Coletânea da Jurisprudência

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

Processo C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
contra
Conseil des ministres,
com a intervenção de:
Child Focus,

[pedido de decisão prejudicial apresentado pela Cour constitutionnelle (Tribunal Constitucional, Bélgica)]

«Reenvio prejudicial — Tratamento de dados pessoais e proteção da privacidade no setor das comunicações eletrónicas — Diretiva 2002/58/CE — Âmbito de aplicação — Artigo 1.º, n.º 3 — Artigo 15.º, n.º 1 — Artigo 4.º, n.º 2, TUE — Carta dos Direitos Fundamentais da União Europeia — Artigos 4.º, 6.º, 7.º, 8.º, 11.º e 52.º, n.º 1 — Obrigação de conservação generalizada e indiferenciada dos dados relativos ao tráfego e de localização — Efetividade da investigação penal e outros objetivos de interesse público»

1. O Tribunal de Justiça tem vindo a manter nos últimos anos uma corrente jurisprudencial constante sobre a conservação e o acesso aos dados pessoais, cujos marcos importantes são:

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

[1] Língua original: espanhol.

[2] C-293/12 e C-594/12, a seguir «Acórdão Digital Rights Ireland e o.», 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).

– O Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o.[4], no qual interpretou o artigo 15.º, n.º 1, da Diretiva 2002/58/CE[5].

– O Acórdão de 2 de outubro de 2018, Ministério Fiscal[6], no qual confirmou a interpretação dessa mesma disposição da Diretiva 2002/58.

2. Estes acórdãos (em especial, o segundo) preocupam as autoridades de alguns Estados-Membros, pois, em seu entender, têm como consequência privá-las de um instrumento que consideram necessário para a salvaguarda da segurança nacional e para a luta contra a criminalidade e o terrorismo. Daí que alguns desses Estados-Membros defendam a revogação ou aperfeiçoamento dessa jurisprudência.

3. Determinados órgãos jurisdicionais dos Estados-Membros expressaram esta mesma preocupação em quatro reenvios prejudiciais[7], relativamente aos quais, nesta mesma data, apresento as minhas conclusões.

4. Os quatro processos colocam, desde logo, 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 nesse âmbito, deve então esclarecer-se, ato contínuo, em que medida podem os Estados-Membros restringir os direitos à privacidade que protege. Por último, deve apreciar-se até que ponto as diferentes legislações nacionais (do Reino Unido[8], belga[9] e francesa[10]) sobre esta matéria estão em conformidade com o direito da União, tal como foi interpretado pelo Tribunal de Justiça.

5. Após a publicação do Acórdão Digital Rights Ireland e o., a Cour constitutionnelle (Tribunal Constitucional, Bélgica) anulou a legislação nacional que tinha transposto parcialmente para o direito nacional a Diretiva 2006/24, declarada inválida nesse acórdão. O legislador belga adotou, então, uma nova regulamentação, cuja compatibilidade com o direito da União voltou a ser posta em causa na sequência do Acórdão Tele2 Sverige e Watson e o.

6. Uma especificidade do presente reenvio reside no facto de suscitar a possibilidade de prorrogar provisoriamente os efeitos de uma lei nacional cuja anulação pelos tribunais nacionais seja imposta devido à sua incompatibilidade com o direito da União.

4 C-203/15 e C-698/15, a seguir «Acórdão Tele2 Sverige e Watson e o.», 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 C-207/16, a seguir «Acórdão Ministério Fiscal», EU:C:2018:788.

7 Além deste (Processo C-520/18, Ordre des barreaux francophones et germanophone e o.) trata-se dos processos apensos C-511/18 e C-512/18, La Quadrature du Net e o. e do Processo C-623/17, Privacy International.

8 Processo Privacy International (C-623/17).

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

10 Processos apensos La Quadrature du Net e o. (C-511/18 e C-512/18).

I. Quadro jurídico

A. Direito da União

7. Remeto para o número correspondente das minhas Conclusões nos processos apensos La Quadrature du Net e o. (C-511/18 e C-512/18, EU:C:2020:6).

B. Direito belga

8. O artigo 4.º da loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11] (Lei relativa à Recolha e à Conservação de Dados no Setor das Telecomunicações Eletrónicas), de 29 de maio de 2016, dispõe que o artigo 126.º da loi relative aux communications électroniques [12] (Lei relativa às Telecomunicações Eletrónicas), de 13 de junho de 2005, passa a ter a seguinte redação:

«1. Sem prejuízo da loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [Lei de 8 de dezembro de 1992 relativa à Proteção da Vida Privada no que diz respeito ao Tratamento de Dados Pessoais], os prestadores de serviços de telefonia ao público, incluindo pela Internet, de acesso à Internet, de correio eletrónico pela Internet, os operadores que fornecem redes públicas de comunicações eletrónicas, bem como os operadores que prestam um destes serviços, devem conservar os dados referidos no n.º 3, que sejam por eles gerados ou tratados no âmbito da prestação dos serviços de comunicação em causa.

O presente artigo não é relativo ao conteúdo das comunicações.

[…]

2. As seguintes entidades serão as únicas a quem, a seu pedido, poderão ser comunicados pelos prestadores e operadores referidos no n.º 1, primeiro parágrafo, os dados conservados por força do presente artigo, para as finalidades e nas condições a seguir indicadas:

1.º as autoridades judiciárias, com vista à investigação, à instrução e à instauração de procedimento criminal em relação a crimes, para a execução das medidas referidas nos artigos 46bis e 88bis do Código de Processo Penal e nas condições fixadas por esses artigos;

2.º os serviços de informações e de segurança, a fim de cumprirem as missões de informação, com recurso aos métodos de recolha de dados referidos nos artigos 16/2, 18/7 e 18/8 da loi du 30 novembre 1998 organique des services de renseignement et de Sécurité [13][(Lei Orgânica dos Serviços de Informações e de Segurança, de 30 de novembro de 1998)] e nas condições previstas na presente lei:

3.º qualquer agente de Polícia Judiciária do Institut [belge des services postaux et des télécommunications (Instituto Belga dos Serviços Postais e Telecomunicações)], com vista à investigação, à instrução e à instauração de procedimento criminal em relação a infrações às [regras de segurança das redes] e ao presente artigo;

11 *Moniteur belge* de 18 de julho de 2016, p. 44717, a seguir «Lei de 29 de maio de 2016».

