Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
M. CAMPOS SÁNCHEZ-BORDONA
apresentadas em 15 de janeiro de 2020[1]

Processos apensos C-511/18 e C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
contra
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

[pedido de decisão prejudicial interposto pelo Conseil d'État (Conselho de Estado, em formação jurisdicional, França)]

«Questão prejudicial — Tratamento de dados pessoais e proteção da vida privada no setor das comunicações eletrónicas — Salvaguarda da segurança nacional e luta contra o terrorismo — Diretiva 2002/58/CE — Âmbito de aplicação — Artigo 1.º, n.º 3 — Artigo 15.º, n.º 3 — Artigo 4.º, n.º 2, TUE — Carta dos Direitos Fundamentais da União Europeia — Artigos 6.º, 7.º, 8.º, 11.º, 47.º e 52.º, n.º 1 — Conservação generalizada e indiferenciada dos dados de ligação e dos dados que permitam identificar os criadores de conteúdos — Recolha de dados de tráfego e de localização — Acesso aos dados»

1. Nos últimos anos o Tribunal de Justiça tem mantido uma linha jurisprudencial constante sobre a conservação e o acesso aos dados pessoais, da qual se destacam:

— O Acórdão de 8 de abril de 2014, Digital Rights Ireland e outros[2], que declarou a invalidade da Diretiva 2006/24/CE[3] por permitir uma ingerência desproporcionada nos direitos reconhecidos pelos artigos 7.º e 8.º da Carta de Direitos Fundamentais da União Europeia (a seguir «Carta»).

— O Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e outros[4], que interpretou o artigo 15.º, n.º 1, da Diretiva 2002/58/CE[5].

— O Acórdão de 2 de outubro de 2018, Ministerio Fiscal[6], que confirmou a interpretação desse mesmo artigo 15.º, n.º 1, da Diretiva 2002/58/CE.

1 Língua original: espanhol.

2 Processos C-293/12 e C-594/12, a seguir, «Acórdão Digital Rights», EU:C:2014:238.

3 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).

4 Processos C-203/15 e C-698/15, a seguir, «Acórdão Tele2 Sverige e Watson», EU:C:2016:970.

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).

6 Processo C-207/16, a seguir, «Acórdão Ministerio Fiscal», EU:C:2018:788.

2. Esses acórdãos (em particular, o segundo) causaram alguma preocupação às autoridades de alguns Estados-Membros, pois, no seu entender, têm como consequência despojá-las de um instrumento que reputam necessário para a salvaguarda da segurança nacional e para a luta contra a criminalidade e o terrorismo. Daí que alguns desses Estados-Membros advoguem pela revogação ou clarificação dessa jurisprudência.

3. Alguns órgãos jurisdicionais dos Estados-Membros manifestaram essa mesma preocupação em quatro reenvios prejudiciais [7], sobre os quais versam as minhas conclusões da presente data.

4. Os quatro processos suscitam principalmente o problema da aplicação da Diretiva 2002/58 a atividades relacionadas com a segurança nacional e com o combate ao terrorismo. Se essa Diretiva for aplicável aplicar neste contexto, devemos esclarecer de seguida em que medida podem os Estados-Membros restringir os direitos de privacidade que protege. Por último, devemos analisar até que ponto os diferentes legislações nacionais (britânica [8], belga [9] e francesa [10]) sobre esta matéria se coadunam com o direito da União, tal como interpretado pelo Tribunal de Justiça.

I. QUADRO NORMATIVO

A. Direito da União

1. Diretiva 2002/58

5. De acordo com o disposto no artigo 1.º («Âmbito e objetivos»):

«1. A presente diretiva harmoniza as disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, 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 Comunidade.

[…]

3. A presente diretiva não é aplicável a atividades fora do âmbito do Tratado que institui a Comunidade Europeia, tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia, 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.»

6. O artigo 3.º («Serviços abrangidos») dispõe que:

«A presente diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas publicamente disponíveis nas redes públicas de comunicações da Comunidade.»

7 Para além destes (processos C-511/18 e C-512/18), os processos C-623/17, Privacy International, e C-520/18, Ordre des barreaux francophones et germanophone e outros.

8 Pocesso Privacy International, C-623/17.

9 Processo Ordre des barreaux francophones et germanophone e o., C-520/18.

10 Processos La Quadrature du Net e o., C-511/18 e C-512/18

7. O n.º 1 do artigo 5.º («Confidencialidade das comunicações») dispõe que:

«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 O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.»

8. O artigo 6.º («Dados de tráfego») preceitua:

«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.»

9. O artigo 15.º («Aplicação de determinadas disposições da Diretiva 95/46/CE [11]»), n.º 1, refere que:

«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».

2. Diretiva 2000/31/CE [12]

10. Dispõe o artigo 14.º que:

«1. Em caso de prestação de um serviço da sociedade da informação que consista no armazenamento de informações prestadas por um destinatário do serviço, os Estados-Membros velarão por que a responsabilidade do prestador do serviço não possa ser invocada no que respeita à informação armazenada a pedido de um destinatário do serviço, desde que:

[…]

11 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).

12 Diretiva do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (Diretiva sobre comércio eletrónico) (JO 2000, L 178, p. 1).

3. O disposto no presente artigo não afeta a faculdade de um tribunal ou autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exigir do prestador que previna ou ponha termo a uma infração, nem afeta a faculdade de os Estados-Membros estabelecerem disposições para a remoção ou impossibilitação do acesso à informação».

11. Nos termos do artigo 15.º:

«1. Os Estados-Membros não imporão aos prestadores, para o fornecimento dos serviços mencionados nos artigos 12.º, 13.º e 14.º, uma obrigação geral de vigilância sobre as informações que estes transmitam ou armazenem, ou uma obrigação geral de procurar ativamente factos ou circunstâncias que indiciem ilicitudes.

2. Os Estados-Membros podem estabelecer a obrigação, relativamente aos prestadores de serviços da sociedade da informação, de que informem prontamente as autoridades públicas competentes sobre as atividades empreendidas ou informações ilícitas prestadas pelos autores aos destinatários dos serviços por eles prestados, bem como a obrigação de comunicar às autoridades competentes, a pedido destas, informações que permitam a identificação dos destinatários dos serviços com quem possuam acordos de armazenagem».

3. Regulamento (UE) 2016/679[13]

12. Nos termos do artigo 2.º («Âmbito de aplicação material»):

«1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

2. O presente regulamento não se aplica ao tratamento de dados pessoais:

a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;

b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE;

c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;

d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

[…]»

13 Regulamento do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados) (JO 2016, L 119, p. 1).

13. Nos termos do n.º 1 do artigo 23.º («Limitações»):

«O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:

a) A segurança do Estado;

b) A defesa;

c) A segurança pública;

d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;

e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social;

f) A defesa da independência judiciária e dos processos judiciais;

g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas;

h) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas a) a e) e g);

i) A defesa do titular dos dados ou dos direitos e liberdades de outrem;

j) A execução de ações cíveis.»

14. O artigo 95.º («Relação com a Diretiva 2002/58/CE») dispõe o seguinte:

«O presente regulamento não impõe obrigações suplementares a pessoas singulares ou coletivas no que respeita ao tratamento no contexto da prestação de serviços de comunicações eletrónicas disponíveis nas redes públicas de comunicações na União em matérias que estejam sujeitas a obrigações específicas com o mesmo objetivo estabelecidas na Diretiva 2002/58/CE.»

B. Direito nacional

1. Code de la sécurité intérieure (Código da Segurança Interna)

15. De acordo com o disposto no artigo L. 851-1:

«Nas condições previstas no capítulo 1 do título II do presente livro, pode ser autorizada, junto dos operadores de comunicações eletrónicas e das pessoas mencionadas no artigo L. 34-1 do code des postes et des communications électroniques [(Código dos Correios e das Comunicações Eletrónicas)], bem como das pessoas mencionadas nos pontos 1 e 2 da parte I do artigo 6.º, da loi n.º 2004-575 […]

pour la confiance dans l'économie numérique [(Lei n.º 2004-575 […], para a Confiança na Economia Digital)], a recolha das informações ou documentos tratados ou conservados pelos respetivos serviços ou redes de comunicações eletrónicas, incluindo os dados técnicos relativos à identificação dos números de assinatura ou de ligação a serviços de comunicações eletrónicas, ao recenseamento de todos os números de assinatura ou de ligação de uma pessoa designada, à localização dos equipamentos terminais e às comunicações de um assinante referentes à lista dos números das chamadas recebidas e efetuadas, duração e data das comunicações […]».

16. Os artigos L. 851-2 e L. 851-4 regulamentam, para diferentes fins e segundo diferentes modalidades, o acesso administrativo em tempo real aos dados de ligação assim conservados.

17. O artigo L. 851-2 autoriza, exclusivamente para efeitos de prevenção do terrorismo, a recolha da informação ou dos documentos previstos no artigo L. 851-1, junto das mesmas pessoas. Esta recolha, que se aplica apenas a um ou mais indivíduos previamente identificados como suscetíveis de estar ligados a uma ameaça terrorista, é realizada em tempo real. O mesmo acontece com as disposições do artigo L. 851-4 do mesmo código, que autorizam a transmissão em tempo real pelos operadores apenas dos dados técnicos relativos à localização dos equipamentos terminais [14].

18. O artigo L. 851-3 permite impor aos operadores de comunicações eletrónicas e aos prestadores de serviços técnicos a obrigação de «aplicação nas suas redes de tratamentos automatizados destinados, em função de parâmetros especificados na autorização, a detetar ligações suscetíveis de revelar uma ameaça terrorista» [15].

19. O artigo L. 851-5 dispõe que, em determinadas condições, «pode ser utilizado um dispositivo técnico que permita a localização em tempo real de uma pessoa, de um veículo ou de um objeto».

20. Nos termos do n.ºI do artigo L. 851-6, é possível, em certas condições, «recolher […] diretamente, através de um aparelho ou de um dos dispositivos técnicos enumerados no n.º 1 do artigo 226-3 do code pénal [(Código Penal)], os dados técnicos de ligação que permitam a identificação de um equipamento terminal ou do número de assinante do seu utilizador, bem como os dados relativos à localização dos equipamentos terminais utilizados».

2. Código dos Correios e das Comunicações Eletrónicas

21. De acordo com o disposto no artigo L. 34-1, na versão aplicável aos factos:

«I. O presente artigo aplica-se ao tratamento de dados pessoais na prestação de serviços de comunicações eletrónicas ao público, aplicando-se, em particular, às redes que albergam os dispositivos de recolha de dados e de identificação.

II. Os operadores de comunicações eletrónicas e, em especial, as pessoas cuja atividade consiste em oferecer acesso a serviços de comunicação ao público em linha, devem eliminar ou anonimizar todos os dados de tráfego, sem prejuízo do disposto nos pontos III, IV, V e VI.

Quem prestar serviços de comunicações eletrónicas ao público deve instituir, em observância do indicado no ponto anterior, procedimentos internos para dar resposta aos pedidos das autoridades competentes.

14 Segundo o órgão jurisdicional de reenvio, estas técnicas não criam para os prestadores de serviços uma obrigação de conservação suplementar relativamente à necessária para a faturação e para a comercialização dos seus serviços, e para a prestação de serviços de valor acrescentado.

