Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
MANUEL CAMPOS SÁNCHEZ-BORDONA
apresentadas em 18 de novembro de 2021 [1]

Processos apensos C-793/19 e C-794/19

Bundesrepublik Deutschland
contra
SpaceNet AG (C-793/19)
Telekom Deutschland GmbH (C-794/19)

[pedido de decisão prejudicial apresentado pelo Bundesverwaltungsgericht (Supremo Tribunal Administrativo Federal, Alemanha)]

«Questão prejudicial — Telecomunicações — Tratamento de dados de natureza pessoal e proteção da vida privada no sector das comunicações eletrónicas — Diretiva 2002/58/CE — Artigo 15.º, n.º 1 — Artigo 4.º, n.º 2, TUE — Carta dos Direitos Fundamentais da União Europeia — Artigos 6.º, 7.º, 8.º, 11.º e 52.º, n.º 1 — Conservação generalizada e indiferenciada dos dados de ligação para efeitos de exercício da ação penal por crimes graves ou de defesa contra um perigo real para a segurança nacional»

1. Os presentes pedidos de decisão prejudicial, aos quais acresce o que foi apresentado no processo C-140/20 [2], evidenciam, uma vez mais, a preocupação suscitada em alguns Estados-Membros pela jurisprudência do Tribunal de Justiça relativa à conservação e ao acesso aos dados pessoais gerados no sector das comunicações eletrónicas.

2. Nas Conclusões apresentadas nos processos C-511/18 e C-512/18, La Quadrature du Net e o. [3], e C-520/18, Ordre des barreaux francophones et germanophone e o. [4], assinalei como marcos dessa jurisprudência, até aquele momento, os seguintes acórdãos:

— O Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. [5], que declarou a invalidade da Diretiva 2006/24/CE [6], na medida em que implicava uma ingerência desproporcionada nos direitos reconhecidos pelos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

1 Língua original: espanhol.

2 Processo C-140/20, Commissioner of the Garda Síochána e o., sobre o qual apresento igualmente conclusões nesta mesma data.

3 A seguir «Conclusões La Quadrature du Net» (EU:C:2020:6).

4 A seguir «Conclusões Ordre des barreaux francophones et germanophone» (EU:C:2020:7).

5 Processos C-293/12 e C-594/12 (EU:C:2014:238; a seguir «Acórdão Digital Rights»).

6 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).

— O Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o.[7], em que se declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58/CE[8] se opõe a uma regulamentação nacional que preveja uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização para efeitos de luta contra a criminalidade grave.

— O Acórdão de 2 de outubro de 2018, Ministerio Fiscal[9], que confirmou a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, especificando a importância do princípio da proporcionalidade a esse respeito.

3. Em 2018, alguns órgãos jurisdicionais de alguns Estados-Membros dirigiram-se ao Tribunal de Justiça, mediante pedidos de decisão prejudicial, exprimindo dúvidas quanto à questão de saber se esses acórdãos (de 2014, 2016 e 2018) eram suscetíveis de subtrair às autoridades estatais um instrumento necessário à salvaguarda da segurança nacional e à luta contra a criminalidade e o terrorismo.

4. Quatro desses pedidos de decisão prejudicial deram origem aos Acórdãos Privacy Internacional[10] e La Quadrature du Net e o.[11], ambos de 6 de outubro de 2020, que corroboraram, em substância, a jurisprudência do Acórdão Tele2 Sverige, introduzindo embora algumas matizes adicionais.

5. Atendendo à sua origem (a Grande Secção do Tribunal de Justiça), ao seu conteúdo e à sua preocupação em explicar pormenorizadamente, em diálogo com os órgãos jurisdicionais de reenvio, as razões que, apesar de tudo, sustentam as teses aí expostas, poder-se-ia esperar que esses dois acórdãos «recapitulativos» de 6 de outubro de 2020 tivessem encerrado o debate. Por conseguinte, qualquer outro pedido de decisão prejudicial relativo ao mesmo assunto seria respondido pelo despacho fundamentado referido no artigo 99.º do Regulamento de Processo do Tribunal de Justiça.

6. Todavia, antes de 6 de outubro de 2020, tinham dado entrada no Tribunal de Justiça três outros pedidos de decisão prejudicial (os dois apensos no presente processo e o do processo C-140/20), cujo teor punha novamente em causa a jurisprudência relativa ao artigo 15.º, n.º 1, da Diretiva 2002/58.

7. O Tribunal de Justiça deu conhecimento dos Acórdãos de 6 de outubro de 2020 aos órgãos jurisdicionais de reenvio, questionando se pretendiam retirar os seus pedidos de decisão prejudicial. Tendo em conta a sua insistência em mantê-los, como exporei adiante[12], foi decidido não aplicar o artigo 99.º do Regulamento de Processo e que a Grande Secção do Tribunal de Justiça lhes daria resposta.

7 Processos C-203/15 e C-698/15 (EU:C:2016:970; a seguir «Acórdão Tele2 Sverige»).

8 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 sector 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).

9 Processo C-207/16 (EU:C:2018:788).

10 Processo C-623/17 (EU:C:2020:790).

11 Processos C-511/18, C-512/18 e C-520/18 (EU:C:2020:791; a seguir «Acórdão La Quadrature du Net»).

12 N.º 30 das presentes conclusões.

I. Quadro jurídico

A. Direito da União: Diretiva 2002/58

8. Nos termos do artigo 5.º («Confidencialidade das comunicações»), n.º 1:

«Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.º 1 do artigo 15. O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.»

9. O artigo 6.º («Dados de tráfego») dispõe:

«1. Sem prejuízo do disposto nos n.ºs 2, 3 e 5 do presente artigo e no n.º 1 do artigo 15.º, os dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações eletrónicas publicamente disponíveis devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.

2. Podem ser tratados dados de tráfego necessários para efeitos de faturação dos assinantes e de pagamento de interligações. O referido tratamento é lícito apenas até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado.

[…]»

10. O artigo 15.º («Aplicação de determinadas disposições da Diretiva 95/46/CE») [13] prevê no seu n.º 1:

«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/CE. 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 Tratado da União Europeia.»

[13] 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).

B. Direito nacional

1. Telekommunikationsgesetz (Lei das Telecomunicações; a seguir «TKG»)

11. O § 113a, n.º 1, estabelece:

«As obrigações relativas à conservação, utilização e segurança dos dados de tráfego definidas nos §§ 113b a 113g dizem respeito aos operadores que prestam aos utilizadores finais serviços de telecomunicações publicamente disponíveis.»