12 *Moniteur belge* de 20 de junho de 2005, p. 28070, a seguir «Lei de 2005»

13 *Moniteur belge* de 18 de dezembro de 1998, p. 40312, a seguir «Lei de 1998».

4.º os serviços de urgência que prestam apoio a nível local, quando, na sequência de uma chamada de emergência, não obtenham do prestador ou do operador em causa os dados de identificação da pessoa que efetua a chamada […] ou obtenham dados incompletos ou incorretos. Apenas os dados de identificação da pessoa que efetua a chamada podem ser pedidos e, o mais tardar, durante as 24 horas seguintes à chamada;

5.º o agente de Polícia Judiciária da divisão de pessoas desaparecidas da Polícia Federal, no âmbito da sua missão de assistência às pessoas em perigo, de procura de pessoas cujo desaparecimento é preocupante e quando existem presunções ou indícios sérios de que a integridade física da pessoa desaparecida se encontra em situação de perigo iminente. Apenas os dados referidos no n.º 3, primeiro e segundo parágrafos, relativos à pessoa desaparecida e conservados durante as 48 horas anteriores ao pedido de obtenção de dados, podem ser solicitados ao operador ou ao prestador em causa por intermédio de um serviço de polícia designado pelo Rei;

6.º o Serviço de Mediação para as Telecomunicações, com vista à identificação da pessoa que utilizou indevidamente uma rede ou um serviço de comunicações eletrónicas […]. Apenas podem ser pedidos os dados de identificação.

Os prestadores e operadores referidos no n.º 1, primeiro parágrafo, devem ter as condições necessárias para que os dados referidos no n.º 3 sejam acessíveis de forma ilimitada a partir da Bélgica e para que esses dados e qualquer outra informação necessária relacionada com eles possam ser transmitidos imediatamente às autoridades referidas no presente número.

Sem prejuízo de outras disposições legais, os prestadores e operadores referidos no n.º 1, primeiro parágrafo, não podem utilizar os dados conservados nos termos do n.º 3 para outras finalidades.

3. Os dados destinados a identificar o utilizador ou o assinante e os meios de comunicação, com exceção dos dados especificamente previstos no segundo e terceiro parágrafos, são conservados durante doze meses a contar da data a partir da qual é possível efetuar pela última vez uma comunicação através do serviço utilizado.

Os dados relativos ao acesso e à ligação do equipamento terminal à rede e ao serviço e à localização deste equipamento, incluindo o ponto terminal da rede, são conservados durante doze meses a partir da data da comunicação.

Os dados de comunicações, com exclusão do conteúdo, incluindo a sua origem e o seu destino, são conservados durante doze meses a partir da data da comunicação.

O Rei determina, por decreto aprovado em Conselho de Ministros, sob proposta do ministro da Justiça e do ministro, e após parecer da Comissão da proteção da vida privada e do Instituto, os dados a conservar por tipo de categorias referidas nos n.os 1 a 3, bem como as exigências que esses dados devem respeitar.

4. Para a conservação dos dados referidos no n.º 3, os prestadores e os operadores referidos no primeiro parágrafo do n.º 1 deverão:

1.º garantir que os dados conservados são da mesma qualidade e estão sujeitos às mesmas exigências de segurança e de proteção que os dados na rede;

2.º assegurar que os dados conservados são objeto de medidas técnicas e organizacionais adequadas para os proteger da destruição acidental ou ilícita, da perda ou da alteração acidental, e do armazenamento, do tratamento, do acesso ou da divulgação não autorizados ou ilegais;

3.º garantir que o acesso aos dados conservados para responder aos pedidos das autoridades referidas no n.º 2 apenas é efetuado por um ou mais membros da Divisão de coordenação referida no artigo 126/1, n.º 1;

4.º conservar os dados no território da União Europeia;

5.º aplicar medidas de proteção tecnológica que tornem os dados conservados, desde o seu registo, ilegíveis e inutilizáveis por qualquer pessoa a quem não tenha sido autorizado o acesso;

6.º eliminar os dados conservados de qualquer suporte quando tiver expirado o prazo de conservação aplicável a esses dados fixado no n.º 3, sem prejuízo dos artigos 122.º e 123.º;

7.º assegurar a rastreabilidade da exploração dos dados conservados relativamente a cada pedido de obtenção destes dados por parte de uma autoridade referida no n.º 2.

A rastreabilidade referida em 7.º será efetuada através de um registo. O Instituto e a Comissão para a proteção da vida privada podem consultar esse registo ou exigir uma cópia integral ou parcial do mesmo. O Instituto e a Comissão para a proteção da vida privada devem celebrar um protocolo de colaboração relativo à tomada de conhecimento e ao controlo do conteúdo do jornal.

5. O ministro e o ministro da Justiça deverão apresentar todos os anos à Câmara dos Representantes estatísticas sobre a conservação de dados gerados ou tratados no âmbito da oferta de serviços ou redes de comunicações publicamente disponíveis.

Estas estatísticas incluem, nomeadamente:

1.º os casos de transmissão de dados às autoridades competentes em conformidade com as disposições legais aplicáveis;

2.º o período de tempo decorrido entre a data a partir da qual os dados foram conservados e a data em que as autoridades competentes pediram a sua transmissão;

3.º os casos em que os pedidos de dados não puderam ser satisfeitos.

Estas estatísticas não podem incluir dados pessoais.

[…]»

9. O artigo 5.º da Lei de 29 de maio de 2016 prevê a inserção de um artigo 126/1 na Lei de 2005, com a seguinte redação:

«1. Em cada operador e prestador dos referidos no artigo 126/1, primeiro parágrafo, deverá ser constituída uma divisão de coordenação, responsável por fornecer às autoridades belgas legalmente habilitadas, a pedido destas, os dados conservados nos termos dos artigos 122.º,

123.º e 126.º, os dados de identificação da pessoa que efetua a chamada nos termos do artigo 107.º, n.º 2, primeiro parágrafo, ou os dados que podem ser pedidos nos termos dos artigos 46bis, 88bis e 90ter do Código de Processo Penal e dos artigos 18/7, 18/8, 18/16 e 18/17, da [Lei de 1998].

[…]

2. Os operadores e os prestadores a que se refere o artigo 126.º, n.º 1, primeiro parágrafo, devem estabelecer um procedimento interno que permita responder aos pedidos de acesso das autoridades aos dados pessoais dos utilizadores. Mediante pedido, devem colocar à disposição do Instituto informações relativas a tais procedimentos, ao número de pedidos recebidos, à base jurídica invocada e à sua resposta.