15 Segundo o órgão jurisdicional de reenvio, esta técnica, que não implica uma conservação generalizada e indiferenciada, visa apenas a recolha, durante um tempo limitado, de entre todos os dados de ligação tratados por essas pessoas, dos que possam estar relacionados com uma infração grave desse tipo.

Nos termos do presente artigo quem, em razão de uma atividade profissional principal ou acessória, oferecer ao público uma ligação que permita uma comunicação em linha através de um acesso à rede, ainda que de forma gratuita, fica obrigado ao cumprimento das disposições aplicáveis aos operadores de comunicações eletrónicas nos termos do presente artigo.

III. Para efeitos de investigação, deteção e perseguição de crimes ou do incumprimento da obrigação definida no artigo L. 336-3 do code de la propriété intellectuelle [(Código da Propriedade Intelectual)] ou para efeitos de prevenção de ataques aos sistemas de tratamento automatizado de dados previstos e punidos pelos artigos 323-1 a 323-3-1 do Código Penal, e com o único objetivo de permitir, se necessário, a colocação à disposição da autoridade judicial ou da alta autoridade mencionada no artigo L. 331-12 do Código da Propriedade Intelectual ou da autoridade nacional de segurança dos sistemas de informação mencionada no artigo L. 2321-1 du code de la défense [(Código da Defesa)], as operações dirigidas a eliminar ou a anonimizar determinadas categorias de dados técnicos poderão ser adiadas por um período máximo de um ano. Por decreto consultado ao do Conseil d'État [(Conselho de Estado, em formação jurisdicional)], adotado após o parecer da Commission nationale de l'informatique et des libertés [(Comissão Nacional de Informática e Liberdades)], deverão ser especificadas, dentro dos limites previstos no ponto VI, essas categorias de dados e a duração da sua conservação, em função da atividade dos operadores e da natureza das comunicações, bem como as modalidades de indemnização, se for caso disso, dos custos adicionais identificáveis e específicos das prestações garantidas a esse título pelos operadores, por solicitação do Estado.

[…]

VI. Os dados conservados e tratados nas condições definidas nos pontos III, IV e V serão relativos exclusivamente à identificação dos utilizadores dos serviços fornecidos pelos operadores, às características técnicas das comunicações disponibilizadas por estes últimos e à localização dos equipamentos terminais.

Não podem em caso algum ser relativos ao conteúdo da correspondência trocada ou às informações consultadas no âmbito dessas comunicações, independentemente da forma.

A conservação e o tratamento dos dados realizam-se com respeito pelas disposições da Lei n.º 78-17 de 6 de janeiro de 1978 relativa à informática, aos ficheiros e às liberdades.

Os operadores adotarão as medidas necessárias para impedir a utilização desses dados para fins distintos dos previstos no presente artigo».

22. Nos termos do artigo R. 10-13, n.ºI, os operadores devem conservar, para fins de investigação, de deteção e de perseguição das infrações penais, os seguintes dados:

«a) As informações que permitam identificar o utilizador;

b) Os dados relativos aos equipamentos terminais de comunicações utilizados;

c) As características técnicas, bem como a data, hora e duração de cada comunicação;

d) Os dados relativos aos serviços adicionais pedidos ou utilizados e os seus fornecedores;

e) Os dados que permitam identificar o ou os destinatários da comunicação».

23. De acordo com o ponto II do mesmo preceito, no caso das atividades de telefonia o operador deve conservar também os dados que permitam a identificação da origem e da localização da comunicação.

24. Nos termos do ponto III do mesmo artigo, os dados acima referidos devem ser conservados durante um ano, a partir do dia do seu registo.

3. Loi n.º°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Lei n.º° 2004-575 de 21 de junho de 2004 para a confiança na economia digital)

25. O parágrafo primeiro do ponto II do artigo 6.º da Lei 2004-575 estabelece que as pessoas cuja atividade consista em oferecer acesso a serviços em linha de comunicação ao público e as pessoas singulares ou coletivas que armazenem, incluindo a título gratuito, para colocação à disposição do público mediante serviços de comunicação ao público em linha, sinais, textos, imagens, sons ou mensagens de qualquer natureza proporcionados pelos destinatários destes serviços, «manterão e conservarão os dados de forma que permita a identificação de quem tenha contribuído para a criação do conteúdo ou de algum dos conteúdos dos serviços de que são prestadores».

26. O parágrafo terceiro do ponto II do mesmo preceito refere que a autoridade judicial poderá solicitar a essas pessoas que comuniquem os dados mencionados no parágrafo primeiro.

27. Segundo o último parágrafo do ponto II, por decreto do Conseil d'État (Conselho de Estado, em formação jurisdicional) «serão definidos os dados mencionados no parágrafo primeiro e será determinada a duração e as modalidades da sua conservação». [16]

II. Factos do litígio e questões prejudiciais submetidas

A. Processo C-511/18

28. A Quadrature du Net, a French Data Network, a Igwan.net e a Fédération des fournisseurs d'accès à internet associatifs (a seguir, «recorrentes») pediram ao Conseil d'État (Conselho de Estado, em formação jurisdicional) a anulação de vários decretos de desenvolvimento de algumas disposições do Código da Segurança Interna [17].

16 A definição foi feita pelo décret n.º 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Decreto n.º 2011-219, de 25 de fevereiro de 2011, sobre a conservação dos dados que permitem a identificação de qualquer pessoa que tenha contribuído para a criação de um conteúdo oferecido em linha). Desse decreto podem destacar-se: a) O artigo 1.º, n.º 1, nos termos do qual, quem proporcione o acesso a serviços de comunicação em linha deve conservar os seguintes dados: o identificador da ligação, o identificador atribuído ao assinante, o identificador do terminal utilizado para a ligação, a data e a hora do início e do fim da ligação, as características da linha do assinante; b) De acordo com o disposto no n.º 2 do artigo 1.º, quem armazenar, incluindo a título gratuito, para colocação à disposição do público mediante serviços de comunicação ao público em linha, sinais, textos, imagens, sons ou mensagens de qualquer natureza proporcionados pelos destinatários destes serviços, deve conservar, para cada operação, os seguintes dados: o identificador da ligação na origem da comunicação, o identificador atribuído ao conteúdo objeto da operação, os tipos de protocolos utilizados para a ligação ao serviço e para a transferência de conteúdos, a natureza da operação, a data e a hora da operação e o identificador utilizado pelo autor da operação; e c) Por fim, o n.º 3 do artigo 1.º preceitua que as pessoas mencionadas nos dois números anteriores devem conservar as seguintes informações disponibilizadas por um utilizador ao subscrever um contrato ou criar uma conta: o identificador da ligação ao criar a conta; nome, apelidos ou razão social; os endereços postais associados, os pseudónimos utilizados, as direções de correio eletrónico ou de contas associadas, os números de telefone, a palavra passe atualizada e os dados que permitam a sua confirmação ou alteração.

17 Os decretos impugnados eram os seguintes: a) décret n.º 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (Decreto n.º 2015-1185, de 28 de setembro de 2015, que designa os serviços especializados de informação); b) décret n.º 2015 -1211 du 1er octubre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (Decreto n.º 2015-1211, de 1 de outubro de 2015, relativo ao contencioso da aplicação das técnicas de informação sujeitas a autorização e dos ficheiros relevantes para a segurança do Estado); c) décret n.º 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du libre VIII du code de la sécurité intérieure (Decreto n.º 2015-1639, de 11 de dezembro de 2015, relativo à designação dos serviços autorizados a recorrer às técnicas referidas no título V do livro VIII do Código da Segurança Interna); e d) décret n.º 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Decreto n.º 2016-67, de 29 de janeiro de 2016, relativo às técnicas de recolha de informação).

29. Os recorrentes sustentam, em síntese, que tanto os decretos impugnados como essas disposições do Código da Segurança Interna violam os direitos ao respeito pela vida privada, à proteção de dados pessoais e à ação efetiva, garantidos, respetivamente, pelos artigos 7.º, 8.º e 47.º da Carta.

30. Nessa linha, o Conseil d'État (Conselho de Estado, em formação jurisdicional) submete ao Tribunal de Justiça as seguintes questões:

«1) Num contexto marcado por ameaças graves e persistentes para a segurança nacional, e em especial pelo risco terrorista, deve a obrigação de conservação generalizada e indiferenciada, imposta aos prestadores de serviços com fundamento nas disposições permissivas do artigo 15.º, n.º 1, da Diretiva 2002/58 […], ser considerada uma ingerência justificada pelo direito das pessoas à segurança, garantido pelo artigo 6.º da Carta […] e pelas exigências de segurança nacional, cuja responsabilidade incumbe unicamente aos Estados-Membros por força do artigo 4.º [TUE]?

2) Deve a Diretiva 2002/58 […], lida à luz da Carta […], ser interpretada no sentido de que autoriza medidas legislativas, tais como as medidas de recolha em tempo real dos dados relativos ao tráfego e à localização de indivíduos específicos, que, embora afetando os direitos e obrigações dos prestadores de serviços de comunicações eletrónicas, não lhes impõem no entanto uma obrigação específica de conservação dos seus dados?

3) Deve a Diretiva 2002/58 […], lida à luz da Carta […], ser interpretada no sentido de que sujeita, em todos os casos, a regularidade dos procedimentos de recolha dos dados de ligação à exigência de informação das pessoas afetadas quando tal informação já não possa comprometer as investigações levadas a cabo pelas autoridades competentes, ou podem tais procedimentos ser considerados regulares tendo em conta o conjunto das outras garantias processuais existentes, desde que estas últimas garantam a efetividade do direito de recurso?»

B. Processo C-512/18

31. Os recorrentes, no litígio que originou o processo C-511/18, com exceção da Igwan.net, pediram também ao Conseil d'État (Conselho de Estado, em formação jurisdicional) que anulasse o indeferimento (tácito) do seu pedido de revogação do artigo R. 10-13 do code des postes et des communications électroniques (Código dos Correios e das Comunicações Eletrónicas) e do Decreto n.º 2011-219 de 25 de fevereiro de 2011.

32. No entender desses recorrentes, as normas impugnadas impõem uma obrigação de conservação de dados de tráfego, de localização e de ligação que, pelo seu caráter geral, constituem um atentado desproporcionado aos direitos ao respeito pela vida privada e familiar, à proteção de dados de caráter pessoal e à liberdade de expressão, protegidos pelos artigos 7.º, 8.º e 11.º da Carta, e violam o artigo 15.º, n.º 1, da Diretiva 2002/58.

33. Nesse recurso, o Conseil d'État (Conselho de Estado, em formação jurisdicional) formulou a seguinte questão prejudicial:

«1) Tendo em conta nomeadamente as garantias e os controlos associados à recolha e à utilização dos dados de ligação, deve a obrigação de conservação generalizada e indiferenciada, imposta aos fornecedores com fundamento nas disposições permissivas do artigo 15.º, n.º 1, da Diretiva [2002/58/CE] ser considerada uma ingerência justificada pelo direito das pessoas à segurança, garantido pelo artigo 6.º da Carta […] e pelas exigências de segurança nacional, cuja responsabilidade incumbe unicamente aos Estados-Membros por força do artigo 4.º do [TUE]?

