obrigação geral de conservação de dados que decorrem do facto de a imensa maioria dos dados conservados dizer respeito a pessoas que nunca estarão relacionadas com uma infração grave. Quanto a esta questão, é imperativo precisar a natureza dos inconvenientes que afetarão estas pessoas. Ora, estes inconvenientes têm naturezas diferentes consoante o nível de ingerência nos seus direitos fundamentais do respeito da vida privada e da proteção dos dados pessoais.

253. No âmbito de uma ingerência «individual», que afeta um determinado individuo, os inconvenientes que resultam de uma obrigação geral de conservação de dados foram descritos com grande acuidade pelo advogado-geral P. Cruz Villalón nos n.os 72 a 74 das conclusões que apresentou no processo DRI [82]. Retomando os termos que este utilizou, a exploração destes dados torna possível «a cobertura cartográfica fiel e exaustiva de uma parte importante dos comportamentos de uma pessoa abrangidos estritamente pela sua vida privada, ou até um retrato completo e preciso da sua identidade privada».

254. Por outras palavras, num contexto individual, uma obrigação geral de conservação de dados permite ingerências tão graves como as medidas de vigilância direcionadas, incluindo as que intercetam o conteúdo das comunicações efetuadas.

255. Embora a gravidade de tais ingerências individuais não possa ser subestimada, afigura-se-me, no entanto, que os riscos específicos decorrentes de uma obrigação geral de conservação de dados surgem no âmbito de ingerências «de massa».

256. Com efeito, ao contrário de medidas de vigilância direcionadas, tal obrigação é suscetível de facilitar consideravelmente as ingerências de massa, ou seja, as ingerências que afetam uma parte substancial ou mesmo toda a população relevante, o que pode ser ilustrado através dos seguintes exemplos.

257. Admitamos, em primeiro lugar, que uma pessoa que tem acesso aos dados conservados tem intenção de identificar, de entre a população do Estado-Membro, todos os indivíduos que sofrem de distúrbios psicológicos. Para este efeito, a análise do conteúdo de todas as comunicações realizadas no território nacional exigiria recursos significativos. Em contrapartida, a exploração das bases de dados relativos às comunicações permitiria identificar instantaneamente todos os indivíduos que contactaram um psicólogo durante o período de conservação dos dados [83]. Acrescento que esta técnica poderia ser alargada a cada um das especialidades médicas registadas num Estado-Membro [84].

82 — C-293/12 e C-594/12, EU:C:2013:845. V. igualmente acórdão DRI (n.os 27 e 37).

83 — Os dados conservados incluem, com efeito, a identidade da fonte e do destinatário de uma comunicação, dados que basta cruzar com a lista dos números de telefones dos psicólogos que exercem no território nacional.

84 — V., a este respeito, Conselho dos Direitos do Homem das Nações Unidas, relatório do relator especial sobre a promoção e a proteção do homem e das liberdades fundamentais na luta contra o terrorismo, 28 de dezembro de 2009, A/HRC/13/37, n.º 42: «[N]a Alemanha, estudos assinalaram uma consequência inquietante das políticas de conservação dos dados: 52% das pessoas interrogadas indicaram que era pouco provável que utilizassem as telecomunicações para entrarem em contacto com um toxicólogo, um psicoterapeuta ou um conselheiro conjugal devido às leis sobre a conservação dos dados».

258. Admitamos, em segundo lugar, que esta mesma pessoa pretende identificar os indivíduos que se opõem à política do governo em funções. De novo, para este efeito, a análise do conteúdo das comunicações exigiria recursos significativos. Em contrapartida, a exploração dos dados relativos às comunicações permitiria identificar todos os indivíduos inscritos em listas de distribuição de mensagens de correio eletrónico que criticam a política do governo. Por outro lado, estes dados também permitiriam identificar os indivíduos que participam em manifestações públicas de oposição ao governo [85].