12. O § 113b prevê:

«(1) Os operadores referidos no § 113a devem conservar os dados no território nacional da seguinte forma:

1. durante dez semanas, no caso dos dados referidos nos n.os 2 e 3,

2. durante quatro semanas, no caso dos dados de localização referidos no n.º 4.

(2) Os prestadores de serviços telefónicos publicamente acessíveis conservam

1. o número de telefone ou outra identificação da linha chamadora e da linha conectada e, no caso de comutações e reencaminhamentos, o de qualquer outra ligação envolvida,

2. a data e a hora do início e do fim da comunicação, mediante indicação do fuso horário utilizado,

3. os dados sobre o serviço utilizado, quando puderem ser utilizados vários serviços no âmbito do serviço telefónico,

4. e ainda, no caso de serviços de comunicação móvel,

   a) a identificação internacional dos assinantes móveis da linha chamadora e da linha conectada,

   b) a identificação internacional do equipamento terminal da linha chamadora e da linha conectada,

   c) a data e a hora da primeira ativação do serviço, com indicação do fuso horário utilizado, se os serviços forem pré-pagos,

5. e, no caso de serviços de comunicação móvel através da Internet, o endereço do protocolo IP da linha chamadora e da linha conectada e os códigos de identificação atribuídos ao utilizador.

O primeiro parágrafo aplica-se com as devidas adaptações

1. em caso de comunicação por SMS, mensagem multimédia ou semelhante; neste caso, os dados referidos no ponto 2 do primeiro parágrafo são substituídos pelos momentos do envio e da receção da mensagem;

2. às comunicações sem resposta ou sem sucesso devido a uma intervenção do operador da rede […].

(3) Os prestadores de serviços de Internet publicamente disponíveis conservam

1. o endereço do protocolo IP atribuído ao assinante para a utilização da Internet,

2. uma identificação inequívoca da ligação através da qual a Internet é utilizada e os identificadores atribuídos aos utilizadores,

3. a data e a hora do início e do fim da utilização da Internet ao abrigo do endereço do protocolo IP atribuído, mediante indicação do fuso horário utilizado.

(4) Em caso de utilização de serviços de comunicação móvel, há que conservar a indicação das células telefónicas utilizadas no início da ligação por quem faz a chamada e por quem a recebe. No que respeita aos serviços de Internet publicamente disponíveis, há que conservar, em caso de utilização móvel, a indicação das células telefónicas utilizadas no início da ligação. Importa igualmente conservar os dados que permitam conhecer a posição geográfica e as direções de radiação máxima das antenas que servem a célula telefónica em causa.

(5) O conteúdo da comunicação, os dados sobre páginas Internet visualizadas e os dados sobre serviços de correio eletrónico não podem ser conservados por força da presente disposição.

(6) Os dados subjacentes às comunicações referidas no artigo 99.º, n.º 2, não podem ser conservados por força da presente disposição. Isto é válido, com as devidas alterações, para as comunicações móveis provenientes das entidades referidas no artigo 99.º, n.º 2. O artigo 99.º, n.º 2, segundo a sétimo períodos, aplica-se com as devidas alterações [14].

[…]»

13. Nos termos do § 113c:

«(1) Os dados conservados por força do § 113b podem

1. ser transferidos para uma autoridade responsável pela ação penal quando esta pede a transferência invocando uma disposição legal que a autoriza a recolher os dados referidos no § 113b efeitos de exercício da ação penal por crimes particularmente graves;

2. ser transferidos para uma autoridade de segurança dos *Länder* quando esta pede a transferência invocando uma disposição legal que a autoriza a reunir os dados referidos no § 113b para efeitos da defesa contra um perigo real para a integridade física, a vida ou a liberdade de uma pessoa ou para a existência do Estado Federal ou do *Land*;

14 As comunicações a que se refere o artigo 99.º, n.º 2, da TKG são comunicações com pessoas, autoridades e organizações no âmbito social ou eclesiástico disponibilizadas a parceiros, em princípio anónimos, serviços de assistência telefónica em caso de urgência psicológica ou social e que estão sujeitos a obrigações especiais de confidencialidade. Nos termos do artigo 99.º, n.º 2, segundo a quarto períodos, da TKG, esta derrogação está subordinada à inscrição numa lista gerida pela Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agência federal das redes de eletricidade, do gás, das telecomunicações, dos correios e dos caminhos de ferro; a seguir «Agência Federal das Redes»), após homologação da natureza dos seus serviços através da certificação conferida por uma entidade, organismo ou fundação de direito público.

3. serem utilizados pelo operador de serviços de telecomunicações publicamente disponíveis para a prestação de informações nos termos do § 113, n.º 1, terceiro período.

(2) Os dados conservados nos termos do § 113b não podem ser utilizados, por quem está sujeito às obrigações previstas no § 113a, n.º 1, para fins diferentes dos referidos no n.º 1.

[…]»

14. O § 113d prevê:

«O destinatário da obrigação prevista no § 113a, n.º 1, deve assegurar que os dados conservados em conformidade com o § 113b, n.º 1, por força da obrigação de conservação são protegidos por medidas técnicas e organizativas conformes com o estado da técnica, contra o controlo e a utilização não autorizadas. Estas medidas incluem, nomeadamente:

1. o recurso a um processo de codificação particularmente seguro,

2. a conservação em infraestruturas de conservação diferentes, separadas das destinadas a funções operacionais correntes,

3. a conservação, dotada de elevado nível de proteção contra os ciberataques, em sistemas informáticos de tratamento de dados desconectados,

4. a limitação do acesso às instalações utilizadas no tratamento dos dados às pessoas que dispõem de uma habilitação especial conferida pelo responsável pela obrigação e

5. a obrigação de fazer intervir, durante o acesso aos dados, pelo menos duas pessoas que disponham de uma habilitação especial conferida pelo responsável pela obrigação.»

15. O § 113e tem a seguinte redação:

«(1) O responsável pela obrigação prevista no § 113a, n.º 1, deve assegurar que, para efeitos de controlo da proteção de dados, se registe cada acesso, em especial, a leitura, a cópia, a alteração, a eliminação e o bloqueio dos dados conservados em conformidade com o § 113b, n.º 1, por força da obrigação de conservação. Devem ser objeto de registo

1. a hora do acesso,

2. as pessoas que acedem aos dados,

3. o objeto e a natureza do acesso.

(2) Os dados registados só podem ser utilizados para o controlo da proteção de dados.

(3) O responsável pela obrigação referida no § 113a, n.º 1, deve assegurar que os dados registados são eliminados ao fim de um ano.»