2) Devem as disposições da Diretiva [2000/31], lidas à luz dos artigos 6.º, 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta […] ser interpretadas no sentido de que permitem a um Estado-Membro instituir uma regulamentação nacional que impõe às pessoas cuja atividade consiste em proporcionar acesso a serviços em linha de comunicação com o público e às pessoas singulares ou coletivas que asseguram, mesmo a título gratuito, para a colocação à disposição do público através de serviços de comunicação ao público em linha, o armazenamento de sinais, textos, imagens, sons, ou mensagens de qualquer natureza fornecidos por destinatários desses serviços, a conservação dos dados suscetíveis de permitir a identificação de qualquer pessoa que tenha contribuído para a criação de conteúdos ou de um dos conteúdos dos serviços que prestam, a fim de que a autoridade judiciária possa, sendo caso disso, pedir a sua comunicação para fazer respeitar as regras relativas à responsabilidade civil ou penal?»

III. Processo no Tribunal de Justiça e posições das partes

34. As questões prejudiciais deram entrada no Tribunal de Justiça em 3 de agosto de 2018.

35. Além da Comissão, depositaram observações escritas a Quadrature du Net, a Fédération des fournisseurs d'accès à Internet associatifs, a French Data Network, os Governos alemão, belga, britânico, checo, cipriota, dinamarquês, espanhol, estónio, francês, húngaro, irlandês, polaco e sueco e ainda a Comissão.

36. Em 9 de setembro de 2019 foi celebrada audiência, em conjunto com a dos processos C-623/17, Privacy International, e C-520/18, Ordre des barreaux francophones et germanophone e o., no qual compareceram as partes dos quatro reenvios prejudiciais, os governos acima referidos, bem como os Governos dos Países Baixos e da Noruega, e ainda a Comissão e a Autoridade Europeia para a Proteção de Dados Pessoais.

IV. Apreciação

37. As questões submetidas pelo Conseil d'État (Conselho de Estado, em formação jurisdicional) podem ser agrupadas em três:

— Em primeiro lugar, saber se é compatível com o direito da União uma legislação nacional que imponha aos prestadores de serviços de comunicações eletrónicas a obrigação de conservarem de forma generalizada e indiferenciada os dados de ligação (primeira questão no processo C-511/18 e no processo C-512/18) e, em particular, os dados que permitam identificar os criadores dos conteúdos oferecidos pelos referidos prestadores (segunda questão no processo C-512/18).

— Em segundo lugar, saber se a licitude do processo de recolha de dados de ligação fica, em qualquer caso, dependente da obrigação de informar as pessoas afetadas, desde que não se ponham em perigo as investigações (terceira questão no processo C-511/18).

— Em terceiro lugar, saber se a recolha em tempo real de dados de tráfego e de localização, sem obrigação de os conservar, é compatível —e em que condições — com a Diretiva 2002/58 (segunda questão no processo C-511/18).

38. Trata-se de determinar, em concreto, se é compatível com o direito da União uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas dois tipos de obrigações: a) por um lado, a *recolha* de determinados dados, mas não a sua conservação; b) por outro lado, a *conservação* dos dados de ligação e dos dados que permitam a identificação dos criadores dos conteúdos dos serviços prestados pelos referidos prestadores.

39. Há que decidir primeiro se, precisamente tendo em conta o contexto [18] em que essa legislação nacional foi adotada (isto é, em circunstâncias em que pode estar comprometida a segurança nacional), é aplicável a Diretiva 2002/58.

A. Sobre a aplicabilidade da Diretiva 2002/58

40. O órgão jurisdicional de reenvio dá por assente que a legislação objeto do litígio se enquadra no âmbito de aplicação da Diretiva 2002/58. No seu entender, é o que resulta da jurisprudência fixada pelo acórdão Tele2 Sverige e Watson e corroborada pelo Acórdão Ministerio Fiscal.

41. Pelo contrário, alguns dos governos que intervieram no processo afirmam que a legislação controvertida não se enquadra no âmbito da referida diretiva. Para defender a sua posição, chamam à colação, entre outros argumentos, o Acórdão de 30 de maio de 2006, Parlamento/Conselho e Comissão [19].

42. Concordo com o Conseil d'État (Conselho de Estado, em formação jurisdicional) quanto ao facto de o Acórdão Tele2 Sverige e Watson ter encerrado esta parte do debate, confirmando que a Diretiva 2002/58 é aplicável, em princípio, quando os prestadores de serviços eletrónicos sejam legalmente obrigados a conservar os dados dos seus assinantes e a permitir que as autoridades públicas acedam aos mesmos. Esta tese não é alterada pelo facto de as obrigações serem impostas aos prestadores por razões de segurança nacional.

43. Adianto desde já que, caso existisse alguma divergência entre o Acórdão Tele2 Sverige e Watson e os anteriores, deveria prevalecer aquele, por ser posterior e por ter sido confirmado pelo Acórdão Ministerio Fiscal. Não obstante, julgo que não existe essa divergência, conforme explicarei mais à frente.

1. Acórdão Parlamento/Conselho e Comissão

44. Os processos decididos pelo Acórdão Parlamento/Conselho e Comissão versavam sobre:

— O Acordo entre a Comunidade Europeia e os Estados Unidos da América sobre o tratamento e a transferência dos PNR [Passenger Name Records (dados de identificação dos passageiros de transporte aéreo)] por parte das companhias aéreas para as autoridades dos Estados Unidos [20].

— O caráter adequado da proteção dos dados pessoais contidos nos registos dos nomes dos passageiros, transferidos para as referidas autoridades. [21]

45. O Tribunal de Justiça concluiu que a transferência desses dados era um tratamento que tinha por objeto a segurança pública e as atividades do Estado em matéria penal. De acordo com o artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, as duas decisões controvertidas não se enquadravam no âmbito de aplicação da Diretiva 95/46.

18 «Um contexto […] [de] ameaças graves e persistentes para a segurança nacional, nomeadamente, de risco terrorista», conforme descrito na primeira questão do processo C-511/18.

19 Processos C-317/04 e C-318/04, a seguir «Acórdão Parlamento/Conselho e Comissão», EU:C:2006:346.

20 Decisão 2004/496/CE do Conselho, de 17 de maio de 2004, relativa à celebração de um acordo entre a Comunidade Europeia e os Estados Unidos da América sobre o tratamento e a transferência de dados contidos nos registos de identificação dos passageiros (PNR) por parte das transportadoras aéreas para o Serviço das Alfândegas e Proteção das Fronteiras do Departamento de Segurança Interna dos Estados Unidos (JO 2004, L 183, p. 83, retificado pelo JO 2005, L 255, p. 168) (processo C-317/04).

21 Decisão 2004/535/CE da Comissão, de 14 de maio de 2004, sobre o nível de proteção adequado dos dados pessoais contidos nos Passenger Name Record transferidos para o Bureau of Customs and Border Protection dos Estados Unidos (JO 2004, L 235, p. 11) (processo C-318/04).

46. Os dados eram inicialmente recolhidos pelas companhias aéreas no quadro de uma atividade —a venda de bilhetes— pertencente à esfera de aplicação do direito da União. Não obstante, o seu tratamento, tal como referido na decisão controvertida, «não visa um tratamento de dados necessário para a realização de uma prestação de serviços, mas [antes] considerado necessário para salvaguardar a segurança pública e para fins repressivos» [22].

47. O Tribunal de Justiça adotou, desta forma, uma abordagem teleológica, atendendo à finalidade prosseguida com o tratamento dos dados: visando-se com o mesmo a proteção da segurança pública, devia considerar-se fora do âmbito de aplicação da Diretiva 95/46. No entanto, essa finalidade não era o único critério determinante [23], pelo que o Acórdão sublinhou que «[se] integra[…] num quadro instituído pelos poderes públicos e que tem em vista a segurança pública» [24].

48. O Acórdão Parlamento/Conselho e Comissão permite, pois, analisar a diferença entre a cláusula de exclusão e as cláusulas de restrição ou limitação previstas na Diretiva 95/46 (análogas às da Diretiva 2002/58). É certo, porém, que umas e outras se referem a objetivos de interesse geral semelhantes, o que gera alguma confusão a respeito do respetivo alcance, como assinalava na altura o advogado geral Y. Bot [25].

49. É provável que esta confusão esteja na origem da tese defendida pelos Estados-Membros que advogam pela inaplicabilidade da Diretiva 2002/58 neste contexto. No seu entender, o interesse da segurança nacional apenas é salvaguardado através da exclusão prevista no artigo 1.º, n.º 3, da Diretiva 2002/58. O certo é que, não obstante, também servem esse mesmo interesse as limitações autorizadas pelo artigo 15.º, n.º 1, da referida Diretiva, entre elas a relativa à segurança nacional. Este último preceito seria supérfluo se a Diretiva 2002/58 fosse inaplicável face a qualquer invocação da segurança nacional.

2. 2. Acórdão Tele2 Sverige e Watson

50. No Acórdão Tele2 Sverige e Watson debateu-se a compatibilidade entre o direito da União e alguns regimes jurídicos nacionais que impunham aos fornecedores de serviços de comunicação eletrónica acessíveis ao público uma obrigação geral de conservar os dados relativos às referidas comunicações. Os casos eram, portanto, substancialmente idênticos aos que se discutem nestes reenvios prejudiciais.

22 Acórdão Parlamento/Conselho e Comissão, n.º 57. No n.º 58 insiste-se em que o «facto de os dados […] terem sido recolhidos por operadores privados para fins comerciais e de serem eles a organizar a sua transferência para um Estado terceiro» não implica que essa transferência não integre um dos casos de não aplicação da Diretiva 95/46 enumerados no seu artigo 3.º, n.º 2, primeiro travessão, pois «essa transferência integra-se num quadro instituído pelos poderes públicos e que tem em vista a segurança pública».

23 Assim o salientava, em momento posterior, o saudoso advogado-geral Y. Bot nas suas Conclusões do processo Irlanda/Parlamento e Conselho (C-301/06, EU:C:2008:558). Afirmava que o Acórdão Parlamento/Conselho e Comissão «não pode […] ser entendido no sentido de que só o exame da finalidade prosseguida por um tratamento de dados pessoais é relevante para incluir ou excluir um tal tratamento do campo de aplicação do sistema de proteção dos dados criado pela Diretiva 95/46. Importa também verificar no quadro de que tipo de atividades se efetua um tratamento de dados. Só no caso [de esse] tratamento ser efetuado no exercício de atividades próprias dos Estados ou das autoridades estatais e alheias aos domínios de atividade dos particulares é que se encontra excluído do sistema comunitário de proteção dos dados pessoais que resulta da Diretiva 95/46, e isto nos termos do artigo 3.º, n.º 2, primeiro travessão, desta Diretiva» (n.º 122).

24 Acórdão Parlamento/Conselho e Comissão, n.º 58. O Acordo tinha por objeto principal exigir às companhias aéreas com serviços de transporte de passageiros entre a União e os Estados Unidos que permitissem às autoridades norte-americanas um acesso eletrónico aos dados PNR dos registos dos nomes de passageiros constantes nos seus sistemas informáticos de controlo de reservas e de saídas. Instituía, pois, uma forma de cooperação internacional entre a União e os Estados Unidos para lutar contra o terrorismo e outros crimes graves, tentando conciliar esse objetivo com o da proteção dos dados pessoais dos passageiros. Nesse contexto, a obrigação imposta às companhias não era muito distinta de um intercâmbio direto de dados entre autoridades públicas.