[…]

3. Os prestadores e os operadores a que se refere o artigo 126.º, n.º 1, primeiro parágrafo, devem designar uma ou várias pessoas encarregadas da proteção dos dados pessoais, que devem respeitar os requisitos cumulativos enumerados no n.º 1, terceiro parágrafo.

[…]

No exercício das suas missões, o ou os encarregados da proteção de dados pessoais atuam de maneira independente e têm acesso a todos os dados pessoais transmitidos às autoridades, assim como a todas as instalações relevantes do prestador ou do operador.

[…]

4. O Rei deve determinar, por decreto aprovado em Conselho de Ministros, após parecer da Comissão para a proteção da vida privada e do Instituto:

[…]

2.º as exigências que a Divisão de coordenação deve respeitar, tendo em conta a situação dos operadores e prestadores que recebem poucos pedidos das autoridades judiciárias, que não tenham sede na Bélgica ou que operem principalmente a partir do estrangeiro;

3.º as informações a fornecer ao Instituto e à Comissão para a proteção da vida privada, em conformidade com os n.os 1 e 3, bem como as autoridades que têm acesso a estas informações;

4.º as outras regras de colaboração entre os operadores e os prestadores referidos no artigo 126.º, n.º 1, primeiro parágrafo, e as autoridades belgas ou algumas destas, para o fornecimento dos dados referidos no n.º 1, incluindo, se necessário por parte da autoridade em causa, a forma e o conteúdo do pedido.

[…]»

10. O artigo 8.º Lei de 29 de maio de 2016 dispõe que o artigo 46bis, n.º 1, do Código de Processo Penal belga terá a seguinte redação:

«1. Ao investigar crimes, o procurador do Rei pode, por decisão fundamentada e escrita, pedindo, se necessário, a assistência do operador de uma rede de comunicações eletrónicas ou de um serviço de polícia designado pelo Rei, proceder ou ordenar que se proceda, com base em todos os dados que possua ou através de acesso aos ficheiros dos clientes do operador ou do fornecedor de serviços:

1.º à identificação do assinante ou do utilizador habitual de um serviço de comunicações eletrónicas ou do meio de comunicação eletrónica utilizado;

2.º à identificação dos serviços de comunicações eletrónicas dos quais uma determinada pessoa seja assinante ou que sejam habitualmente utilizados por uma determinada pessoa.

A medida adotada deve ser comprovadamente proporcionada, à luz do respeito da vida privada, e subsidiária em relação a qualquer outro dever de investigação.

Em caso de extrema urgência, cada agente de Polícia Judiciária pode, com prévia autorização verbal do procurador do Rei, e por decisão fundamentada por escrito, pedir esses dados. O agente de Polícia Judiciária deverá comunicar essa decisão fundamentada por escrito, bem como as informações recolhidas, no prazo de vinte e quatro horas ao procurador do Rei e apresentar uma justificação para a extrema urgência.

No que respeita a crimes a que não corresponda pena de prisão principal de um ano ou mais grave, o procurador do Rei ou, em caso de extrema urgência, o agente de Polícia Judiciária, apenas podem pedir os dados referidos no primeiro parágrafo em relação a um período de seis meses anterior à sua decisão.

2. O operador de uma rede de comunicações eletrónicas e o prestador de serviços de comunicações eletrónicas ao qual seja pedido que comunique os dados referidos no n.º 1, deverá facultar ao procurador do Rei ou ao agente de Polícia Judiciária os dados pedidos dentro de um prazo a fixar pelo Rei […].

[…]

Qualquer pessoa que, pela função que ocupa, tiver conhecimento da medida ou para ela contribua, tem dever de sigilo. A violação do sigilo é punida em conformidade com o artigo 458.º do Código Penal.

A recusa de comunicação dos dados é punida com multa de vinte e seis euros a dez mil euros.»

11. O artigo 9.º Lei de 29 de maio de 2016 dá a seguinte redação ao artigo 88bis do Código de Processo Penal belga:

«1. Se existirem indícios sérios de que os crimes são suscetíveis de conduzir a uma pena de prisão principal de um ano ou mais grave, e quando o juiz de instrução considere que existem circunstâncias que tornam a deteção de comunicações eletrónicas ou a localização da origem ou do destino de comunicações eletrónicas necessária para o apuramento da verdade, pode ordenar

que se proceda, pedindo, diretamente ou por intermédio de um serviço de polícia designado pelo Rei, a assistência técnica do operador de uma rede de comunicações eletrónicas ou do fornecedor de um serviço de comunicações eletrónicas:

1.º a identificação dos dados de tráfego de meios de comunicação eletrónica a partir dos quais ou para os quais as comunicações eletrónicas sejam ou tenham sido enviadas;

2.º a localização da origem ou do destino de comunicações eletrónicas.

Nos casos referidos no primeiro parágrafo, em relação a cada meio de comunicação eletrónica cujos dados de chamada sejam identificados ou cuja origem ou destino da telecomunicação seja localizada, o dia, a hora, a duração e, se necessário, o local da comunicação eletrónica, são indicados e consignados num auto.

O juiz de instrução indica em despacho fundamentado as circunstâncias de facto do processo que justificam a medida, o seu caráter proporcionado à luz do respeito da vida privada e, subsidiariamente, qualquer outro dever de investigação.

Deve também precisar o período durante o qual a medida poderá ser aplicada no futuro, período que não pode exceder dois meses desde a data do despacho, sem prejuízo de prorrogação e, se necessário, o período anterior a que o despacho se estende em conformidade com o n.º 2.

[…]

2. No que respeita à aplicação da medida referida no n.º 1, primeiro parágrafo, aos dados de tráfego ou de localização conservados com fundamento no artigo 126.º da Lei [de 2005], são aplicáveis as disposições seguintes:

– nos casos dos crimes previstos no livro II, título Iter, do Code pénal [Código Penal], o juiz de instrução pode, no seu despacho, pedir os dados relativos ao período de doze meses anterior ao despacho;

– nos casos dos outros crimes previstos no artigo 90ter, n.ºs 2 a 4, não referidos no primeiro travessão ou nos casos de crimes previstos cometidos no âmbito de uma organização criminosa referida no artigo 324bis do Código Penal, ou nos casos de crimes passíveis de pena de prisão principal de cinco anos ou de pena mais grave, o juiz de instrução pode, no seu despacho, pedir os dados relativos ao período de nove meses anterior ao despacho;

– nos casos dos outros crimes, o juiz de instrução apenas pode pedir os dados relativos ao período de seis meses anterior ao despacho.