2. Strafprozessordnung (Código de Processo Penal; a seguir «StPO»)

16. O § 100g dispõe:

«[…]

(2) Caso determinados factos permitam suspeitar que uma pessoa cometeu, na qualidade de autor ou de cúmplice, um dos crimes particularmente graves referidos no segundo período ou, nos casos em que a tentativa é punível, a pessoa a tenha cometido e o crime em causa seja também particularmente grave, os dados de tráfego, conservados em conformidade com o § 113b da [TKG], podem ser recolhidos se a investigação sobre os factos ou a localização da pessoa investigada forem excessivamente difíceis ou inviáveis por outros meios e a recolha dos dados for proporcional à importância do processo.

[…]

(4) Não é autorizada a recolha de dados de tráfego nos termos do n.º 2 […] que possa conduzir a informações sobre as quais a pessoa em causa possa recusar testemunhar […]».

17. Por força do § 101a, n.º 2, dessa mesma lei, a decisão judicial deve ponderar a necessidade e a pertinência da medida no caso concreto, cuja adoção deve ser notificada aos participantes na comunicação (§ 101, n.º 6, do StPO).

II. Matéria de facto, litígios e questões prejudiciais

18. A SpaceNet AG e a Telekom Deutschland GmbH são sociedades que, na República Federal de Alemanha, prestam serviços de comunicações eletrónicas publicamente disponíveis.

19. Essas duas sociedades intentaram ações no Verwaltungsgericht (Tribunal Administrativo, Alemanha) contestando a obrigação de conservarem os dados de tráfego de telecomunicações dos seus clientes a partir de 1 de julho de 2017, imposta pelo § 113a, n.º 1, em conjugação com o § 113b, da TKG.

20. Tendo ambas as ações sido julgadas procedentes em primeira instância, a Agência Federal das Redes interpôs dois recursos de «*Revision*» no Bundesverwaltungsgericht (Supremo Tribunal Administrativo Federal, Alemanha), que, antes de se pronunciar, decidiu submeter, em ambos os processos, as seguintes questões prejudiciais:

«Deve o artigo 15.º da Diretiva 2002/58/CE, à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta […], por um lado, e do artigo 6.º da Carta […] e do artigo 4.º [TUE], por outro, ser interpretado no sentido de que se opõe a uma regulamentação nacional que obriga os prestadores de serviços de comunicações publicamente disponíveis a conservarem os dados de tráfego e de localização dos utilizadores finais destes serviços, quando:

— esta obrigação não pressuponha nenhum motivo específico de ordem local, temporal ou geográfica,

— esta obrigação de conservação no âmbito da prestação de serviços de comunicações publicamente disponíveis, incluindo a transmissão de notícias curtas ou de notícias

multimédia ou semelhantes, bem como chamadas não atendidas ou comunicações falhadas, tiver por objeto os seguintes dados:

— o número de telefone ou outra identificação da linha chamadora e da linha conectada e, no caso de comutações e reencaminhamentos, o de qualquer outra ligação envolvida,

— a data e a hora do início e do fim da comunicação ou, no caso de transmissão de notícias curtas ou de notícias multimédia ou semelhantes, as datas da transmissão e da receção da notícia, mediante indicação do fuso horário utilizado,

— dados sobre o serviço utilizado, quando puderem ser utilizados vários serviços no âmbito do serviço telefónico,

— e ainda, no caso de serviços de comunicação móvel,

— a identificação internacional dos assinantes móveis da linha chamadora e da linha conectada,

— a identificação internacional do equipamento terminal da linha chamadora e da linha conectada,

— a data e a hora da primeira ativação do serviço, com indicação do fuso horário utilizado, se os serviços forem pré-pagos,

— a indicação das células utilizadas para a linha chamadora e a linha conectada no início da ligação,

— e, no caso de serviços telefónicos através da Internet, o endereço do protocolo IP da linha chamadora e da linha conectada e os códigos de identificação atribuídos ao utilizador,

— a obrigação de conservação, no âmbito da prestação de serviços de Internet publicamente disponíveis, tiver por objeto os seguintes dados:

— o endereço do protocolo IP atribuído ao assinante para a utilização da Internet,

— uma identificação inequívoca da ligação através da qual a Internet é utilizada e os identificadores atribuídos aos utilizadores,

— a data e a hora do início e do fim da utilização da Internet ao abrigo do endereço do protocolo IP atribuído, mediante indicação do fuso horário utilizado,

— em caso de utilização móvel, a indicação da célula utilizada no início da ligação à Internet,

— os seguintes dados não puderem ser conservados:

— o conteúdo da comunicação,

— dados sobre páginas Internet visualizadas,

— dados sobre serviços de correio eletrónico,

— dados subjacentes a determinadas ligações de ou para pessoas, autoridades e organizações no âmbito social ou eclesiástico,

— a duração da conservação de dados de localização, ou seja, a identificação da célula utilizada for de quatro semanas e a dos restantes dados, de dez semanas,

— for garantida a proteção eficaz dos dados conservados contra riscos de abuso e contra qualquer acesso não autorizado, e

— os dados conservados só puderem ser utilizados para efeitos de exercício da ação penal por crimes particularmente graves e de defesa contra um perigo real para a integridade física, a vida ou a liberdade de uma pessoa ou para a existência do Estado Federal ou de um *Land*, com exceção do endereço do protocolo IP atribuído ao assinante para efeitos de utilização da Internet, cuja utilização seja permitida no âmbito da obtenção de dados para efeitos de exercício da ação penal por quaisquer crimes, de defesa contra um risco para a segurança pública e para a ordem pública, bem como para o cumprimento das tarefas dos serviços de informação?»

21. Como explica o órgão jurisdicional de reenvio, a regulamentação da obrigação em causa foi alterada por uma Lei de 10 de dezembro de 2015 [15], cuja aprovação era necessária após:

— o Acórdão do Bundesverfassungsgericht (Tribunal Constitucional Federal, Alemanha) de 2 de março de 2010 [16], que declarou inconstitucionais as disposições anteriores que regulavam a conservação dos dados; e

— a declaração de nulidade da Diretiva 2006/24, para cuja transposição tinham sido adotadas as disposições anteriores.

22. O órgão jurisdicional de reenvio considera que a obrigação de conservação em causa restringe os direitos consagrados nos artigos 5.º, n.º 1, 6.º, n.º 1, e 9.º, n.º 1, da Diretiva 2002/58. Em seu entender, essa restrição só seria justificada se se pudesse fundamentar no artigo 15.º, n.º 1, dessa diretiva.