25 Conclusões do advogado-geral Y. Bot no processo Irlanda/Parlamento e Conselho (C-301/06, EU:C:2008:558), n.º 127.

51. Suscitada de novo a questão da aplicabilidade do direito da União —agora já com a cobertura da Diretiva 2002/58—, o Tribunal de Justiça começou por salientar que «a apreciação do alcance do âmbito de aplicação da Diretiva 2002/58 deve ter em conta, nomeadamente, a economia geral desta» [26].

52. Nesta perspetiva, o Tribunal de Justiça assinalou que «[é] certo que as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 dizem respeito a atividades próprias dos Estados ou das autoridades estatais, alheias aos domínios de atividade dos particulares […] Além disso, as finalidades a que, nos termos desta disposição, essas medidas devem responder, no caso em apreço a salvaguarda da segurança nacional […], coincidem substancialmente com as finalidades prosseguidas pelas atividades referidas no artigo 1.º, n.º 3, desta diretiva» [27].

53. Assim, a finalidade das medidas que, de acordo com o artigo 15.º, n.º 1, da Diretiva 2002/58, os Estados-Membros podem adotar para limitar o direito à privacidade coincide (nesse ponto) com a que justifica excluir certas atividades estatais do regime da diretiva, nos termos do seu artigo 1.º, n.º 3.

54. Não obstante, o Tribunal de Justiça entendeu que, «atendendo à economia geral da Diretiva 2002/58», isso não permitia «concluir que as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 estão excluídas do âmbito de aplicação desta diretiva, sob pena de privarem esta disposição de efeito útil. Com efeito, a referida disposição pressupõe necessariamente que as medidas nacionais aí mencionadas […] se enquadram no âmbito de aplicação desta mesma diretiva, uma vez que esta última só autoriza expressamente que os Estados-Membros as adotem desde que respeitadas as condições que prevê» [28].

55. A isto acresce que as limitações autorizadas pelo artigo 15.º, n.º 1, da Diretiva 2002/58 «regulam, para os efeitos mencionados nesta disposição, a atividade dos prestadores de serviços de comunicações eletrónicas». Por conseguinte, este artigo 15.º, n.º 1, lido em conjugação com o artigo 3.º da referida diretiva, «deve ser interpretado no sentido de que tais medidas legislativas estão abrangidas pelo âmbito de aplicação desta mesma diretiva» [29].

56. Por conseguinte, o Tribunal de Justiça sustentou que se integram no âmbito de aplicação da Diretiva 2002/58 tanto uma medida legislativa que imponha a esses prestadores «a conservação dos dados de tráfego e dos dados de localização, uma vez que tal atividade implica necessariamente, da parte destes, o tratamento de dados pessoais» [30], como uma que regule o acesso das autoridades aos dados conservados por esses prestadores [31].

57. A interpretação dada à Diretiva 2002/58 pelo Tribunal de Justiça no Acórdão Tele2 Sverige e Watson é reiterada no Acórdão Ministerio Fiscal.

58. Poderia afirmar-se que o Acórdão Tele2 Sverige e Watson representa uma inversão, mais ou menos implícita, relativamente à jurisprudência assente no Acórdão Parlamento/Conselho e Comissão? Assim entende, por exemplo, o Governo da Irlanda, para quem apenas este último seria compatível com os fundamentos jurídicos da Diretiva 2002/58 e conforme com o artigo 4.º, n.º 2, TUE [32].

26 Acórdão Tele2 Sverige e Watson, n.º 67.

27 *Ibidem*, n.º 72.

28 *Ibidem*, n.º 73.

29 *Ibidem*, n.º 74.

30 *Ibidem*, n.º 75.

31 *Ibidem*, n.º 76.

32 N.ºs 15 e 16 das observações escritas do Governo irlandês.

59. Por seu lado, o Governo francês, entende que poderá não existir contradição se se tiver em conta que a jurisprudência do Acórdão Tele2 Sverige e Watson alude a atividades dos Estados-Membros no âmbito do direito penal, enquanto a fixada no Acórdão Parlamento/Conselho e Comissão tem que ver com a segurança do Estado e a defesa. Assim, a jurisprudência do Acórdão Tele2 Sverige e Watson não seria aplicável ao caso em apreço, no qual se deveria continuar na solução adotada no Acórdão Parlamento/Conselho e Comissão [33].

60. Como já adiantei, creio que se pode encontrar uma via de integração entre ambos os acórdãos, distinta da defendida pelo Governo francês. Não partilho desta última, pois, na minha opinião as considerações do Acórdão Tele2 Sverige e Watson reportadas explicitamente à luta contra o terrorismo [34], são extensíveis a qualquer outra ameaça contra a segurança nacional (das quais o terrorismo é uma mais).

3. 3. Possibilidade de uma interpretação integradora do Acórdão Parlamento/Conselho e Comissão com o Acórdão Tele2 Sverige e Watson

61. Na minha opinião, nos Acórdãos Tele2 Sverige e Watson e Ministerio Fiscal, o Tribunal de Justiça teve em conta a razão de ser das cláusulas de exclusão e de restrição, bem como a relação sistemática entre os dois tipos de cláusulas.

62. Se no processo Parlamento/Conselho e Comissão o Tribunal de Justiça decidiu que o tratamento dos dados era alheio ao âmbito da Diretiva 95/46, deveu-se, como já recordei, a que, no contexto da cooperação entre a União Europeia e os Estados Unidos, num quadro tipicamente internacional, devia prevalecer a dimensão estatal da atividade face ao facto de esse tratamento comportar também uma dimensão comercial ou privada. Uma das questões então debatidas era, precisamente, a do fundamento jurídico adequado para a decisão controvertida.

63. Pelo contrário, no que respeita às medidas nacionais analisadas nos Acórdãos Tele2 Sverige e Watson e Ministerio Fiscal, o Tribunal de Justiça colocou em primeiro plano a dimensão interna do tratamento de dados: o quadro normativo em que este se realizou era exclusivamente nacional, faltando a dimensão externa que caracterizava o objeto do Acórdão Parlamento/Conselho e Comissão.

64. O diferente peso das dimensões internacional e interna (comercial e privada) do tratamento dos dados teve como consequência que, no primeiro caso, se impusesse a cláusula de exclusão do direito da União como mais adequada para a proteção do interesse geral, traduzido na segurança nacional. No segundo, pelo contrário, esse mesmo interesse podia ser assegurado de forma eficaz através da cláusula de limitação prevista no artigo 15.º n.º 1, da Diretiva 2002/58.

65. Poderíamos ainda analisar outra divergência, ligada ao diferente contexto normativo: cada um desses acórdãos incidiu na interpretação de dois preceitos que, pese embora a sua aparência, não são iguais.

66. Com efeito, o Acórdão Parlamento/Conselho e Comissão pronunciou-se sobre a interpretação do artigo 3.º, n.º 2, da Diretiva 95/46, ao passo que o Acórdão Tele2 Sverige e Watson o fez sobre o artigo 1.º, n.º 3, da Diretiva 2002/58. A leitura atenta desses artigos evidencia uma divergência suficiente para sustentar o sentido das decisões do Tribunal de Justiça num e noutro caso.

33 N.ºs 34 a 50 das observações escritas do Governo francês.

34 Acórdão Tele2 Sverige e Watson, n.ºs 103 e 119.

67. De acordo com o artigo 3.º, n.º 2, da Diretiva 95/46, «[a] presente diretiva *não se aplica ao tratamento de dados pessoais* […] efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário […] e, em qualquer caso, *ao tratamento de dados* que tenha por objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse *tratamento* disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal» [35].

68. Por seu lado, de acordo com o seu artigo 1.º, n.º 3, a Diretiva 2002/58 «*não é aplicável a atividades* fora do âmbito do Tratado que institui a Comunidade Europeia […], 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» [36].

69. Enquanto o artigo 3.º n.º 2, da Diretiva 95/46 exclui o *tratamento de dados* que tenha por objeto — no que ao caso interessa — a segurança do Estado, o artigo 1.º, n.º 3, da Diretiva 2002/58 fá-lo relativamente às *atividades* dirigidas a preservar — também no que aqui interessa — a segurança estatal.

70. A diferença não é de somenos importância. A Diretiva 95/46 deixava fora do seu âmbito de aplicação uma atividade (o «tratamento de dados pessoais») que qualquer um pode realizar. Dessa atividade ficavam especificamente excluídos os tratamentos cujo objeto fosse, entre outros, a segurança do Estado. A natureza do *sujeito* que levasse a cabo o tratamento dos dados era irrelevante. A abordagem adotada para a identificação das ações excluídas era, pois, teleológica ou finalista, sem distinção de pessoas quanto aos seus autores.

71. Entende-se assim que, no processo Parlamento/Conselho e Comissão, o Tribunal de Justiça atendesse primeiramente à finalidade prosseguida com o tratamento de dados. Não importava o «facto de os dados PNR […] terem sido recolhidos por operadores privados para fins comerciais e de serem eles a organizar a sua transferência para um Estado terceiro», pois o fundamental era que «essa transferência se integrasse num quadro instituído pelos poderes públicos e que tem em vista a segurança pública» [37].

72. Em contrapartida, «as atividades que têm por objeto a segurança do Estado», alheias ao âmbito de aplicação da Diretiva 2002/58 e analisadas no processo Tele2 Sverige e Watson, não podem abranger um qualquer sujeito, mas apenas o próprio Estado. Além disso, não se integram nelas as funções normativas ou reguladoras do Estado, mas apenas a competência material dos poderes públicos.

73. Com efeito, as *atividades* enumeradas no artigo 1.º, n.º 3, da Diretiva 2002/58 «dizem respeito a atividades próprias dos Estados ou das autoridades estatais, alheias aos domínios de atividade dos particulares» [38]. Considero que essas «atividades» não podem ser de natureza normativa. Se assim fosse, todas as disposições adotadas pelos Estados-Membros relativas ao tratamento de dados pessoais ficavam fora do âmbito da Diretiva 2002/58, à medida que se fossem justificando como necessárias para garantir a segurança do Estado.

74. Por um lado, resultaria numa notável perda de eficácia da Diretiva, pois a mera invocação de um conceito jurídico tão indeterminado como o da segurança nacional seria suficiente para tornar inaplicáveis aos Estados-Membros as salvaguardas concebidas pelo legislador da União para proteger os dados pessoais dos cidadãos. Essa proteção é impraticável sem a participação dos Estados-Membros e, a sua garantia para os cidadãos também é assegurada face aos poderes públicos nacionais.

35 Sublinhado nosso.

36 Sublinhado nosso.

37 Parlamento/Conselho e Comissão, n.º 58.

38 Acórdão Ministerio Fiscal, n.º 32. No mesmo sentido, Acórdão Teje2 Sverige e Watson, n.º 72.

75. Por outro lado, uma interpretação do conceito «atividades estatais» que englobe as que se traduzem na promulgação de normas e disposições jurídicas deixaria sem sentido o artigo 15.º da Diretiva 2002/58, que habilita, precisamente, os Estados-Membros a — por razões de proteção, *inter alia*, da segurança nacional — adotarem «medidas legais» com o propósito de delimitar o alcance de certos direitos e obrigações previstos na mesma Diretiva [39].