259. Faço questão de sublinhar que os riscos ligados ao acesso aos dados relativos às comunicações (ou «metadados») podem ser equivalentes, ou inclusivamente superiores, aos que resultam do acesso ao conteúdo destas comunicações, conforme salientaram a Open Rights Group e a Privacy Internacional, a Law Society of England and Wales, bem como um recente relatório do Alto Comissariado das Nações Unidas para os Direitos do Homem [86]. Em particular, como demonstram os exemplos acima referidos, os «metadados» permitem catalogar quase instantaneamente uma população no seu conjunto, o que o conteúdo das comunicações não permite.

260. Acrescento que os riscos de acesso abusivo ou ilegal aos dados conservados nada têm de teórico. Por um lado, o risco de acesso abusivo pelas autoridades competentes deve ser relacionado com os números extremamente elevados de pedidos de acesso evocados nas observações apresentadas ao Tribunal de Justiça. No âmbito do regime sueco, a Tele2 Sverige indicou que recebia cerca de 10 000 pedidos de acesso por mês, número que não inclui os pedidos recebidos por outros prestadores ativos no território sueco. No que respeita ao regime do Reino Unido, T. Watson reproduziu numerosos excertos de um relatório oficial que refere 517 236 autorizações e 55 346 autorizações orais urgentes, só no ano de 2014. Por outro lado, o risco de acesso ilegal, por qualquer pessoa, é consubstancial à própria existência de bases de dados conservadas em suportes informáticos [87].

261. Em meu entender, cabe aos órgãos jurisdicionais de reenvio apreciar se os inconvenientes causados pelas obrigações gerais de conservação de dados em causa nos litígios nos processos principais não são desmesurados, numa sociedade democrática, face aos objetivos visados, em aplicação da jurisprudência recordada no n.º 247 das presentes conclusões. No âmbito desta apreciação, estes órgãos jurisdicionais deverão ponderar os riscos e as vantagens associados a tal obrigação, a saber:

— por um lado, as vantagens associadas à concessão de uma capacidade limitada de ler o passado às autoridades responsáveis pela luta contra as infrações graves [88] e,

85 — Uma vez que os dados conservados incluem a localização da fonte e do destinatário de uma comunicação, qualquer pessoa que efetue ou recebe uma comunicação no âmbito de uma manifestação poderá ser facilmente identificada graças aos dados conservados. A este respeito, Marc Goodman, especialista do FBI e da Interpol no domínio dos riscos ligados às novas tecnologias, relata que, num passado recente, o Governo ucraniano, por ocasião de uma manifestação da oposição, procedeu à identificação de todos os telefones móveis localizados perto de confrontos de rua entre as forças da ordem e os opositores ao governo. Todos estes telefones receberam, então, uma mensagem que o autor descreveu como sendo possivelmente a mensagem mais «orweliana» jamais enviada por um governo: «Caro assinante, foi registado como tendo participado num grave incidente de ordem pública» (Goodman, M., *Future Crimes*, Anchor Books, New York, 2016, p. 153, tradução livre). V. igualmente Conselho dos Direitos do Homem das Nações Unidas, relatório do relator especial sobre a promoção e a proteção do direito à liberdade de opinião e de expressão, 17 de abril de 2013, A/HRC/23/40, n.º 75, e Conselho dos Direitos Humanos das Nações Unidas, relatório do Alto-Comissariado das Nações Unidas para os Direitos Humanos sobre o direito à vida privada na era digital, 30 de junho de 2014, A/HRC/27/37, n.º 3.

86 — V., a este respeito, Conselho dos Direitos Humanos das Nações Unidas, relatório do Alto-Comissariado das Nações Unidas para os Direitos Humanos sobre o direito à vida privada na era digital, 30 de junho de 2014, A/HRC/27/37, n.º 19: «Na mesma ordem de ideias, há quem alegue que a interceção – ou a recolha – de dados numa comunicação, e já não o conteúdo da comunicação, não constitui, por si só, uma interferência na vida privada. Ora, do ponto de vista do direito à vida privada, esta distinção não é convincente. Os agregadores de informação comummente designados 'metadados' podem dar indicações sobre a conduta de um individuo, as suas relações sociais, as suas preferências privadas e a sua identidade *que vão muito além do que é obtido através do acesso ao conteúdo* de uma comunicação privada» (o sublinhado é nosso). V., igualmente, Assembleia-Geral das Nações Unidas, relatório do relator especial sobre a promoção e a proteção dos direitos do homem e das liberdades fundamentais na luta contra o terrorismo, 23 de setembro de 2014, A/69/397, n.º 53.