[15] Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Lei de Introdução de uma Obrigação de Conservação e de uma Obrigação Máxima de Conservação de Dados de Tráfego).

[16] 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (DE:BVerfG:2010:rs20100302.1bvr025608).

23. Para o órgão jurisdicional de reenvio, sem prejuízo da jurisprudência do Acórdão Tele2 Sverige, a obrigação controvertida poderia fundamentar-se no artigo 15.º, n.º 1, da Diretiva 2002/58, uma vez que:

— As normas nacionais aplicáveis não exigem a conservação de todos os dados de tráfego de telecomunicações de *todos* os assinantes e utilizadores registados no que diz respeito a *todos* os meios de comunicação eletrónicos.

— Essas normas reduziram significativamente (para um máximo de dez semanas) o prazo de conservação, em relação ao previsto pelas legislações analisadas no Acórdão Tele2 Sverige e o estabelecido pela Diretiva 2006/24, o que torna mais difícil a obtenção de perfis.

— Foram impostas limitações estritas em matéria de proteção, de acesso e de utilização dos dados conservados.

— O legislador nacional ter-se-ia limitado a cumprir o dever de intervenção que o direito à segurança (artigo 6.º da Carta) implica [17].

— Caso a conservação de dados «sem motivo» [18] não se possa fundamentar, em termos gerais, no artigo 15.º, n.º 1, da Diretiva 2002/58 (ou seja, se fosse irrelevante a regulamentação em matéria de meios de comunicação abrangidos, categorias dos dados a conservar, duração da conservação, requisitos de acesso aos dados conservados e proteção contra abusos) a margem de atuação dos legisladores nacionais no domínio da ação penal e da segurança pública, que, nos termos do artigo 4.º, n.º 2, terceiro período, TUE, continua, em todo o caso, a ser da responsabilidade exclusiva dos Estados-Membros, seria consideravelmente restringida.

— Deve velar-se pela necessária coerência entre os direitos consagrados na Carta e os direitos correspondentes garantidos pela Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (a seguir «CEDH»), interpretados pelo Tribunal Europeu dos Direitos do Homem (a seguir «TEDH»), sem prejuízo da independência do direito da União e da autoridade do Tribunal de Justiça.

III. Tramitação do Tribunal de Justiça

24. Os pedidos de decisão prejudicial deram entrada no Tribunal de Justiça em 29 de outubro de 2019.

25. Apresentaram observações escritas a SpaceNet, a Telekom Deutschland, os Governos alemão, dinamarquês, espanhol, estónio, finlandês, francês, irlandês, neerlandês, polaco e sueco, bem como a Comissão Europeia.

26. Tendo o órgão jurisdicional de reenvio sido convidado a pronunciar-se sobre a eventual retirada da questão prejudicial, na sequência da prolação do Acórdão La Quadratura du Net, manifestou, em 13 de janeiro de 2021, a sua intenção de a manter, uma vez que não podia considerar-se decidida com esse acórdão.

[17] Segundo o órgão jurisdicional de reenvio, a jurisprudência do Tribunal de Justiça não fecha totalmente a porta a que os legisladores nacionais possam introduzir a conservação de dados sem motivo, eventualmente complementada por rigorosas normas de acesso, com base numa apreciação global, a fim de terem em conta o potencial específico de risco que é associado aos novos meios de telecomunicação.

[18] É esta a expressão literal utilizada pelo órgão jurisdicional de reenvio.

27. A audiência pública realizada conjuntamente com a do processo conexo C-140/20 teve lugar em 13 de setembro de 2021, tendo comparecido, além dos intervenientes neste processo que apresentaram observações escritas, a Agência Federal das Redes e a Autoridade Europeia para a Proteção de Dados.

IV. Análise

A. Apreciação preliminar

28. A tramitação destes dois pedidos de decisão prejudicial pode ser efetuada analisando-os tal como foram submetidos, ou preferencialmente à luz das considerações que o órgão jurisdicional de reenvio invocou, em resposta ao Tribunal de Justiça, em 13 de janeiro de 2021, para justificar a sua manutenção, após ter tomado conhecimento do Acórdão La Quadrature du Net.

29. Embora aborde sucintamente os pontos mais pertinentes do pedido de decisão prejudicial originário, focar-me-ei na análise dos motivos pelos quais, na opinião do órgão jurisdicional de reenvio, a intervenção do Tribunal de Justiça continua a ser pertinente. Em resumo, todos estes motivos dizem respeito ao facto de a situação normativa de base ser distinta da examinada no Acórdão La Quadrature du Net.

30. Na sua comunicação de 13 de janeiro de 2021, o órgão jurisdicional de reenvio invocou os seguintes argumentos:

— As diferenças entre as disposições alemãs e as disposições francesas e belgas que deram lugar ao Acórdão La Quadrature du Net são consideráveis. Nos termos das primeiras, os dados relativos aos sítios Internet consultados, os do correio eletrónico e os relativos às comunicações para ou a partir de serviços de assistência via comunicação móvel de natureza social ou religiosa não são conservados.

— Outra diferença ainda mais relevante reside no facto de a duração da conservação, nos termos do § 113b, n.º 1, da TKG, ser de quatro ou dez semanas, e não de um ano. Este aspeto reduz o risco de elaboração de um perfil global das pessoas em causa.

— As normas alemãs conferem uma proteção eficaz dos dados conservados contra os perigos de abuso e de acesso ilícito.

— Após uma decisão recente do Bundesverfassungsgericht (Tribunal Constitucional Federal) sobre o § 113 da TKG[19], a validade dessa disposição ficou sujeita a condições cuja compatibilidade com o direito da União não é fácil de determinar.

— Subsistem dúvidas quanto às exigências do direito da União sobre os endereços IP, uma vez que o Acórdão La Quadrature du Net não permite deduzir claramente se a sua conservação é genericamente excluída, observando-se alguma tensão entre os seus n.os 168 e 155.

[19] Acórdão de 27 de maio de 2020, 1 BvR 1873/13, 1 BvR 2618/13 (DE:BVerfG:2020:rs20200527.1bvr187313). Em conformidade com esse acórdão, o § 113 da TKG é incompatível com os artigos 2.º, n.º 1, e 10.º, n.º 1, da Grundgesetz (Constituição) e só pode ser aplicado até à adoção de novas regras, o mais tardar até 31 de dezembro de 2021.

B. Aplicabilidade da Diretiva 2002/58

31. No essencial, a República da Irlanda e os Governos francês, neerlandês, polaco e sueco defendem que a Diretiva 2002/58 não é aplicável a regulamentações nacionais como as que estão em causa nestes litígios. Tendo por objeto a salvaguarda da segurança nacional, bem como a prevenção e repressão de crimes graves, essas regulamentações são da competência exclusiva dos Estados-Membros, em conformidade com o artigo 4.º, n.º 2, TUE.