76. Como salientou o Tribunal de Justiça no processo Tele2 Sverige e Watson, «a apreciação do alcance do âmbito de aplicação da Diretiva 2002/58 deve ter em conta, nomeadamente, a [sua sistemática]». [40]. Dessa perspetiva, a interpretação do artigo 1.º, n.º 3, e do artigo 15.º, n.º 1, da Diretiva 2002/58 que lhes confere sentido sem perda da sua eficácia é a que identifica, no primeiro de ambos os preceitos, uma exclusão material referida às *atividades* desempenhadas pelos Estados-Membros no âmbito da segurança nacional (e equivalentes) e, no segundo, uma habilitação para estabelecer *medidas legislativas* (isto é, normas com força geral) que, por questões de segurança nacional, afetem as atividades dos indivíduos sujeitos ao *imperium* dos Estados-Membros, restringindo os direitos garantidos pela Diretiva 2002/58.

4. 4. Exclusão da segurança nacional na Diretiva 2002/58

77. A segurança nacional (ou a expressão sinónima, «a segurança do Estado», como salienta o artigo 15.º, n.º 1) é objeto de uma consideração dupla na Diretiva 2002/58. Por um lado, constitui um motivo de exclusão (da aplicação desta diretiva) para todas as atividades dos Estados-Membros que, especificamente, a «tenham por objeto». Por outro, apresenta se como um motivo de limitação, que tem que ser desenvolvido por lei, dos direitos e obrigações estabelecidos na Diretiva 2002/58, ou seja, relativamente a atividades de natureza privada ou comercial e fora do domínio das atividades da autoridade pública [41].

78. A que atividades se refere o artigo 1.º, n.º 3, da Diretiva 2002/58? Em meu entender, o próprio Conseil d'État (Conselho de Estado, em formação jurisdicional) dá um bom exemplo ao mencionar os artigos L. 851 5 e L. 851 6 do Código da Segurança Interna, referindo as «técnicas de recolha de informação diretamente aplicadas pelo Estado sem reger as atividades dos fornecedores de serviços de comunicações eletrónicas mediante a imposição de obrigações específicas» [42].

79. Considero que é este o ponto fundamental para identificar o âmbito de exclusão do artigo 1.º, n.º 3, da Diretiva 2002/58. Não estarão sujeitas ao seu regime as atividades destinadas a preservar a segurança nacional que os poderes públicos realizem por conta própria, sem requererem a colaboração de particulares e, por conseguinte, sem lhes imporem obrigações na sua gestão empresarial.

80. No entanto, o leque de atividades dos poderes públicos isentas do regime geral do tratamento dos dados pessoais deve ser interpretado de forma restritiva. Em concreto, não é possível alargar o conceito de segurança nacional, cuja responsabilidade cabe exclusivamente a cada Estado-Membro por força do artigo 4.º, n.º 2, TUE, a outros setores, mais ou menos próximos, da vida pública.

39 De facto, seria difícil sustentar que o artigo 15.º, n.º 1, da Diretiva 2002/58 permite limitar os direitos e obrigações estabelecidos num âmbito que, como o da segurança nacional, estaria, em princípio fora do seu âmbito de aplicação, em virtude do artigo 1.º, n.º 3, da própria Diretiva. Como afirmou o Tribunal de Justiça no Acórdão Tele2 Sverige e Watson, n.º 73, o artigo 15.º, n.º 1, da Diretiva 2002/58 «pressupõe necessariamente que as medidas nacionais aí mencionadas […] se enquadram no âmbito de aplicação desta mesma diretiva, uma vez que esta última só autoriza expressamente que os Estados-Membros as adotem desde que respeitadas as condições que prevê».

40 Acórdão Tele2 Sverige e Watson, n.º 67.

41 Como observava, de forma incidental, o advogado geral Saugmandsgaard Øe nas suas conclusões no processo Ministerio Fiscal (C-207/16, EU:C:2018:300), ponto 47, «não se deve confundir, por um lado, os dados pessoais tratados *diretamente* no âmbito das atividades —o exercício da autoridade pública— do Estado no domínio do direito penal e, por outro, as questões tratadas no âmbito das atividades —de natureza comercial— de um fornecedor de serviços de comunicações eletrónicas que são *seguidamente* utilizadas pelas autoridades estatais competentes».

42 N.ºs 18 e 21 do auto de reenvio no processo C-511/18.

81. Como nestas questões prejudiciais se verifica o envolvimento de particulares (quer dizer, de quem presta aos utilizadores os serviços de comunicações eletrónicas) e não a mera intervenção das autoridades estatais, não será necessário alargar-me na delimitação dos contornos da segurança nacional *stricto sensu*.

82. Não obstante, considero que pode servir como orientação o critério da Decisão Quadro 2006/960/JAI [43], cujo artigo 2.º, alínea a), estabelece uma distinção entre os serviços de segurança em sentido amplo — os quais incluem «uma autoridade nacional policial, aduaneira ou outra, habilitada pelo direito interno a detetar, prevenir e investigar infrações ou atividades criminosas e a exercer a autoridade e tomar medidas de coação no contexto dessas funções»—, por um lado, e os «serviços ou unidades que se dediquem especificamente a questões de segurança nacional», por outro [44].

83. No considerando décimo primeiro da Diretiva 2002/58 afirma-se que esta, «tal como a Diretiva 95/46 […], não trata questões relativas à proteção dos direitos e liberdades fundamentais relacionadas com atividades não reguladas pelo direito [da União]». Por isso, a Diretiva 2002/58 «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 da presente diretiva, necessárias para a proteção da […] segurança do Estado […]».

84. Existe, com efeito, uma continuidade entre a Diretiva 95/46 e a Diretiva 2002/58 no que diz respeito às competências dos Estados-Membros em matéria de segurança nacional. Nenhuma das duas tem por objeto a proteção dos direitos fundamentais nesse domínio específico, uma vez que as atividades dos Estados-Membros não são «reguladas pelo direito [da União]».

85. O «equilíbrio» referido no considerando [décimo primeiro da Diretiva 2002/58] resulta da necessidade de respeitar as competências dos Estados-Membros em matéria de segurança nacional, quando estas são exercidas de forma direta e pelos seus próprios meios. Pelo contrário, quando, incluindo pelas mesmas razões de segurança nacional, é exigida a participação de particulares, aos quais são impostas algumas obrigações, esta circunstância determina a entrada num âmbito (a proteção da privacidade exigível a estes agentes privados) regulado pelo direito da União.

86. Tanto a Diretiva 95/46 como a Diretiva 2002/58 pretendem alcançar este equilíbrio autorizando a limitação dos direitos dos particulares através de medidas legislativas adotadas pelos Estados ao abrigo dos seus artigos 13.º, n.º 1, e 15.º, n.º 1, respetivamente. No que respeita a este ponto, não existe qualquer diferença entre ambas.

87. Quanto ao Regulamento n.º 2016/679, que configura um (novo) quadro geral para a proteção de dados pessoais, o seu artigo 2.º, n.º 2, não permite o «tratamento de dados pessoais» quando os Estados-Membros «levem a cabo atividades compreendidas no âmbito de aplicação do capítulo 2 do título V do TUE».

88. Enquanto na Diretiva 95/46 o tratamento de dados pessoais estava qualificado apenas pela sua finalidade, independentemente do sujeito que o levasse a cabo, no Regulamento n.º 2016/679 os tratamentos excluídos identificam-se tanto pela sua finalidade como pelos seus autores: excetuam-se os realizados pelos Estados-Membros no exercício de uma *atividade* não compreendida no âmbito de aplicação do direito da União [alíneas a) e b) do n.º2 do artigo 2.º], e os executados pelas autoridades *com fins de luta contra as infrações penais e de proteção* face às ameaças à segurança pública [45].

43 Decisão quadro do Conselho, de 18 de dezembro de 2016, relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia (JO 2006, L 386, p. 89).

44 Nessa mesma linha, o artigo 1.º, n.º 4, da Decisão quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO 2008, L 350, p. 60), previa que «não prejudica interesses essenciais de segurança nacional nem atividades específicas de informação no domínio da segurança nacional».

45 O Regulamento n.º 2016/679 exclui, de facto, o tratamento de dados feito pelos Estados-Membros no exercício de uma *atividade* que não se englobe no âmbito de aplicação do direito da União, para além do executado pelas autoridades *com fins de proteção* da segurança pública.

89. A identificação destas atividades do poder público terá de ser necessariamente restritiva, sob pena de privar de eficácia a legislação da União em matéria de proteção da privacidade. O Regulamento n.º 2016/679 prevê no seu artigo 23.º — em conformidade com o artigo 15.º, n.º 1, da Diretiva 2002/58— a limitação, mediante medidas legislativas, dos direitos e obrigações que estabelece, sempre que isso for necessário para assegurar, designadamente, a segurança do Estado, a defesa ou a segurança pública. Mais uma vez, se a proteção destes objetivos fosse suficiente para determinar a exclusão do âmbito de aplicação do Regulamento n.º 2016/679, seria desnecessário invocar a segurança do Estado como fator justificativo da restrição, através de medidas legislativas, dos direitos garantidos por este regulamento.

90. Tal como acontece com a Diretiva 2002/58, não seria coerente que as medidas legislativas previstas no artigo 23.º do Regulamento n.º 2016/679 (que, repito, autoriza limitações estatais aos direitos de privacidade dos cidadãos por razões de segurança do Estado) integrassem o âmbito de aplicação deste e, ao mesmo tempo, que a cobertura da segurança do Estado torne inaplicável, sem mais, o próprio regulamento, o que implicaria o não reconhecimento de qualquer direito subjetivo.

B. B. Confirmação e eventual de desenvolvimento da jurisprudência do Acórdão Tele2 Sverige e Watson

91. Nas minhas conclusões do processo C-520/18 faço uma análise detalhada[46] da jurisprudência do Tribunal de Justiça nesta matéria e, em consequência, proponho a sua confirmação, ao mesmo tempo que sugiro uma via interpretativa para perfilar o seu conteúdo.

92. Remeto para essa análise, que julgo não ser imprescindível transcrever agora por mera economia. As reflexões que, de seguida, farei sobre as questões prejudiciais suscitadas pelo Conseil d'Etat (Conselho de Estado) devem ler-se, assim, tendo por referência as correspondentes epígrafes das Conclusões do processo C-520/18.

C. C. Resposta às questões prejudiciais

1. 1. Sobre a obrigação de conservação dos dados (primeira questão prejudicial nos processos C-511/18 e C-512/18 e segunda questão prejudicial do processo C-512/18)

93. Quanto à obrigação de conservação de dados imposta aos prestadores de serviços de comunicações eletrónicas, o tribunal de reenvio pretende saber, em concreto:

— Se essa obrigação, exigível por força do artigo 15.º, n.º 1, da Diretiva 2002/58, constitui uma ingerência justificada pelo «direito à segurança» garantido pelo artigo 6.º da Carta e por imperativos de segurança nacional (primeira questão nos processos C-511/18 e C-512/18, e terceira questão do processo C-511/18).

— Se a Diretiva 2000/31 permite a conservação de dados que possam permitir a identificação de quem tenha contribuído para a criação dos conteúdos acessíveis ao público em linha (segunda questão no processo C-512/18).

46 Pontos 27 a 68.

a) Consideração preliminar

94. O Conseil d'État (Conselho de Estado, em formação jurisdicional) alude aos direitos fundamentais reconhecidos nos artigos 7.º (respeito pela vida privada e familiar), 8.º (proteção de dados pessoais) e 11.º (liberdade de expressão e de informação) da Carta. São, com efeito, os que, segundo o Tribunal de Justiça, poderiam ver-se afetados pela obrigação de conservação de dados de tráfego imposta pelas autoridades nacionais aos prestadores de serviços de comunicações eletrónicas [47].