3. A medida apenas pode abranger os meios de comunicação eletrónica de advogados ou médicos se estes forem suspeitos de ter cometido ou participado na prática de uma infração prevista no n.º 1, ou se houver factos precisos que permitam presumir a utilização dos seus meios de comunicação eletrónica por terceiros suspeitos de terem cometido esses crimes.

A medida não pode ser executada sem que o Bastonário da Ordem dos Advogados ou o representante da ordem regional dos médicos, consoante o caso, seja informado. Estas mesmas pessoas serão informadas pelo juiz de instrução dos elementos que este considera abrangidos pelo sigilo profissional. Esses elementos não serão consignados em auto.

4. […]

Qualquer pessoa que, pela função que ocupa, tiver conhecimento da medida ou para ela contribua, tem um dever de sigilo. A violação do sigilo é punida em conformidade com o artigo 458.º do Código Penal.

[…]»

12. Em conformidade com o artigo 12.º da Lei de 29 de maio de 2016, o artigo 13.º da Lei de 1998 tem a seguinte redação:

«Os serviços de informações e de segurança podem pesquisar, recolher, receber e tratar informações e dados pessoais que possam ser úteis para a execução das suas missões e manter atualizada uma documentação relativa, nomeadamente, a eventos, agrupamentos e pessoas que tenham interesse para a execução das suas funções.

As informações constantes da documentação devem apresentar um nexo com a finalidade do ficheiro e limitar-se às exigências que daí decorrem.

Os serviços de informações e de segurança devem garantir a segurança dos dados relativos às suas fontes e às informações e dos dados pessoais fornecidos por essas fontes.

Os agentes dos serviços de informações e de segurança têm acesso às informações e dados pessoais recolhidos e tratados pelo seu serviço, desde que estes sejam úteis no exercício da sua função ou da sua missão.»

13. O artigo 14.º da Lei de 29 de maio de 2016 dá uma nova redação ao artigo 18/3 da Lei de 1998, que passou a dispor:

«1. Podem ser adotados os métodos específicos de recolha de dados referidos no artigo 18/2, n.º 1, tendo em conta a potencial ameaça referida no artigo 18/1, se os métodos ordinários de recolha de dados forem considerados insuficientes para permitir recolher as informações necessárias à conclusão de uma missão de informação. O método específico deve ser escolhido em função do grau de gravidade da potencial ameaça para a qual é adotado.

O método específico apenas pode ser adotado após decisão escrita e fundamentada do dirigente do serviço e após notificação dessa decisão à Comissão.

2. A decisão do dirigente do serviço deve mencionar:

1.º a natureza do método específico;

2.º consoante o caso, as pessoas singulares ou coletivas, as associações ou os agrupamentos, os objetos, os locais, os eventos ou as informações sujeitas ao método específico;

3.º a potencial ameaça que justifica o método específico;

4.º as circunstâncias de facto que justificam o método específico, a fundamentação em matéria de subsidiariedade e de proporcionalidade, incluindo o nexo entre os pontos 2.º e 3.º;

5.º o período durante o qual o método específico pode ser aplicado, a contar da notificação da decisão da Comissão;

[…]

9.º eventualmente, os indícios sérios que confirmam que o advogado, o médico ou o jornalista participa ou participou pessoal e ativamente na criação ou no desenvolvimento da potencial ameaça;

10.º caso seja aplicado o artigo 18/8, a fundamentação da duração do período a que se refere a recolha de dados;

[…]

8. O dirigente do serviço deve pôr termo ao método específico quando a potencial ameaça que o justifica tiver desaparecido, quando o método já não seja útil para a finalidade para a qual foi adotado ou quando concluía pela existência de uma ilegalidade. Deve informar imediatamente a Comissão da sua decisão.»

14. Ao artigo 18/8 da Lei de 1988 é dada a seguinte redação:

«1. Os serviços de informações e de segurança podem, para o exercício das suas missões, pedir para o efeito, se necessário, a assistência técnica do operador de uma rede de comunicação eletrónica ou do prestador de um serviço de comunicação eletrónica, proceder ou ordenar que se proceda:

1.º à identificação dos dados de tráfego de meios de comunicação eletrónica a partir dos quais ou para os quais as comunicações eletrónicas são, ou foram, enviadas;

2.º à localização da origem ou do destino de comunicações eletrónicas.

[…]

2. No que respeita à aplicação do método referido no n.º 1 aos dados conservados com fundamento no artigo 126.º da Lei [de 2005] são aplicáveis as disposições seguintes:

1.º no que se refere a uma potencial ameaça relacionada com uma atividade que possa estar ligada a organizações criminosas ou a organizações sectárias prejudiciais, o dirigente do serviço, na sua decisão, apenas pode pedir os dados relativos a um período de seis meses anterior à decisão;

2.º no que se refere a uma potencial ameaça distinta das referidas nos pontos 1.º e 3.º, o dirigente do serviço, na sua decisão, pode pedir os dados relativos a um período de nove meses anterior à decisão;

3.º no que se refere a uma potencial ameaça relacionada com uma atividade que possa estar ligada ao terrorismo ou ao extremismo, o dirigente do serviço, na sua decisão, pode pedir os dados relativos a um período de doze meses anterior à decisão. […]»

II. II. Factos no processo principal e questões prejudiciais

15. No seu Acórdão de 11 de junho de 2015 [14], a Cour constitutionnelle (Tribunal Constitucional) anulou a nova redação do artigo 126.º da Lei de 2005, com base nos mesmos fundamentos que levaram o Tribunal de Justiça a anular a Diretiva 2006/24 no Acórdão Digital Rights Ireland e o.

16. Em face dessa anulação, o legislador nacional adotou a Lei de 29 de maio de 2016 (antes de ter sido proferido o Acórdão Tele 2 Sverige e Watson e o.).

17. VZ e o., a Ordre des barreaux francophones et germanophone (a seguir «Ordre des barreaux»), a Liga voor Mensenrechten ASBL («LMR»), a Ligue des Droits de l'Homme ASBL («LDH») e a Académie Fiscale ASBL («Académie Fiscale») interpuseram no órgão jurisdicional de reenvio diversos recursos de anulação da referida lei, alegando, em síntese, que ia além do que era estritamente necessário e não previa suficientes garantias de proteção.