32. A objeção foi claramente rejeitada pelo Tribunal de Justiça no Acórdão La Quadrature du Net, ao declarar que «uma regulamentação nacional que impõe aos prestadores de serviços de comunicações eletrónicas a conservação de dados de tráfego e de dados de localização para efeitos da proteção da segurança nacional e da luta contra a criminalidade, tal como os que estão em causa no processo principal, se integra no âmbito de aplicação da Diretiva 2002/58» [20].

33. O órgão jurisdicional de reenvio acolhe esta premissa ao corroborar a apreciação da primeira instância e acrescenta que a aplicabilidade da Diretiva 2005/58 nesta situação tinha sido «definitivamente estabelecida» pelo Acórdão Tele2 Sverige [21].

34. Por conseguinte, não me alargarei sobre este ponto, sobre o qual tive a oportunidade de me pronunciar em devido tempo, em linha com a posição adotada pelo Tribunal de Justiça, nas Conclusões La Quadrature du Net [22].

C. Conservação generalizada e indiferenciada versus conservação seletiva dos dados de tráfego e dos dados de localização

35. A ideia central da jurisprudência do Tribunal de Justiça relativa à Diretiva 2002/58 é a de que os utilizadores dos meios de comunicações eletrónicas têm o direito de esperar, em princípio, que, as suas comunicações e respetivos dados permaneçam anónimos e não possam ser objeto de registo, a não ser que tenham dado consentimento [23].

36. O artigo 15.º, n.º 1, da Diretiva 2002/58, admite exceções à obrigação de assegurar a confidencialidade e as obrigações correspondentes, nos termos que exporei adiante. O Acórdão La Quadrature du Net desenvolve a análise da conciliação dessas derrogações com os direitos fundamentais cujo exercício é suscetível de ser afetado [24].

37. A conservação generalizada e indiferenciada dos dados de tráfego só pode ser justificada, segundo o Tribunal de Justiça, pelo objetivo de salvaguarda da segurança nacional, cuja importância «ultrapassa a dos outros objetivos referidos no artigo 15.º, n.º 1, da Diretiva 2002/58» [25].

38. Nesse caso (segurança nacional), o Tribunal de Justiça declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, «não se opõe, em princípio, a *uma medida legislativa que autoriza as autoridades competentes a impor* aos

20 Acórdão La Quadrature du Net, n.º 104.

21 N.º 19, alínea a), do despacho de reenvio.

22 Conclusões La Quadrature du Net, n.ºs 40 a 90.

23 Acórdão La Quadrature du Net, n.º 109.

24 *Ibidem*, n.ºs 111 a 133.

25 Acórdão La Quadrature du Net, n.º 136.

prestadores de serviços de comunicações eletrónicas o dever de procederem *à conservação* de dados de tráfego e de dados de localização de todos os utilizadores de meios de comunicações eletrónicos *durante um período limitado*, desde que existam circunstâncias suficientemente concretas que permitam considerar que o Estado-Membro em causa enfrenta uma ameaça grave […] para a segurança nacional que se afigure real e atual ou previsível» [26].

39. É certo que estas disposições dão origem a um regime mais rigoroso e mais estrito do que o que resulta da jurisprudência do TEDH relativa ao artigo 8.º da CEDH. O facto de «o sentido e o âmbito dos direitos» da Carta correspondentes aos da CEDH terem de ser iguais aos conferidos nesta última não obsta, nos termos do artigo 52.º, n.º 3, *in fine*, da Carta, a que o direito da União confira uma proteção mais ampla.

40. De resto, a jurisprudência do TEDH nos seus Acórdãos de 25 de maio de 2021, Big Brother Watch e o. c. Reino Unido [27] e Centrum for Rättvisa c. Suécia [28], bem como no de 4 de dezembro de 2015, Zakharov c. Rússia [29], diz respeito a casos que, como defenderam predominantemente as partes na audiência, não são equiparáveis aos debatidos nos reenvios prejudiciais aqui em causa. A solução para estes últimos deve ser encontrada aplicando normas nacionais consideradas conformes com a regulamentação *exaustiva* da Diretiva 2002/58, como interpretada pelo Tribunal de Justiça.

41. Seja qual for a opinião quanto à invocação da segurança nacional, no Acórdão La Quadrature du Net, como motivo para levantar, sob determinadas condições, a proibição de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização (na minha opinião, os limites traçados pelo Tribunal de Justiça são excessivamente amplos), as regras enumeradas nos n.ºs 137 a 139 desse acórdão devem ser respeitadas.

42. Fora desta hipótese, haverá que examinar se a regulamentação nacional assenta em critérios suficientemente *seletivos* para, em conformidade com a jurisprudência do Tribunal de Justiça, preencher as condições suscetíveis justificar uma ingerência particularmente grave, como a conservação de dados, nos direitos fundamentais em causa.

43. A *conservação seletiva* dos dados de tráfego e dos dados de localização [30] constitui a pedra angular da fundamentação dos acórdãos do Tribunal de Justiça nesta matéria. Essa seleção pode ser realizada em função das categorias de pessoas em causa [31] ou assentar num critério geográfico [32], entre outros.

[26] *Ibidem*, n.º 137 (o sublinhado é meu). Com efeito, segundo o Tribunal de Justiça, «[e]mbora tal medida vise, de forma indiferenciada, todos os utilizadores de meios de comunicações eletrónicos sem que, à primeira vista, se afigure estarem relacionados […] com uma ameaça para a segurança nacional desse Estado-Membro», há que «considerar, no entanto, que a existência de tal ameaça é, por si só, suscetível de demonstrar essa relação» (*loc. ult. cit.*).

[27] CE:ECHR:2021:0525JUD005817013.

[28] CE:ECHR:2021:0525JUD003525208.

[29] CE:ECHR:2015:1204JUD004714306.

[30] Acórdão La Quadrature du Net, n.º 147: «o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não se opõe a que um Estado-Membro adote uma regulamentação que permita, a título preventivo, a *conservação seletiva* dos dados de tráfego e dos dados de localização, para efeitos da luta contra a criminalidade grave e da prevenção das ameaças graves contra a segurança pública, tal como para efeitos da salvaguarda da segurança nacional, desde que tal conservação seja, no que diz respeito às categorias de dados a conservar, aos meios de comunicação visados, às pessoas em causa e à duração de conservação fixada, limitada ao estritamente necessário». O sublinhado é meu.