95. O tribunal de reenvio alude também ao direito à segurança protegido pelo artigo 6.º da Carta. Mais do que como direito eventualmente afetado, invoca-o como fator capaz de legitimar a imposição dessa obrigação.

96. Concordo com a Comissão quanto ao facto de a invocação do artigo 6.º nesses termos poder tornar-se equívoca. Tal como a Comissão, julgo que o preceito não se deve interpretar no sentido de que tem aptidão «para impor à União uma obrigação positiva de adotar medidas dirigidas a proteger as pessoas contra atos criminosos» [48].

97. A segurança garantida por esse artigo da Carta não se identifica com a segurança pública. Ou, se se preferir, tem tanto que ver com esta última como qualquer outro direito fundamental, na medida em que a segurança pública é uma condição indispensável para o gozo dos direitos e liberdades fundamentais.

98. Segundo recorda a Comissão, o artigo 6.º da Carta corresponde ao artigo 5.º da Convenção Europeia de Direitos Humanos (a seguir, «CEDH»), como se afirma nas explicações que a acompanham. Da leitura do artigo 5.º da CEDH resulta que a «segurança» que nela se protege é unicamente a segurança pessoal, entendida como garantia do direito à liberdade física face à prisão ou ao internamento arbitrários. Em definitivo, a segurança de que ninguém pode ser privado da sua liberdade, salvo nos casos, com os requisitos e em conformidade com os procedimentos estabelecidos por lei.

99. Trata-se, portanto, da *segurança pessoal*, respeitante às condições em que se pode restringir a liberdade física das pessoas [49], e não da *segurança pública* inerente à existência do Estado, que é pressuposto imprescindível, numa sociedade desenvolvida, para conciliar o exercício dos poderes públicos com o gozo dos direitos individuais.

100. Não obstante, alguns governos pedem que se interprete o direito à segurança, preferencialmente, neste segundo sentido. Na realidade, o Tribunal de Justiça não o ignorou, e mencionou-o expressamente nos seus Acórdãos [50] e pareceres [51]. Nunca negou a importância dos objetivos de interesse geral de proteção da segurança nacional e da ordem pública [52], de luta contra o terrorismo internacional, de manutenção da paz e da segurança internacionais e da luta contra os crimes graves para garantir a segurança pública [53], que qualificou, acertadamente, de «primordial» [54]. Como sublinhou, em tempos, «a proteção da segurança pública também contribui para a proteção dos direitos e liberdades dos demais» [55].

47 Neste sentido, Acórdão Tele2 Sverige e Watson, n.º 92, citando, por analogia, o Acórdão Digital Rights, n.ºs 25 e 70.

48 N.º 37 das observações da Comissão.

49 É esta a interpretação do TEDH. Por todos, o Acórdão de 5 de julho de 2016, Buzadji c. República da Moldávia, ECHR:2016:0705JUD002375507, em cujo § 84 se afirma que o propósito fundamental do direito reconhecido pelo artigo 5.º da CEDH é prevenir a privação arbitrária ou injustificada da liberdade individual.

50 Acórdão Digital Rights, n.º 42.

51 Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017 (a seguir, «Parecer 1/15», EU:C:2017:592), n.º 149 e jurisprudência aí referida.

52 Acórdão de 15 de fevereiro de 2016, N. (C-601/15 PPU, EU:C:2016:84), n.º 53.

53 Acórdão Digital Rights, n.º 42 e jurisprudência aí referida.

54 *Ibidem*, n.º 51.

55 Parecer 1/15, n.º 149.

101. Poderia aproveitar-se a oportunidade com que estes reenvios prejudiciais nos brindam para propor mais claramente a procura de um equilíbrio entre o direito à segurança, por um lado, e o direito à intimidade e o direito à proteção dos dados pessoais, por outro. Assim se evitariam as críticas de favorecimento dos segundos em detrimento do primeiro.

102. A esse equilíbrio aludem, na minha opinião, o considerando décimo primeiro e o artigo 15.º, n.º 1, da Diretiva 2002/58, quando falam dos requisitos de necessidade e proporcionalidade das medidas *numa sociedade democrática*. O direito à segurança, repito, é inerente à própria existência e sobrevivência de uma democracia, o que justifica que se tenha plenamente em conta no contexto da valoração dessa proporcionalidade. Por outras palavras, se a preservação do princípio da confidencialidade dos dados é primordial numa sociedade democrática, também não se deve subestimar a importância da sua segurança.

103. O contexto das ameaças graves e persistentes à segurança nacional e, em particular, o risco de terrorismo, deve, pois, ter-se em conta, na linha do afirmado na última frase do n.º 119 do Acórdão Tele2 Sverige e Watson. Um sistema nacional pode responder de um modo proporcional à natureza e intensidade das ameaças que enfrenta, sem que necessariamente essa resposta tenha de ser idêntica à de outros Estados-Membros.

104. Devo acrescentar, por fim, que as reflexões anteriores não obstam a que, em situações consideradas *excecionais*, caracterizadas por uma ameaça iminente ou por um risco extraordinário que justifiquem a declaração oficial da situação de emergência num Estado-Membro, a legislação nacional contemple, por um tempo limitado, a possibilidade de impor uma obrigação de conservação de dados tão ampla e geral quanto se considere imprescindível [56].

105. Em consequência, a primeira questão de ambos os reenvios prejudiciais deveria ser reformulada, direcionando-se antes para a possibilidade de justificar a ingerência por motivos de segurança nacional. A dúvida versaria, pois, sobre se a obrigação imposta aos operadores de serviços de comunicações eletrónicas é compatível com o artigo 15.º, n.º 1, da Diretiva 2002/58.

b) b) Apreciação

1) 1) Caracterização das normas internas, tal como expostas nos dois reenvios prejudiciais, à luz da jurisprudência do Tribunal de Justiça

106. De acordo com os autos de reenvio, o normativo controvertido nos processos de origem obriga à conservação dos dados:

— pelos operadores de comunicações eletrónicas e, em particular, por quem oferecer acesso a serviços de comunicação ao público em linha; e

— pelas pessoas individuais ou coletivas que armazenem, incluindo a título gratuito, para colocação à disposição do público em linha, sinais, escritos, sons, imagens ou mensagens de qualquer natureza proporcionados pelos destinatários desses serviços [57].

56 Vejam-se os n.ºs 105 a 107 das minhas Conclusões no processo C-520/18.

57 É o que resulta do artigo L. 851-1 do Código da Segurança Interno, que remete para o artigo L. 34-1 do Código dos Correios e das Comunicações Eletrónicas e para o artigo 6.º da Lei n.º 2004-575, relativa à confiança na economia digital.

107. Os operadores devem conservar, durante um ano a contar do dia do registo, as informações que permitam identificar o utilizador, os dados relativos aos equipamentos terminais de comunicações utilizados, as características técnicas, a data, a hora e a duração de cada transação, os dados relativos aos serviços suplementares solicitados ou empregados e os seus fornecedores, bem como os dados que permitam identificar o destinatário da comunicação e, no caso das atividades de telefonia, a origem e a localização da comunicação [58].

108. Tratando-se, concretamente, dos serviços de acesso à internet e dos serviços de armazenamento, a lei nacional parece pedir a conservação das direções IP [59], as chaves de acesso e, se existir subscrição de um contrato ou faturação, o tipo de pagamento efetuado, bem como a referência, o montante, a data e a hora da transação [60].

109. Esta obrigação de conservação é exigida para fins de investigação, deteção e perseguição das infrações penais [61]. Quer dizer, ao contrário — como se mostrará — do que sucede com a obrigação de *recolha* de dados de tráfego e de localização, o dever de *conservá-los* não tem como único objetivo a prevenção do terrorismo [62].

110. Quanto às condições de *acesso* aos dados guardados, resulta da informação carreada para os autos que ou são as previstas para o regime comum (intervenção da autoridade judicial) ou o acesso é restringido a agentes individualmente designados e habilitados, mediante autorização prévia do Primeiro-Ministro dada com base no parecer não vinculativo de uma autoridade administrativa independente [63].

111. É fácil verificar, como referiu a Comissão [64], que os dados cuja conservação as normas nacionais pretendem são substancialmente os mesmos que os analisados pelo Tribunal de Justiça nos Acórdãos Digital Rights e Tele2 Sverige e Watson [65]. Tal como então, estes dados são objeto de uma «obrigação de conservação generalizada e indiferenciada», segundo salienta expressamente o Conseil d'État (Conselho de Estado, em formação jurisdicional) no início das suas questões prejudiciais.

112. Sendo assim, resta concluir que a norma em questão comporta uma «ingerência […] nos direitos fundamentais reconhecidos nos artigos 7.º e 8.º da Carta [que], de grande magnitude, devendo considerar-se especialmente grave» [66].

113. Nenhuma das partes representadas pôs em questão que uma norma com estas características implica uma ingerência nesses direitos. Não é preciso determo-nos agora nesse ponto, nem sequer para recordar que o comprometimento desses direitos redunda inevitavelmente em prejuízo dos próprios fundamentos de uma sociedade que pretende respeitar, entre outros valores, a privacidade pessoal que a Carta auspicia.

58 É o que resulta do artigo R. 10-13 do Código dos Correios e das Comunicações Eletrónicas.

59 Compete ao tribunal de reenvio verificar este tema, sobre o qual se verificaram discrepâncias no julgamento.

60 Artigo 1.º do Decreto n.º 2011-219.

61 Artigo R. 10-13 do Código dos Correios e das Comunicações Eletrónicas.

62 Tanto a Quadrature du Net como a Fédération des founisseurs d'accès à Internet associatifs sublinham a amplitude dos fins a que se destina a conservação, a faculdade de apreciação discricionária atribuída às autoridades, a ausência de critérios objetivos na sua definição e a relevância concedida a formas de criminalidade que não se podem qualificar como graves.

63 A Commission nationale de contrôle des techniques de renseignement (Comissão nacional de controlo das técnicas de informação). Vejam-se, a esse respeito, os n.ºs 145 a 148 das observações do Governo francês.

64 N.º 60 das observações da Comissão.

65 Na realidade, vão um pouco mais além, pois também parecem prever, no caso dos serviços de acesso à internet, a conservação da direção de IP ou das chaves de acesso.

66 Acórdão Tele2 Sverige e Watson, n.º 100.

114. A aplicação da jurisprudência estabelecida no Acórdão Tele2 Sverige e Watson e ratificada no Acórdão Ministerio Fiscal levaria naturalmente a sustentar que um normativo como o que aqui se discute «excede […] os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática, como exige o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º, bem como do artigo 52.º, n.º 1, da Carta» [67].

115. Com efeito, tal como o analisado no Acórdão Tele2 Sverige e Watson, o normativo que agora nos ocupa «abrange de forma generalizada todos os assinantes e utilizadores registados e […] tem por objeto todos os meios de comunicação eletrónica, bem como todos os dados de tráfego, [e] não prevê nenhuma diferenciação, limitação ou exceção em função do objetivo prosseguido» [68]. Por conseguinte, «aplica-se inclusivamente a pessoas em relação às quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com infrações penais», sem prever qualquer exceção, «pelo que também é aplicável a pessoas cujas comunicações estão sujeitas ao segredo profissional, segundo as regras do direito nacional» [69].