18. Neste quadro, a Cour constitutionnelle (Tribunal Constitucional) submeteu ao Tribunal de Justiça as seguintes questões:

«1) Deve o artigo 15.º, n.º 1, da Diretiva 2002/58/CE, lido em conjugação com o direito à segurança, garantido pelo artigo 6.º da Carta dos Direitos Fundamentais da União Europeia, e o direito ao respeito dos dados pessoais, garantido pelos artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, ser interpretado no sentido de que se opõe a uma regulamentação nacional como a que está em causa, que prevê uma obrigação geral de os operadores e prestadores de serviços de comunicações eletrónicas conservarem os dados de tráfego e de localização na aceção da Diretiva 2002/58/CE, gerados ou tratados por estes no âmbito da prestação de tais serviços, regulamentação nacional que não tem apenas por objetivo a investigação, a deteção e a instauração de procedimento criminal em relação a factos constitutivos de criminalidade grave, mas igualmente a garantia da segurança nacional, a defesa do território e a segurança pública, a investigação, a deteção e a instauração de procedimento criminal em relação a factos não constitutivos de criminalidade grave ou a prevenção de uma utilização proibida dos sistemas de comunicação eletrónica, ou a realização de outro objetivo identificado pelo artigo 23.º, n.º 1, do Regulamento (UE) 2016/679 [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 sobre a Proteção de Dados) (JO 2016, L 119, p. 1)] e que, além disso, está sujeita a garantias precisadas nesta regulamentação no plano da conservação dos dados e do acesso aos mesmos?

2) Deve o artigo 15.º, n.º 1, da Diretiva [2002/58], conjugado com os artigos 4.º, 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta […], ser interpretado no sentido de que se opõe a uma regulamentação nacional como a que está em causa, que prevê uma obrigação geral de os operadores e prestadores de serviços de comunicações eletrónicas conservarem os dados de tráfego e de localização na aceção da Diretiva [2002/58], gerados ou tratados por estes no âmbito da prestação de tais serviços, se esta regulamentação tiver designadamente por objeto o cumprimento das obrigações positivas que incumbem à autoridade por força dos artigos 4.º e 8.º da Carta, que consistem em prever um quadro legal que permita uma fase de inquérito efetiva e uma repressão efetiva do abuso sexual de menores e que permita efetivamente identificar o autor do crime, mesmo quando são utilizados meios de comunicações eletrónicos?

[14] Acórdão n.º 84/2015, *Moniteur belge* de 11 de agosto de 2015.

3) No caso de, com base nas respostas à primeira ou à segunda questão prejudicial, a Cour constitutionnelle [Tribunal Constitucional] concluir que a lei impugnada viola uma ou mais das obrigações decorrentes das disposições referidas nestas questões, pode manter provisoriamente os efeitos da Lei de 29 de maio de 2016, relativa à recolha e à conservação dos dados no setor das comunicações eletrónicas, a fim de evitar a insegurança jurídica e permitir que os dados recolhidos e conservados anteriormente possam ainda ser utilizados para efeitos dos objetivos prosseguidos pela lei?»

III. Tramitação do processo no Tribunal de Justiça

19. O pedido de decisão prejudicial deu entrada na Secretaria do Tribunal de Justiça em 2 de agosto de 2018.

20. Apresentaram observações escritas VZ e o., a Académie Fiscale, a LMR, a LDH, a Ordre des barreaux, a Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), os Governos belga, checo, dinamarquês, alemão, estónio, irlandês, espanhol, francês, cipriota, húngaro, neerlandês, polaco, sueco e do Reino Unido e a Comissão.

21. Em 9 de setembro de 2019 realizou-se uma audiência pública conjuntamente com as dos processos apensos C-511/18, C-512/18, La Quadrature du Net e o., e do processo C-623/17, Privacy International, na qual se fizeram representar as partes nos quatro processos de reenvio prejudicial, os Governos acima referidos e do Reino da Noruega, a Comissão e a Autoridade Europeia para a Proteção de Dados (AEPD).

IV. Apreciação

22. A primeira questão do presente reenvio coincide, em substância, com as que estão em causa nos processos apensos C-511/18 e C-512/28, La Quadrature du Net e o. Distingue-se, todavia, destas últimas quanto aos objetivos prosseguidos pela legislação nacional: não apenas a luta contra o terrorismo e contra as formas mais graves de criminalidade, ou a salvaguarda da segurança nacional, mas também «a defesa do território, a segurança pública, a investigação, a deteção e a instauração de procedimento criminal em relação a factos não constitutivos de criminalidade grave» e, de um modo geral, qualquer dos previstos no artigo 23.º, n.º 1, do Regulamento 2016/679.

23. A segunda questão vem no seguimento da primeira, mas completa-a na medida em que questiona se as obrigações positivas que competem ao poder público no que respeita à investigação e repressão do abuso sexual de menores justificam as medidas impugnadas.

24. A terceira questão é formulada para o caso de a legislação nacional ser incompatível com o direito da União. O órgão jurisdicional de reenvio pretende saber se, nessa hipótese, poderá manter provisoriamente os efeitos da Lei de 29 de maio de 2016.

25. Abordarei estas questões analisando, em primeiro lugar, a aplicabilidade da Diretiva 2002/58, para o que remeto para as minhas conclusões noutros destes processos de reenvio prejudicial. Em segundo lugar, irei apresentar as principais orientações jurisprudenciais do Tribunal de Justiça nesta matéria e as suas possibilidades de desenvolvimento. Por último, abordarei a resposta a dar a cada uma das questões prejudiciais.

Aplicabilidade da Diretiva 2002/58

26. Como nos outros três processos de reenvio prejudicial, também neste foi posta em causa a aplicabilidade da Diretiva 2002/58. Tendo em conta o caráter idêntico das abordagens dos Estados-Membros a este respeito, remeto sobre este ponto para as Conclusões dos processos apensos C-511/18 e C-512/18 [15], La Quadrature du Net e o.

Jurisprudência do Tribunal de Justiça sobre a conservação e aceso das autoridades públicas aos dados pessoais no âmbito da Diretiva 2002/58

Princípio da confidencialidade das comunicações e dos respetivos dados

27. As disposições da Diretiva 2002/58 «especificam e complementam» a Diretiva 95/46/CE [16] a fim de assegurar um elevado nível de proteção dos dados pessoais, no âmbito da prestação de serviços de comunicações eletrónicas [17].