[31] Acórdão La Quadrature du Net, n.ºs 148 e 149.

[32] Acórdão La Quadrature du Net, n.º 150.

44. Tanto o órgão jurisdicional de reenvio como a maioria das partes que apresentaram observações estão de acordo em sublinhar as dificuldades criadas pelos critérios elaborados pelo Tribunal de Justiça. Eu próprio indiquei algumas dessas dificuldades [33] nas Conclusões no processo Ordre des barreaux francophones et germanophone [34].

45. Ora, não se pode excluir fórmulas de conservação seletivas baseadas nesses critérios que possam ser eficazes e, simultaneamente, não discriminatórias. Compete aos legisladores nacionais, e não ao Tribunal de Justiça, concebê-los de um modo conforme com os direitos fundamentais garantidos pela Carta [35].

46. De resto, insisto no facto de que seria errado deduzir que os critérios pessoal e geográfico são os únicos compatíveis com o artigo 15.º, n.º 1, da Diretiva 2002/58, à luz dos direitos protegidos na Carta.

47. Ainda que o Governo francês sustente que se revelaram ineficazes [36], também não considero que se possam rejeitar as modalidades propostas pelos grupos de trabalho reunidos no âmbito do Conselho [37] para definir regras de conservação e de acesso compatíveis com a jurisprudência do Tribunal de Justiça [38].

48. Na minha opinião, deve dar-se preferência a uma conservação temporária de algumas *categorias* de dados de tráfego e de localização, limitadas em função de estritas necessidades de segurança, que não permitam, no seu conjunto, obter uma imagem específica e detalhada da vida das pessoas em causa. Na prática, isto significa que, em relação às duas categorias principais (dados de tráfego e dados de localização) devem apenas conservar-se, com os filtros adequados, os dados *mínimos* que se considerem absolutamente imprescindíveis para a prevenção e o controlo eficazes da criminalidade e para salvaguardar a segurança nacional [39].

49. Em todo o caso, repito, compete aos Estados-Membros ou às instituições da União realizar, por via legislativa (com a colaboração dos seus próprios peritos), este exercício de seleção, abandonando qualquer tentativa de impor um armazenamento generalizado e indiferenciado de todos os dados de tráfego e de localização [40].

50. Por essa razão, nas Conclusões no processo Ordre des barreaux francophones et germanophone afirmava que «[a] dificuldade legislativa — que reconheço — de configurar com precisão os casos e as condições em que é necessário efetuar uma conservação seletiva não justifica que os Estados-Membros, fazendo da exceção uma regra, convertam a conservação

[33] Além da sua insuficiência, a possibilidade de levarem à instauração de um regime de suspeição geral sobre alguns segmentos da população ou à estigmatização de zonas geográficas.

[34] Conclusões no processo Ordre des barreaux francophones et germanophone, n.os 88 e 89.

[35] *Ibidem*, n.º 90.

[36] N.º 47 das suas observações escritas. Apreciação que foi igualmente objeto de insistência por parte de alguns Governos durante a audiência.

[37] Groupe Échange d'informations et protection des données (DAPIX). O Governo sueco pronunciou-se no mesmo sentido no n.º 21 das suas observações escritas.

[38] No n.º 92 das Conclusões no processo Ordre des barreaux francophones et germanophone salientei que esses grupos de trabalho consideraram, como meios de exploração, a limitação das categorias de dados conservados, a pseudonimização dos dados, a previsão de períodos de conservação limitados, a exclusão de determinadas categorias de prestadores de serviços de comunicações eletrónicas, as autorizações de armazenamento renováveis, a obrigação de conservar os dados armazenados dentro da União ou o controlo sistemático e periódico por parte de uma autoridade administrativa independente das garantias oferecidas pelos prestadores de serviços de comunicações eletrónicas contra a utilização indevida dos dados.

[39] Conclusões Ordre des barreaux francophones et germanophone, n.os 93 e 94.

[40] *Ibidem*, n.º 95.

generalizada de dados pessoais no princípio essencial das suas legislações. Se assim acontecesse, estaria a admitir-se a vigência indefinida de uma importante violação do direito à proteção dos dados pessoais» [41].

D. N.º 168 do Acórdão La Quadrature du Net

51. Neste contexto, na minha opinião, os elementos indispensáveis para responder ao órgão jurisdicional de reenvio decorrem diretamente da jurisprudência do Tribunal de Justiça relativa ao artigo 15.º, n.º 1, da Diretiva 2002/58, que foi recapitulada no Acórdão La Quadrature du Net.

52. Por conseguinte, recordo, antes de mais, a jurisprudência do Tribunal de Justiça nesse acórdão, que é sintetizada no seu n.º 168 do seguinte modo:

«[O] artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a medidas legislativas que preveem, para as finalidades previstas nesse artigo 15.º, n.º 1, a título preventivo, uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização. Em contrapartida, o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que:

— permitam, para efeitos da salvaguarda da segurança nacional, impor aos prestadores de serviços de comunicações eletrónicas que procedam a uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, quando o Estado-Membro em causa enfrente uma ameaça grave para a segurança nacional que se revele real e atual ou previsível, quando a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva quer por um órgão jurisdicional quer por uma entidade administrativa efetiva independente, cuja decisão produza efeitos vinculativos, destinada a verificar a existência de uma dessas situações e o respeito dos requisitos e das garantias que devem estar previstos, e quando a referida imposição apenas possa ser aplicada por um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça;

— prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação selecionada dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

— prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

— prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública, uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, e

[41] *Ibidem*, n.º 104.

— permitam, para efeitos da luta contra a criminalidade grave e, *a fortiori*, da salvaguarda da segurança nacional, impor aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, o dever de procederem, por um determinado período, à conservação rápida de dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem,

desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa dispõem de garantias efetivas contra os riscos de abuso.»

E. Avaliação da legislação em causa nestes reenvios prejudiciais, à luz do Acórdão La Quadrature du Net

53. Segundo o órgão jurisdicional de reenvio, a quem compete a título exclusivo a sua interpretação, a legislação alemã impõe «a conservação, sem motivo, universal e indiferenciada em termos pessoais, temporais e geográficos, da maior parte de todos os dados relevantes de tráfego de telecomunicações» [42].

54. A regulamentação nacional em causa não se limita a autorizar as autoridades competentes a exigir a conservação dos dados de tráfego e dos dados de localização durante um período limitado: é o legislador que impõe diretamente, e de forma indefinida, a obrigação de os conservar.