116. De igual modo, a norma em litígio «não exige nenhuma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a segurança pública. Nomeadamente, não está limitada a uma conservação que tenha por objeto dados relativos a período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de uma maneira ou de outra numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus dados, podiam contribuir para a luta contra a criminalidade» [70].

117. Deduz-se do exposto que esse normativo «excede […] os limites do estritamente necessário e não pode ser considerad[o] justificad[o], numa sociedade democrática, como exige o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º, bem como do artigo 52.º, n.º 1, da Carta» [71].

118. O exposto foi suficiente para que o Tribunal de Justiça concluísse que as correlativas normas nacionais não eram compatíveis com o artigo 15.º, n.º 1, da Diretiva 2002/58, na medida em que consagravam, «para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica» [72].

119. A questão que agora se coloca é se o Tribunal de Justiça poderá reformular ou, pelo menos, clarificar a sua jurisprudência em matéria de conservação de dados pessoais quando a finalidade da conservação «generalizada e indiferenciada» for a luta contra o terrorismo. A primeira questão do processo C-511/18 é formulada, precisamente, «num contexto caracterizado por ameaças graves e persistentes para a segurança nacional, em particular pelo risco terrorista».

120. Ora, sendo esse o *contexto fáctico* no qual se impõe a obrigação de conservação dos dados, o certo é que no seu *contexto normativo* não se tem apenas em consideração o terrorismo. O regime de conservação e acesso aos dados que se debate no processo no Conseil d'État (Conselho de Estado, em formação jurisdicional) sujeita essa obrigação aos fins de investigação, deteção e perseguição das infrações penais de caráter geral.

67 *Ibidem*, n.º 107.
68 *Ibidem*, n.º 105.
69 *Loc. ult. cit.*
70 Acórdão Tele2 Sverige e Watson, n.º 106.
71 *Ibidem*, n.º 107.
72 *Ibidem*, n.º 112.

121. De qualquer forma, recordo que a luta contra o terrorismo não ficou à margem dos argumentos do Acórdão Tele2 Sverige e Watson, sem que o Tribunal de Justiça entendesse então que esse tipo de infração precisava de alguma reorientação na sua jurisprudência [73].

122. Assim, entendo que à questão do órgão judicial de reenvio, centrada na especificidade da ameaça terrorista, se deverá responder no mesmo sentido em que se pronunciou o Tribunal de Justiça no Acórdão Tele2 Sverige e Watson.

123. Como defendi nas conclusões do processo Stichting Brein, «[a] certeza na aplicação do direito impõe aos órgãos jurisdicionais, se não a aplicação do *stare decisis* em termos absolutos, pelo menos a prudência de manter o que eles próprios tenham decidido, após aturada reflexão, relativamente a uma dada questão jurídica» [74].

2) 2) Restrição da conservação de dados perante as ameaças contra a segurança do Estado, incluindo a terrorista.

124. Seria possível, ainda assim, flexibilizar ou completar essa doutrina, atendendo às suas consequências para a luta contra o terrorismo ou para a proteção do Estado face a outras ameaças análogas contra a segurança nacional?

125. Já salientei que a mera conservação de dados pessoais por si só implica uma ingerência nos direitos garantidos pelos artigos 7.º, 8.º e 11.º da Carta [75]. Independentemente de, em última instância, o que com ela se pretende ser possibilitar o *acesso*, retrospetivo ou simultâneo, aos dados num determinado momento [76], a mera conservação de dados que exceda o estritamente indispensável para a transmissão de uma comunicação ou para a faturação dos serviços prestados pelo fornecedor traduz-se na inobservância dos limites previstos nos artigos 5.º e 6.º da Diretiva 2002/58.

126. Os utilizadores desses serviços (na realidade, a quase totalidade dos cidadãos nas sociedades mais desenvolvidas) desfrutam, ou devem desfrutar, de uma expectativa legítima no sentido de que, não tendo o seu consentimento, não se conservam mais dados seus para além dos que são armazenados de acordo com esses preceitos. As exceções do artigo 15.º, n.º 1, da Diretiva 2002/58 devem ler-se a partir dessa premissa.

127. Como já expliquei, o Tribunal de Justiça, no Acórdão Tele2 Sverige e Watson, também em relação à luta contra o terrorismo, recusou a conservação generalizada e indiferenciada dos dados pessoais [77].

73 *Ibidem*, n.º 103.

74 Processo C-527/15, EU:C:2016:938, ponto 41.

75 Tal como recordou o Tribunal de Justiça no Parecer 1/15, n.º 124, «a comunicação de dados pessoais a um terceiro, como uma autoridade pública, constitui uma ingerência no direito fundamental consagrado no artigo 7.º da Carta, seja qual for a utilização posterior da informação comunicada. O mesmo se diga da conservação dos dados pessoais e do acesso aos referidos dados com vista à sua utilização pelas autoridades públicas. A este respeito, pouco importa que as informações relativas à vida privada em questão sejam ou não sensíveis, ou que os interessados tenham ou não sofrido inconvenientes em razão dessa ingerência».

76 Como assinalava o advogado-geral P. Cruz Villalón nas Conclusões do processo Digital Rights, C-293/12 e C-594/12 (EU:C:2013:845), n.º 72, «a recolha e, sobretudo, a conservação, em gigantescas bases de dados, de múltiplos dados, gerados ou tratados no âmbito da maior parte das comunicações eletrónicas correntes dos cidadãos da União constitui uma ingerência caracterizada na sua vida privada, embora estas criem apenas as condições que permitem um controlo retrospetivo das suas atividades pessoais e profissionais. A recolha destes dados cria as condições para uma vigilância que, apesar de destinada a ser exercida apenas retrospetivamente aquando da sua exploração, ameaça, no entanto, permanentemente, durante toda a duração do seu período de conservação, o direito dos cidadãos da União ao segredo das suas vidas privadas. O sentimento difuso de vigilância gerado coloca de forma especialmente premente a questão da duração da conservação de dados».

77 Acórdão Tele2 Sverige e Watson, n.º 103: «não pode […] justificar que uma regulamentação nacional que prevê a conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização seja considerada necessária para efeitos da referida luta».

128. Face às críticas recebidas, não creio que a jurisprudência assente nesse acórdão desvalorize a ameaça terrorista, enquanto forma de criminalidade particularmente grave que comporta um propósito explícito de contestação à autoridade do Estado e de desestabilização ou destruição das suas instituições. A luta antiterrorista é, literalmente, vital para o Estado e o seu êxito, um objetivo de interesse geral irrenunciável para um Estado de direito.

129. Praticamente todos os Governos que integram o processo e a Comissão coincidiram em assinalar que, para além das dificuldades técnicas, uma conservação parcial e diferenciada de dados pessoais privaria os serviços de informação nacionais da possibilidade de acederem a informações indispensáveis para a identificação de ameaças à segurança pública e à defesa do Estado, bem como para a perseguição dos autores de atentados terroristas [78].

130. Face a esta apreciação parece-me pertinente salientar que a luta antiterrorista não se deve fazer apenas do ponto de vista da sua eficácia. Daí a sua dificuldade, mas também a sua grandeza quando os seus meios e os seus métodos se ajustam às exigências do Estado de direito, que é, antes de mais, sujeição do poder e da força aos limites do direito e, em especial, a uma ordem jurídica que tem na defesa dos direitos fundamentais a razão e o fim da sua existência.

131. Se, para o terrorismo, a justificação dos seus meios não tem em conta outro critério que não seja o da pura (e máxima) efetividade dos seus ataques à ordem estabelecida, para o Estado de direito a eficácia mede-se em moldes que não toleram prescindir, na sua defesa, dos procedimentos e garantias que a qualificam como uma ordem legítima. Abandonando-se sem mais à mera eficácia, o Estado de Direito perderia a qualidade que o distingue e poderia converter-se ele próprio, em casos extremos, numa ameaça para o cidadão. Nada poderia assegurar que, apetrechado o poder público de instrumentos desmesurados para a perseguição do crime, com os quais possa ignorar ou desvirtuar os direitos fundamentais, a sua ação descontrolada e inteiramente livre acabasse por se desenvolver em prejuízo da liberdade de todos.

132. A eficácia do poder público, repito, encontra uma barreira intransponível nos direitos fundamentais dos cidadãos, cujas restrições, segundo prescreve o artigo 52.º, n.º 1, da Carta, apenas podem ser previstas por lei e desde que respeitem o seu conteúdo essencial «se forem necessárias e corresponderem, efetivamente, a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros» [79].

133. Sobre as condições em que, de acordo com o Acórdão Tele2 Sverige e Watson, seria admissível uma conservação *seletiva* de dados, remeto para as minhas Conclusões do processo C-520/18 [80].

78 É, por exemplo, a interpretação do Governo francês, que ilustra esta afirmação com exemplos concretos da utilidade da conservação generalizada de dados, que permitiu a reação do Estado face aos graves atentados terroristas sofridos no seu país nos últimos anos (n.ºs 107 e 122 a 126 das observações do Governo francês).

79 Acórdão de 15 de fevereiro de 2016, N. (C-601/15 PPU, EU:C:2016:84), n.º 50. Trata-se, pois, do difícil equilíbrio entre a ordem pública e a liberdade, ao qual já me referi, e ao qual aspira, por princípio, toda a norma da União. Exemplo disso, temos a Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho (JO 2017, L 88, p. 6). Ao mesmo tempo que dispõe no seu artigo 20.º, n.º 1, que os Estados-Membros devem garantir que «sejam disponibilizados instrumentos de investigação eficazes» aos responsáveis pela investigação ou pelo julgamento de crimes de terrorismo, declara no seu considerando vigésimo primeiro que o recurso a esses instrumentos eficazes «deverá ser seletiv[o], ter em conta o princípio da proporcionalidade, a natureza e gravidade das infrações investigadas, e respeitar o direito à proteção de dados pessoais».

80 Pontos 87 a 95.

134. A circunstância de a informação disponível em poder dos serviços de segurança permitir confirmar a suspeita fundada da preparação de um atentado terrorista pode constituir um caso legítimo de imposição da obrigação de conservar certos dados. Por maioria de razão poderá fazê-lo a prática efetiva de um atentado. Se, neste último caso, a perpetração do crime pode ser por si só um fator justificativo da adoção dessa medida, ante a mera suspeita de um eventual atentado será necessário que as circunstâncias que a fundamentam ofereçam um grau mínimo de verosimilhança, imprescindível para uma ponderação objetiva dos indícios que possam justificá-la.

135. Embora seja difícil, não é impossível determinar com precisão e com base em critérios objetivos tanto as categorias de dados cuja conservação é considerada imprescindível, como o grupo das pessoas em causa. É certo que o mais prático e eficaz seria a conservação generalizada e indiscriminada de todos os dados que os prestadores dos serviços de comunicação eletrónica podem recolher, mas mas já salientei que a questão não pode ser dirimida em termos de eficácia prática, mas sim de eficácia jurídica e no âmbito de um Estado de direito.

136. Este trabalho de determinação é tipicamente legislativo, dentro dos limites que a jurisprudência do Tribunal de Justiça estabeleceu. Remeto, de novo, para o que expus sobre este assunto nas Conclusões do processo C-520/18 [81].