28. O artigo 5.º, n.º 1, da Diretiva 2002/58 refere que os Estados-Membros devem garantir, na sua legislação nacional, a confidencialidade das comunicações realizadas através de uma rede pública de comunicações e dos serviços de comunicações eletrónicas publicamente disponíveis, bem como a confidencialidade dos respetivos dados de tráfego.

29. A confidencialidade das comunicações implica, nomeadamente (artigo 5.º, n.º 1, segundo período, da Diretiva 2002/58), a proibição do armazenamento de dados de tráfego relativos a comunicações eletrónicas, por pessoas que não os utilizadores, sem o consentimento destes. São objeto de derrogação «as pessoas legalmente autorizadas […] e o armazenamento técnico que é necessário para o envio de uma comunicação» [18].

30. Os artigos 5.º, 6.º e 9.º, n.º 1, da Diretiva 2002/58 visam garantir a confidencialidade das comunicações e dos dados correspondentes e reduzir ao mínimo o risco de abuso. O seu alcance deve ser apreciado à luz do considerando 30 da referida diretiva, nos termos do qual «[o]s sistemas de fornecimento de redes e serviços de comunicações eletrónicas devem ser concebidos de modo a limitar ao *mínimo* o volume necessário de dados pessoais» [19].

31. No que se refere a estes dados, podem distinguir-se:

– Os dados de *tráfego*, cujo tratamento e armazenamento só é autorizado na medida e para o período de tempo necessários para a faturação e comercialização de serviços e para a prestação de serviços de valor acrescentado (artigo 6.º da Diretiva 2002/58). Depois de expirado esse prazo, os dados tratados e armazenados devem ser apagados ou tornados anónimos [20];

15 N.ºs 40 e segs.

16 Diretiva do Parlamento Europeu e do Conselho de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31). V. artigo 1.º, n.º 2, da Diretiva 2002/58. A Diretiva 95/46 foi revogada, com efeitos a partir de 25 de maio de 2018, pelo Regulamento 2016/679. Assim, na medida em que a Diretiva 2002/58 remete para a Diretiva 95/46 ou não preveja regras próprias, é imprescindível ter em conta as disposições desse regulamento (v. artigo 94.º, n.ºs 1 e 2, do Regulamento 2016/679).

17 V. Acórdão Tele2 Sverige e Watson e o., n.ºs 82 e 83.

18 *Ibidem*, n.º 85 e jurisprudência referida.

19 *Ibidem*, n.º 87. O sublinhado é meu.

20 *Ibidem*, n.º 86 e jurisprudência referida.

– Os dados de *localização* diferentes dos dados de tráfego, que só podem ser tratados sob certas condições e depois de terem sido tornados anónimos ou de se ter obtido o consentimento dos utilizadores ou dos assinantes (artigo 9.º, n.º 1, da Diretiva 2002/58) [21].

Cláusula de limitação prevista no artigo 15.º, n.º 1, da Diretiva 2002/58

32. O artigo 15.º, n.º 1, da Diretiva 2002/58 permite aos Estados-Membros «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» dessa diretiva.

33. Qualquer restrição deve constituir «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]».

34. Tal enumeração de objetivos reveste um caráter exaustivo [22]: a título de exemplo («designadamente»), podem ser adotadas «medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número»;

35. De qualquer forma, «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». Por conseguinte, o artigo 15.º, n.º 1, da Diretiva 2002/58 deve ser interpretado à luz dos direitos fundamentais garantidos pela Carta [23].

36. Dos direitos consagrados na Carta, o Tribunal de Justiça referiu, no que ora interessa, o direito ao respeito da vida privada (artigo 7.º), o direito à proteção dos dados pessoais (artigo 8.º) e o direito à liberdade de expressão (artigo 11.º) [24].

37. O Tribunal de Justiça também sublinhou, como referência para a sua interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, que as restrições à obrigação de garantir a confidencialidade das comunicações e dos respetivos dados de tráfego devem ser interpretadas em sentido estrito.

38. Concretamente, recusou «que a exceção a essa obrigação de princípio e, em especial, a proibição de armazenar esses dados, prevista no artigo 5.º desta diretiva, se converta na regra, sob pena de esvaziar em grande medida esta última disposição do seu alcance» [25].

39. Esta dupla observação parece-me decisiva para compreender por que razão o Tribunal de Justiça considerou incompatível com a Diretiva 2002/58 a conservação generalizada e indiferenciada dos dados de tráfego e de localização relativos às comunicações eletrónicas.

21 *Ibidem, n.º* 86 *in fine*.

22 *Ibidem*, n.º 90.

23 *Ibidem*, n.º 91 e jurisprudência referida.

24 *Ibidem*, n.º 93 e jurisprudência referida.

25 *Ibidem*, n.º 89.

40. Com esta declaração, o Tribunal de Justiça mais não fez do que aplicar «rigorosamente» [26] o critério de proporcionalidade já anteriormente utilizado [27]: «a proteção do direito fundamental ao respeito da vida privada a nível da União exige que as derrogações e as limitações à proteção dos dados pessoais operem na estrita medida do necessário» [28].

Proporcionalidade na conservação dos dados

Caráter desproporcionado de uma conservação generalizada e indiferenciada

41. O Tribunal de Justiça reconheceu que a luta contra a criminalidade grave, designadamente a criminalidade organizada e o terrorismo, assume primordial importância para garantir a segurança pública e que a sua eficácia pode depender em larga medida da utilização das técnicas modernas de investigação. Acrescentou que, «[n]o entanto, tal objetivo de interesse geral, por muito fundamental que seja, não pode, por si só, justificar que uma medida de conservação como a que foi instituída pela Diretiva 2006/24 seja considerada necessária para efeitos da referida luta» [29].

42. Para determinar se uma medida dessa natureza se limitava ao estritamente indispensável, o Tribunal de Justiça salientou, desde logo, a particular gravidade da sua ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta [30]. Particular gravidade decorrente, justamente, do facto de a legislação nacional prever «uma conservação generalizada e indiferenciada de *todos os dados de tráfego e dos dados de localização de todos os assinantes e utilizadores registados relativos a todos os meios de comunicação eletrónica*, e […] obriga[r] os prestadores de serviços de comunicações eletrónicas a conservarem esses dados *de forma sistemática, contínua e sem nenhuma exceção*» [31].

43. Essa medida provocava uma ingerência na vida dos cidadãos que se reflete nestas considerações do Tribunal de Justiça sobre os efeitos da conservação dos dados.