55. Assente esta premissa, aquele órgão jurisdicional enumerou, na sua comunicação de 13 de janeiro de 2021, as diferenças entre as normas nacionais e as referidas no Acórdão La Quadrature du Net, que poderiam conduzir a uma solução diferente da então adotada.

56. Procederei à análise dessas diferenças seguindo a ordem em que o órgão jurisdicional de reenvio as expõe, mas antes devo reconhecer que o legislador alemão se empenhou seriamente na tarefa de adaptar a regulamentação nacional às exigências que, neste domínio, decorrem da jurisprudência do Tribunal de Justiça.

57. Como sublinha o órgão jurisdicional de reenvio, a regulamentação em causa procede de uma alteração legislativa favorecida pela jurisprudência do Bundesverfassgericht (Tribunal Constitucional, Alemanha) e pelos efeitos da jurisprudência decorrente do Acórdão Digital Rights.

58. Por conseguinte, são de elogiar os progressos realizados na legislação nacional em causa, fruto de uma vontade determinada de adaptação à jurisprudência do Tribunal de Justiça.

59. Todavia, talvez o esforço legislativo tenha acentuado mais os aspetos relativos à proteção e ao acesso aos dados conservados, do que os relativos à delimitação seletiva daqueles cuja conservação se impõe.

1. Tipologia dos dados conservados

60. Na minha opinião, a tipologia dos dados conservados (os dados relativos aos sítios Internet consultados, os do correio eletrónico e os relativos às comunicações para ou a partir de serviços de assistência via comunicação móvel de natureza social ou religiosa não são conservados) não

[42] N.º 25b, alínea b), do original alemão do despacho de reenvio.

impede que se ignore que a obrigação de conservação generalizada e indiferenciada se estende a um conjunto amplíssimo de muitos outros dados de tráfego e de localização, que é semelhante, no seu todo, ao analisado no Acórdão La Quadrature du Net.

61. Neste sentido, é quase indiferente, dadas as suas características específicas e a sua incidência muito limitada na contabilização global [43], que sejam excluídos os dados subjacentes a determinadas ligações de assistência a comunicações móveis a cargo de pessoas, autoridades e organizações no âmbito social ou eclesiástico.

62. Também não é determinante que a obrigação de conservar não abranja os conteúdos (quer os dados sobre páginas Internet visualizadas, quer os dados sobre serviços de correio eletrónico), uma vez que o Acórdão La Quadrature du Net não lhes faz referência, mas sim aos dados de tráfego e aos dados de localização das comunicações eletrónicas.

2. Duração da obrigação de conservar os dados

63. A diferença mais relevante com as normas nacionais em causa no Acórdão La Quadrature du Net diz respeito à duração da conservação que, segundo o § 113b, n.º 1, da TKG, é de quatro ou de dez semanas (quatro semanas para os dados de localização e dez semanas para os outros), e não de um ano.

64. Tanto o órgão jurisdicional de reenvio como alguns governos que intervieram no processo insistem nesse aspeto, sublinhando que a regulamentação em causa reduz significativamente o prazo de conservação dos dados. Para o órgão jurisdicional de reenvio, a menor duração diminui o risco de elaboração de um perfil global das pessoas em causa.

65. Como defendi nas Conclusões Ordre des barreaux francophones et germonophone, fazendo especificamente eco da regulamentação nacional que aqui nos ocupa, é necessário que os dados conservados só o possam ser durante um período limitado [44], em função da sua pertença a uma ou a outras categorias [45].

66. Ora, se a limitação temporal do período de conservação constitui um elemento relevante para a apreciação da regulamentação em causa, esta circunstância não pode compensar o facto de que impõe a conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização.

67. Já referi que, segundo a jurisprudência do Tribunal de Justiça, excetuando a situação justificada pela defesa da segurança nacional, os dados relativos às comunicações eletrónicas só podem ser conservados seletivamente devido ao sério risco que a sua conservação generalizada implicaria.

[43] Na audiência, o Governo alemão estimou em 1 300 o número de entidades cujas comunicações eletrónicas estão excluídas da obrigação de conservação e clarificou que a exclusão não se pode aplicar aos profissionais sujeitos a deveres de sigilo profissional (como os advogados ou os médicos), em razão do seu elevado número.

[44] Conclusões Ordre des barreaux francophones et germonophone, n.º 96. Deste modo evita-se que «permitam proporcionar uma imagem detalhada da vida das pessoas em causa. Esse período de conservação deve, além do mais, ser adequado em função da natureza dos dados, para que os que proporcionem informação mais específica sobre os estilos de vida e os hábitos dessas pessoas sejam armazenados durante um período de tempo mais curto».

[45] *Ibidem*, n.º 97. «Por outras palavras, a diferenciação do período de conservação de cada categoria de dados, em função da sua utilidade para atingir os objetivos de segurança, é um recurso a explorar. Ao limitar o tempo durante o qual umas e outras categorias de dados são armazenadas simultaneamente (e, por conseguinte, podem ser utilizadas para estabelecer correlações que revelem o estilo de vida das pessoas em causa) está a ampliar-se a proteção do direito consagrado pelo artigo 8.º da Carta.»

68. Em suma, esse risco inspirou a jurisprudência do Tribunal de Justiça na matéria: «os dados de tráfego e os dados de localização são suscetíveis de revelar informações sobre um número significativo de aspetos da vida privada das pessoas em causa, incluindo informações sensíveis, tais como a orientação sexual, as opiniões políticas, as convicções religiosas, filosóficas, sociais ou outras, bem como o estado de saúde, uma vez que tais dados beneficiam, além disso, de uma proteção especial no direito da União. Considerados no seu todo, estes dados podem permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais dessas pessoas e os meios sociais que frequentam. Em especial, estes dados fornecem os meios para determinar o perfil das pessoas em causa, informação tão sensível, à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações» [46].

69. É certo que, como afirma o órgão jurisdicional de reenvio, uma conservação muito limitada no tempo pode dificultar a elaboração de perfis.

70. Todavia, a maior ou menor dificuldade a esse respeito depende não só da duração da conservação, mas também da quantidade e da qualidade dos dados conservados: quanto maior for o número de dados, maior será a possibilidade de obtenção de informações sensíveis durante períodos cuja extensão dependerá, por sua vez, da evolução das técnicas de monitorização, de correlação e de avaliação do conjunto dos dados relativos às comunicações eletrónicas. Um período que pode atualmente revelar-se insuficiente para a acumulação de informações que facilitem a obtenção de perfis, pode ser mais do que suficiente para o conseguir num futuro mais ou menos imediato [47].