87 — V., nomeadamente, Conselho dos Direitos do Homem das Nações Unidas, relatório do relator especial sobre a promoção e a proteção do direito à liberdade de opinião e de expressão, 17 de abril de 2013, A/HRC/23/40, n.º 67: «As bases de dados de comunicações tornam-se vulneráveis ao furto, à fraude e à divulgação acidental».

88 — V. n.os 178 a 183 das presentes conclusões.

— por outro, os graves riscos que resultam, numa sociedade democrática, do poder de cartografia da vida privada de um individuo e do poder de catalogar uma população no seu conjunto.

262. Esta apreciação deve ser efetuada à luz de todas as características relevantes dos regimes nacionais em causa nos litígios nos processos principais. A este respeito, sublinho que as garantias imperativas enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão DRI constituem apenas garantias mínimas para limitar à estrita medida do necessário a afetação dos direitos consagrados na Diretiva 2002/58 e nos artigos 7.º e 8.º da Carta. Por conseguinte, não se exclui que um regime nacional que inclua todas estas garantias deva, não obstante, ser considerado desproporcionado numa sociedade democrática, devido à desproporção entre os graves riscos resultantes desta obrigação numa sociedade democrática e as vantagens que dela decorrem na luta contra as infrações graves.

VI – Conclusão

263. Atendendo ao que precede, proponho ao Tribunal de Justiça que responda da seguinte forma às questões prejudiciais do Kammarrätten i Stockholm (Tribunal administrativo de recurso de Estocolmo, Suécia) e da Court of Appeal (England & Wales) (Civil Division) [Tribunal de recurso (Inglaterra e País de Gales) (Divisão Cível), Reino Unido]:

O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas («Diretiva relativa à privacidade e às comunicações eletrónicas»), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, bem como os artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia devem ser interpretados no sentido de que não se opõem a que um Estado-Membro imponha aos prestadores de serviços de comunicações eletrónicas uma obrigação de conservar todos os dados relativos às comunicações realizadas pelos utilizadores dos seus serviços quando estiverem preenchidos todos os requisitos em seguida enunciados, o que cabe aos órgãos jurisdicionais de reenvio verificar à luz de todas as características relevantes dos regimes nacionais em causa nos litígios nos processos principais:

— esta obrigação e as garantias que a acompanham devem estar previstas em medidas legislativas ou regulamentares que possuam as qualidades de acessibilidade, de previsibilidade e de proteção adequada contra o livre arbítrio;

— esta obrigação e as garantias que a acompanham devem respeitar o conteúdo essencial dos direitos reconhecidos nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais;

— esta obrigação deve ser estritamente necessária na luta contra as infrações graves, o que implica que nenhuma outra medida ou combinação de medidas deve ser considerada tão eficaz na luta contra as infrações graves sendo, simultaneamente, menos atentatória dos direitos consagrados na Diretiva 2002/58 e nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais;

— esta obrigação deve ser acompanhada de todas as garantias enunciadas pelo Tribunal de Justiça nos n.os 60 a 68 do acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238), relativas ao acesso aos dados, à duração da conservação, bem como à proteção e à segurança dos dados, para limitar à estrita medida do necessário a afetação dos direitos consagrados na Diretiva 2002/58 e nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais, e

— esta obrigação deve ser proporcionada, numa sociedade democrática, ao objetivo de luta contra as infrações graves, o que implica que os graves riscos decorrentes desta obrigação numa sociedade democrática não devem ser desmesurados face às vantagens que dela resultam na luta contra as infrações graves.