Esses dados [32]:

– «permitem encontrar e identificar a origem de uma comunicação e o seu destino, determinar a data, a hora, a duração e o tipo de uma comunicação, o equipamento de comunicação dos utilizadores, bem como localizar o equipamento de comunicação móvel» [33];

– «permitem, designadamente, saber quem é a pessoa com a qual um assinante ou um utilizador registado comunicou e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Além disso, permitem saber com que frequência o

26 A utilização deste advérbio no Acórdão Tele2 Sverige e Watson e o., n.º 95, provém do considerando 11 da Diretiva 2002/58.

27 Acórdão Digital Rights Ireland e o., n.º 48: «[T]endo em conta, por um lado, o importante papel desempenhado pela proteção dos dados pessoais na perspetiva do direito fundamental ao respeito da vida privada e, por outro, a amplitude e a gravidade da ingerência neste direito que a Diretiva 2006/24 comporta, o poder de apreciação do legislador da União fica reduzido, havendo que proceder a uma fiscalização estrita».

28 Acórdão Tele2 Sverige e Watson e o., n.º 96 e jurisprudência referida.

29 Acórdão Digital Rights Ireland e o., n.º 51. Nessa mesma linha, o Acórdão Tele2 Sverige e Watson e o., n.º 103.

30 Acórdãos Digital Rights Ireland e o., n.º 65, e Tele2 Sverige y Watson e o., n.º 100.

31 Acórdão Tele2 Sverige e Watson e o., n.º 97. O sublinhado é meu.

32 De entre os quais constam, designadamente, o nome e o endereço do assinante ou do utilizador registado, o número de telefone do chamador e o número chamado, bem como, em relação aos serviços de Internet, um endereço IP.

33 Acórdão Tele2 Sverige e Watson e o., n.º 98.

assinante ou o utilizador registado comunicam com certas pessoas durante um determinado período» [34];

– «são suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais dessas pessoas e os meios sociais que frequentam» [35];

– «fornecem os meios para determinar […] o perfil das pessoas em causa, informação tão sensível, à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações» [36].

44. Além do mais, a ingerência é suscetível de gerar «no espírito das pessoas em causa a sensação de que a sua vida privada é objeto de constante vigilância», pelo facto de «a conservação dos dados ser efetuada sem que os utilizadores dos serviços de comunicações eletrónicas disso sejam informados» [37].

45. Atendendo à gravidade da ingerência, só a luta contra a criminalidade grave pode justificar uma medida de conservação de dados com essas características [38]. No entanto, a referida medida não pode passar a ser regra geral, pois «o sistema implementado pela Diretiva 2002/58 exige que essa conservação dos dados seja a exceção» [39].

46. Além do mais, constata-se a existência de dois aspetos decorrentes do facto de a medida impugnada não prever «nenhuma diferenciação, limitação ou exceção em função do objetivo prosseguido» [40] e «não exig[ir] nenhuma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a segurança pública» [41]:

– Por um lado, a medida afetava «globalmente todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que essas pessoas se encontrem, mesmo indiretamente, numa situação suscetível de justificar um procedimento penal […] Além disso, não prevê nenhuma exceção, pelo que também é aplicável a pessoas cujas comunicações estão sujeitas ao segredo profissional, segundo as regras do direito nacional» [42];

– Por outro lado, «[…] não está limitada a uma conservação que tenha por objeto dados relativos a um 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» [43].

34 *Ibidem*, n.º 98.
35 *Ibidem*, n.º 99.
36 *Ibidem, n.º* 99 *in fine*.
37 *Ibidem*, n.º 100.
38 *Ibidem*, n.º 102.
39 *Ibidem*, n.º 104.
40 *Ibidem*, n.º 105.
41 *Ibidem*, n.º 106.
42 *Ibidem*, n.º 105.
43 *Ibidem*, n.º 106.

47. Nestas condições, a legislação nacional objeto de apreciação excedia os limites do estritamente necessário. Por conseguinte, não se pode considerar justificada numa sociedade democrática, como exige o artigo 15.º, n.º 1, da Diretiva 2002/58, à luz dos artigos 7.º, 8.º e 11.º e do artigo 52.º, n.º 1, da Carta [44].

Viabilidade de uma conservação seletiva dos dados

48. O Tribunal de Justiça admitiu a adequação ao direito da União de uma legislação nacional que «permita, a título preventivo, a *conservação seletiva* dos dados de tráfego e dos dados de localização, para efeitos de luta contra a criminalidade grave» [45].

49. A validade dessa conservação seletiva dos dados depende do facto de ser «limitada ao estritamente necessário, no que se refere às categorias de dados a conservar, aos equipamentos de comunicação visados, às pessoas em causa e à duração de conservação fixada».

50. As linhas que o Acórdão Tele 2 Sverige e Watson e o. fornece para determinar se essas condições se encontram preenchidas não são (talvez não o possam ser) taxativas e são formuladas sobretudo em termos genéricos. Para as respeitar, os Estados-Membros devem:

– prever normas claras e precisas que regulem o âmbito e a aplicação dessa medida de conservação dos dados [46];

– fixar «critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido» [47];

– «basear-se em elementos objetivos que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, de contribuir de uma maneira ou outra para a luta contra a criminalidade grave ou de prevenir um risco grave para a segurança pública» [48].

51. Para exemplificar estes elementos objetivos, o Tribunal de Justiça refere a possibilidade de utilizar um critério geográfico para delimitar o público e as situações potencialmente abrangidas. O recurso a este critério, ao qual se referiram de forma crítica alguns Estados-Membros, não visa, na minha opinião, uma limitação tal que este apareça como o único critério de seleção admissível.

44 *Ibidem*, n.º 107.

45 *Ibidem*, n.º 108. O sublinhado é meu.

46 *Ibidem*, n.º 109. Em especial, deve indicar «em que circunstâncias e em que condições se pode adotar uma medida de conservação dos dados, a título preventivo, garantindo assim que essa medida se limita ao estritamente necessário».

47 *Ibidem*, n.º 110.

48 *Ibidem*, n.º 111.

A proporcionalidade no acesso aos dados

Acórdão Tele2 Sverige e Watson e o.

52. O Tribunal de Justiça aborda o *acesso* das autoridades nacionais aos dados independentemente do alcance da obrigação de conservação imposta aos prestadores de serviços de comunicações eletrónicas, designadamente, do caráter generalizado ou específico da conservação desses dados [49].