3) 3 Acesso aos dados conservados

137. Partindo da premissa de que os operadores recolheram os dados de acordo com as disposições da Diretiva 2002/58 e que a conservação dos mesmos foi efetuada nos termos do seu artigo 15.º, n.º 1 [82], o acesso das autoridades competentes a essa informação deve ser realizado nas condições que o Tribunal de Justiça exigiu e que analiso nas Conclusões apresentadas no processo C-520/18, para as quais remeto [83].

138. Por conseguinte, também no presente processo a legislação nacional deve estabelecer os requisitos materiais e processuais que regulam o acesso das autoridades competentes aos dados conservados [84]. No âmbito destes reenvios prejudiciais, tais requisitos autorizam o acesso aos dados das pessoas suspeitas de planearem, cometerem, terem cometido ou poderem estar envolvidas num ato terrorista [85].

139. No entanto, o essencial é que, exceto em casos de urgência devidamente justificados, o acesso aos dados em causa esteja sujeito à fiscalização de um órgão jurisdicional ou de uma autoridade administrativa independente cuja decisão responda a um pedido fundamentado das autoridades competentes [86]. Deste modo, quando não for possível chegar ao juízo abstrato da lei é garantido o juízo *in concreto* dessa autoridade independente, igualmente obrigada a garantir a segurança do Estado e a defesa dos direitos fundamentais dos cidadãos.

81 Pontos 100 a 107.

82 Desde que se verifiquem as condições mencionadas no n.º 122 do Acórdão Tele2 Sverige e Watson: o Tribunal de Justiça recordou que o artigo 15.º, n.º 1, da Diretiva 2002/58 não admite excecionar o próprio artigo 4.º, n.ºs 1 e 1 *bis*, que exige aos fornecedores a adoção de medidas que permitam garantir a proteção dos dados conservados contra os riscos de abuso e contra o acesso ilícito. Neste sentido, declarava que, «[t]endo em conta a quantidade de dados conservados, do caráter sensível desses dados e do risco de acesso ilícito a estes, os fornecedores de serviços de comunicações eletrónicas devem garantir, para assegurar a plena integridade e confidencialidade desses dados, um nível particularmente elevado de proteção e de segurança mediante medidas técnicas e de gestão adequadas. Em particular, a norma nacional deve prever a conservação dos dados no território da União e a destruição definitiva dos dados no termo do período de conservação destes».

83 Pontos 52 a 60.

84 Acórdão Tele2 Sverige e Watson, n.º 118.

85 *Ibidem*, n.º 119.

86 *Ibidem*, n.º 120.

4) 4 Obrigação de conservação de dados que permitam identificar os autores de conteúdos, à luz da Diretiva 2000/31 (segunda questão prejudicial do processo C-512/18)

140. O tribunal de reenvio reporta-se à Diretiva 2000/31 como ponto de referência para determinar se é possível obrigar certas pessoas [87] e os operadores que oferecem serviços de comunicação ao público, a conservar os dados «suscetíveis de permitir a identificação de qualquer pessoa que tenha contribuído para a criação de conteúdos ou de um dos conteúdos dos serviços que prestam, a fim de que a autoridade judiciária possa, sendo caso disso, pedir a sua comunicação para fazer respeitar as regras relativas à responsabilidade civil ou penal».

141. Concordo com a Comissão quanto ao facto de estar fora de questão a análise da compatibilidade dessa obrigação com a Diretiva 2000/31 [88], uma vez que o seu artigo 1.º, n.º 5, alínea b), exclui do seu âmbito de aplicação as «questões relacionadas com serviços da sociedade da informação incluídas nas Diretivas 95/46/CE e 97/66/CE», diplomas que correspondem agora ao Regulamento n.º n.º 2006/679 e à Diretiva 2002/58 [89], cujos respetivos artigos 23.º, n.º 1, e 15.º, n.º 1, devem ser interpretados, no meu entender, nos termos anteriormente expostos.

2. 2. Sobre a obrigação de recolha em tempo real de dados de tráfego e de localização (segunda questão prejudicial do processo C-511/18)

142. Para o tribunal de reenvio, o artigo L. 851-2 do Código da Segurança Interna autoriza, apenas para fins de prevenção do terrorismo, a recolha, em tempo real, de informação acerca de pessoas previamente identificadas como suspeitas de estar ligadas a uma ameaça terrorista. De igual forma, o artigo L. 851-4 desse Código permite a transmissão em tempo real, pelos operadores, dos dados técnicos relativos à localização dos equipamentos terminais.

143. Segundo o órgão judicial de reenvio, estas técnicas não impõem aos fornecedores uma obrigação de conservação suplementar à necessária para a faturação e para a comercialização dos seus serviços.

144. Além disso, nos termos do artigo L. 851-3 do Código da Segurança Interna, os operadores de comunicações eletrónicas e os prestadores de serviços técnicos podem ser obrigados a «aplicar nas suas redes tratamentos automatizados de dados destinados, em função dos parâmetros estabelecidos na autorização, a detetar ligações que possam representar uma ameaça terrorista». Esta técnica não comporta uma conservação generalizada e indiferenciada de dados e visa recolher, durante um tempo limitado, os dados de ligação que possam estar relacionados com uma infração de natureza terrorista.

145. No meu entender, as condições exigíveis para o acesso aos dados pessoais armazenados devem aplicar-se igualmente ao acesso em tempo real aos dados gerados no decurso das comunicações eletrónicas. Remeto, pois, para o que já disse sobre esse tema. É irrelevante que se trate de dados conservados ou de dados obtidos no momento, pois em ambos os casos se toma conhecimento de dados pessoais, não importando que sejam passados ou atuais.

146. Em concreto, se o acesso em tempo real for consequência de ligações detetadas em consequência de um tratamento automatizado, como o previsto no artigo L. 851-3 do Código da Segurança Interna, impõe-se que os modelos e critérios pré-estabelecidos para esse tratamento sejam específicos, fiáveis e não discriminatórios, de modo que facilitem a identificação de indivíduos sobre os quais recaia uma suspeita fundada de participação em atividades terroristas [90].

87 As que «armazenam […] para a colocação à disposição do público através de serviços de comunicação ao público em linha, sinais, textos, imagens, sons ou mensagens de qualquer natureza proporcionados pelos destinatários desses serviços […]».

88 Esta diretiva é mencionada, em termos genéricos e sem especificar nenhum preceito, pelo tribunal de reenvio na segunda questão do processo C-512/18.

89 N.ºs 112 e 113 das observações da Comissão.

90 Acórdão Digital Rights, n.º 59.

3. 3. Sobre a obrigação de informar os afetados (terceira questão prejudicial do processo C-511/18)

147. O Tribunal de Justiça afirmou que as autoridades às quais se conceda o acesso aos dados devem informar desta circunstância as pessoas afetadas, desde que não sejam comprometidas as investigações em curso. O fundamento desse dever estriba-se no facto de a referida informação ser necessária para que aquelas pessoas possam exercer o seu direito à tutela judicial efetiva, expressamente referido no artigo 15.º, n.º 2, da Diretiva 2002/58, em caso de violação dos seus direitos [91].

148. O Conseil d'État (Conselho de Estado, em formação jurisdicional) pretende saber, com a sua terceira questão no processo C-511/18, se essa exigência de informação é imprescindível ou se pode ser dispensada quando se tenham previsto outras garantias, como as que descreve no seu despacho de reenvio.

149. De acordo com a exposição do tribunal de reenvio [92], as mencionadas garantias traduzem-se na possibilidade de quem deseje certificar-se se uma técnica de informação foi aplicada de forma ilegal se dirigir ao próprio Conseil d'État (Conselho de Estado, em formação jurisdicional). Este órgão poderá chegar, consoante as circunstâncias, a anular a autorização da medida e ordenar a destruição do material recolhido, num procedimento que não prevê o princípio do contraditório habitual nos processos jurisdicionais.

150. O órgão de reenvio considera que esse normativo não viola o direito à tutela judicial efetiva. Considero, porém, que, em teoria, poderia ser admitido relativamente às pessoas que decidam comprovar se são objeto de uma operação de informações. Pelo contrário, não esse direito não é respeitado relativamente àqueles que, sendo ou tendo sido objeto dessa operação, não tenham sido advertidos dessa circunstância e, portanto, nem sequer possam colocar a questão de saber se os seus direitos foram ou não afetados.

151. As garantias jurisdicionais a que se refere o órgão judicial de reenvio parecem estar condicionadas à iniciativa de quem suspeite ser objeto de uma recolha de informação sobre a sua pessoa. Não obstante, o acesso aos tribunais para a defesa dos seus direitos deve ser efetivo para todos, o que significa que quem tenha sido objeto de um tratamento dos seus dados pessoais deve ter a possibilidade de questionar judicialmente a legalidade desse tratamento e, em consequência, deve ser notificado da ocorrência do mesmo.

152. Segundo resulta da informação disponibilizada, a ação da justiça pode desencadear-se oficiosamente ou por denúncia administrativa, mas deve dar-se ao afetado, em qualquer caso, a possibilidade de ser ele próprio a recorrer à justiça, para o que é necessário que lhe seja revelado que os seus dados pessoais foram objeto de determinado tratamento. Não pode confiar a defesa dos seus direitos ao facto de vir a ter conhecimento desse tratamento por terceiros ou pelos seus próprios meios.

153. Assim, na medida em que não se comprometa o curso das investigações para as quais se concedeu o acesso aos dados conservados, deve-se comunicar à pessoa afetada esse acesso.

154. Questão diferente é, uma vez movido o processo judicial pelo afetado depois de lhe ter sido comunicado o acesso aos seus dados, o subsequente processo judicial ficar sujeito às exigências de confidencialidade e de reserva inerentes à fiscalização da ação dos poderes públicos em âmbitos sensíveis como o da segurança e da defesa do Estado. Essa questão é, porém, alheia a estes reenvios, de maneira que, no meu entender, o Tribunal de Justiça não se deve pronunciar a esse respeito.

91 Acórdão Tele2 Sverige e Watson, n.º 121.

92 N.ºs 8 a 11 do despacho de reenvio.

V. Conclusão

155. Em face do exposto, sugiro ao Tribunal de Justiça que responda ao Conseil d'État (Conselho de Estado, em formação jurisdicional) 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 dos dados pessoais e à proteção da intimidade no setor das comunicações eletrónicas (Diretiva sobre a privacidade e as comunicações eletrónicas), 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, deve ser interpretado no sentido de que:

1) Se opõe a um normativo nacional que, num contexto caracterizado por ameaças graves e persistentes para a segurança nacional, em especial pelo risco terrorista, impõe aos operadores e prestadores de serviços de comunicações eletrónicas a obrigação de conservarem, de modo geral e indiferenciado, os dados de tráfego e de localização de todos os assinantes, bem como os dados que permitam identificar os criadores dos conteúdos oferecidos pelos fornecedores dos referidos serviços.

2) Se opõe a um normativo nacional que não prevê a obrigação de informar as pessoas afetadas acerca do tratamento dos seus dados pessoais, levado a cabo pelas autoridades competentes, salvo se essa comunicação comprometer a ação das referidas autoridades.

3) Não se opõe a uma norma nacional que permite recolher em tempo real os dados de tráfego e de localização de pessoas singulares, na medida em que essas ações se realizem de acordo com os procedimentos estabelecidos para o acesso aos dados pessoais legitimamente conservados e com as mesmas garantias.»