71. Em todo o caso, e segundo o Tribunal de Justiça, «a ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que comporta o acesso, por uma autoridade pública, a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados, apresenta, de qualquer modo, um caráter grave *independentemente da duração do período em relação ao qual o acesso aos referidos dados é solicitado* e da quantidade ou da natureza dos dados disponíveis em relação a esse período, quando […] esse conjunto de dados seja suscetível de permitir tirar conclusões precisas sobre a vida privada da pessoa ou das pessoas em causa» [48].

72. Em suma, considero que, apesar das diferenças salientadas pelo órgão jurisdicional de reenvio, as semelhanças nesta matéria entre a regulamentação em causa nos processos principais e as legislações controvertidas nos processos que deram origem ao Acórdão La Quadrature du Net não permitem abstrair da jurisprudência deste último.

3. Proteção dos dados contra o seu acesso ilícito

73. O órgão jurisdicional de reenvio afirma que as normas alemãs conferem uma proteção eficaz dos dados conservados contra os perigos de abuso e de acesso ilícito.

[46] Acórdão La Quadrature du Net, n.º 117.

[47] Como foi salientado na audiência, mesmo um período de dez semanas de cumulação de metadados (dados de tráfego e dados de localização) poderia bastar para identificar padrões de comportamento do assinante que, pela sua repetição, revelariam traços sensíveis da sua personalidade e da sua vida.

[48] Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152, n.º 39). O sublinhado é meu.

74. Sem querer menorizar o esforço regulatório efetuado em matéria de proteção dos dados e do seu acesso, não se pode esquecer que, para o Tribunal de Justiça, «a conservação de dados de tráfego e de dados de localização constitui, *em si mesma* […] uma ingerência nos direitos fundamentais do respeito pela vida privada e da proteção dos dados pessoais» [49]. Nesse sentido, «o acesso a tais dados constitui, independentemente da utilização que deles seja feita posteriormente, uma *ingerência distinta*» nos referidos direitos fundamentais [50].

75. Por conseguinte, não é pertinente para o que ora importa que o regime de proteção dos dados conservados previsto pelo legislador alemão: a) assegure efetivamente a inviolabilidade desses dados; b) delimite as condições de acesso com rigor e eficácia, restringindo o círculo de pessoas que lhes podem aceder; e c) só permita a utilização dos dados conservados para efeitos de exercício da ação penal por crimes graves e de defesa contra um perigo real para a vida ou a liberdade de uma pessoa ou para a existência do Estado.

76. O que é verdadeiramente determinante é o facto de, como o órgão jurisdicional de reenvio também sublinha, a obrigação de conservação em causa, em si mesma, não estar sujeita a nenhuma condição específica.

4. Relevância do Acórdão do Bundesverfassungsgericht (Tribunal Constitucional Federal) de 27 de maio de 2020

77. O órgão jurisdicional de reenvio refere-se a uma decisão do Bundesverfassungsgericht (Tribunal Constitucional Federal) sobre o § 113 da TKG [51], na sequência da qual, após ter declarado a sua inconstitucionalidade, a validade dessa disposição teria ficado sujeita a condições cuja compatibilidade com o direito da União não seria fácil de determinar.

78. Nesta fase, o Tribunal de Justiça nada tem a declarar sobre os efeitos desse acórdão e muito menos sobre os contornos das novas regras que o legislador alemão tenha de adotar (ou, se for o caso, tenha adotado).

79. Se, como sustenta o órgão jurisdicional de reenvio, for chamado a proferir o seu acórdão de «*Revision*» à luz do direito em vigor à data em que for proferido, terá de apreciar, por si próprio, a sua compatibilidade com o direito da União à luz da jurisprudência do Tribunal de Justiça relativa à proteção de dados das comunicações eletrónicas.

5. Endereços IP

80. Segundo o órgão jurisdicional de reenvio, resulta do n.º 168 do Acórdão La Quadrature du Net que o Tribunal de Justiça exige, para os endereços IP, um motivo de conservação relacionado com o objetivo da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública. Todavia, resultaria do n.º 155 que esses endereços IP podem ser conservados sem que se verifique um motivo específico, sendo que apenas a utilização dos dados conservados exigiria um motivo relacionado com esse objetivo.

[49] Acórdão La Quadrature du Net, n.º 115.

[50] *Ibidem*, n.º 116. O sublinhado é meu.

[51] V. nota 19 das presentes conclusões.

81. No entanto, não considero que exista essa tensão (e ainda menos uma contradição). Embora se afirme, no n.º 155, que a conservação generalizada e indiferenciada apenas dos endereços IP atribuídos à fonte de uma ligação «não se afigura, em princípio, contrária ao artigo 15.º, n.º 1, da Diretiva 2002/58», declara-se em seguida, no n.º 156, que, «[t]endo em conta o caráter grave da ingerência nos direitos fundamentais […] que esta conservação comporta, só a luta contra a criminalidade grave e a prevenção das ameaças graves contra a segurança pública são suscetíveis, à semelhança da salvaguarda da segurança nacional, de justificar essa ingerência […]».

82. Por conseguinte, resulta da leitura conjugada dos n.ºs 155 e 156 do Acórdão La Quadratura du Net a resposta coerente que, no seu n.º 168, o Tribunal de Justiça deu às questões prejudiciais então submetidas sobre a conservação dos endereços IP.

83. Na audiência, foram suscitados determinados problemas que, segundo alguns intervenientes, exigiriam uma clarificação do Tribunal de Justiça, relativamente à conservação dos endereços IP. Em meu entender, a solução para esses problemas (entre outros, os decorrentes da diferença entre os endereços IP dinâmicos e os endereços IP estáticos, bem como da incidência do protocolo IPv6) excede o âmbito da questão submetida pelo órgão jurisdicional de reenvio, cujos pedidos iniciais de decisão prejudicial [52] e a comunicação de 13 de janeiro de 2021 têm, no que respeita a este aspeto, um alcance muito mais limitado.

V. Conclusão

84. Atendendo ao exposto, proponho que o Tribunal de Justiça responda ao Bundesverwaltungsgericht (Supremo Tribunal Administrativo Federal, Alemanha) nos seguintes termos:

«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 sector 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, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia e do artigo 4.º, n.º 2, TUE, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que obriga os prestadores de serviços de comunicações publicamente disponíveis a conservarem, de modo preventivo, geral e indiferenciado, os dados de tráfego e de localização dos utilizadores finais destes serviços para efeitos distintos da salvaguarda da segurança nacional em face de uma ameaça grave que se revele real e atual ou previsível.»

[52] N.º 30 do despacho de reenvio.