53. Com efeito, embora a lógica da conservação seja facilitar o acesso posterior aos dados, uma e outro podem originar diferentes violações dos direitos fundamentais consagrados na Carta. Essa distinção não implica, todavia, que algumas das considerações relativas à conservação não sejam também aplicáveis ao acesso aos dados conservados.

54. Nesse sentido, o acesso:

– «deve responder efetiva e estritamente a um desses objetivos» constantes do artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58. Também deve existir uma correspondência entre a gravidade da ingerência e o objetivo prosseguido. Se a ingerência for qualificada de grave, só pode ser justificada pela luta contra a criminalidade grave [50];

– Só pode ser autorizado dentro dos limites do estritamente necessário [51]. Além disso, as medidas legislativas devem prever «normas claras e precisas que indiquem em que circunstâncias e em que condições os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes acesso aos dados. Do mesmo modo, uma medida desta natureza deve também ser vinculativa em direito interno» [52];

– Mais concretamente, a regulamentação nacional deve prever «as condições materiais e processuais que regulam o acesso das autoridades nacionais competentes aos dados conservados» [53].

55. Pode concluir-se do exposto que «um acesso generalizado a todos os dados conservados, independentemente de uma qualquer relação, no mínimo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário» [54].

56. Segundo o Tribunal de Justiça, «a regulamentação nacional em causa deve basear-se em critérios objetivos para definir as circunstâncias e as condições nas quais deve ser concedido às autoridades nacionais competentes o acesso aos dados dos assinantes ou dos utilizadores registados» [55]. A este respeito, «só poderá, em princípio, ser concedido acesso, em relação com o objetivo da luta contra a criminalidade *aos dados de pessoas suspeitas de terem planeado, de estarem a cometer ou de terem cometido uma infração grave ou ainda de estarem envolvidas de uma maneira ou de outra numa infração deste tipo*» [56].

49 *Ibidem*, n.º 113.

50 *Ibidem*, n.º 115.

51 *Ibidem*, n.º 116.

52 *Ibidem*, n.º 117.

53 *Ibidem*, n.º 118.

54 *Ibidem*, n.º 119.

55 *Idem.*

56 *Idem*. O sublinhado é meu.

57. Por outras palavras, as disposições nacionais que concedem às autoridades nacionais competentes o acesso aos dados conservados devem ter um alcance suficientemente limitado. Tem de existir um vínculo entre as pessoas visadas e o objetivo prosseguido, de modo a que o acesso não venha a abranger um número significativo de pessoas ou, inclusivamente, todas as pessoas, todos os meios de comunicação eletrónica e todos os dados armazenados.

58. No entanto, estas regras podem ser mitigadas em determinadas circunstâncias. O Tribunal de Justiça prevê «situações específicas, como aquelas em que os interesses vitais da segurança nacional, da defesa ou da segurança pública estejam ameaçados por atividades terroristas». Nessas situações, «pode também ser concedido acesso aos dados de outras pessoas quando existam elementos objetivos que permitam considerar que esses dados podem, num caso concreto, trazer uma contribuição efetiva para a luta contra essas atividades» [57].

59. Este esclarecimento do Tribunal de Justiça permite que os Estados-Membros instaurem um regime específico de acesso aos dados mais amplo, quando seja excecionalmente necessário para combater as ameaças aos interesses primordiais do Estado (a segurança nacional, a defesa e a segurança pública) [58], de forma a abranger mesmo as pessoas que apenas têm uma ligação indireta a esses riscos.

60. O acesso das autoridades nacionais aos dados armazenados, seja qual for a respetiva natureza, deve preencher três condições:

– Estar sujeito, «em princípio, salvo em casos de urgência devidamente justificados, […] a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente». A decisão desse órgão jurisdicional ou dessa entidade deve ser adotada «na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal» [59];

– Que «as autoridades nacionais competentes às quais foi concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível de comprometer as investigações levadas a cabo por essas autoridades» [60];

– Os Estados-Membros devem adotar regras relativas à segurança e à proteção dos dados conservados pelos prestadores de serviços de comunicações eletrónicas, a fim de evitar o uso indevido e o acesso ilícito aos dados [61].

Acórdão Ministério Fiscal

61. Nesse processo, colocou-se a questão de saber se era compatível com o artigo 15.º, n.º 1, da Diretiva 2002/58, interpretado à luz dos artigos 7.º e 8.º da Carta, uma disposição nacional que prevê o acesso das autoridades competentes aos dados relativos à identificação civil dos titulares de determinados cartões SIM.

57 *Idem.*

58 Além das atividades terroristas, esse caráter excecional podia ser justificado por outras eventualidades, como um ataque informático em grande escala contra infraestruturas sensíveis do Estado ou uma ameaça relacionada com a proliferação nuclear.

59 Acórdão Tele2 Sverige e Watson e o., n.º 120.

60 *Ibidem*, n.º 121.

61 *Ibidem*, n.º 122.

62. O Tribunal de Justiça declarou que o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 não limita o objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais à luta contra as infrações graves, mas visa as «infrações penais» em geral [62].

63. Acrescentou que, para justificar o acesso aos dados por parte das autoridades nacionais competentes, deve existir uma correspondência entre a gravidade da ingerência e a gravidade das infrações em questão. Assim:

– Uma «ingerência grave só pode ser justificada […] por um objetivo de luta contra a criminalidade, devendo também esta ser qualificada de "grave"» [63];

– Em contrapartida, «quando a ingerência que esse acesso implica não for grave, o referido acesso é suscetível de ser justificado por um objetivo de prevenção, de investigação, de deteção e de repressão de "infrações penais" em geral» [64].

64. Partindo dessa premissa, e contrariamente ao que acontecia no Acórdão Tele2 Sverige e Watson e o., o Tribunal de Justiça não qualificou de «grave» a ingerência nos direitos consagrados nos artigos 7.º e 8.º da Carta, pois o pedido de acesso tem «por único objetivo identificar os titulares dos cartões SIM ativados durante um período de 12 dias, com o código IMEI do telemóvel roubado» [65].

65. Para evidenciar a menor gravidade da ingerência, explicou que «os dados visados pelo pedido de acesso em causa no processo principal permitem apenas associar, durante um determinado período, o cartão ou os cartões SIM ativados no telemóvel roubado à identidade civil dos titulares desses cartões SIM. Sem um cruzamento com os dados relativos às comunicações efetuadas com os referidos cartões SIM e os dados de localização, esses dados não permitem conhecer a data, a hora, a duração e os destinatários das comunicações efetuadas com o ou os cartões SIM em causa, nem os locais onde essas comunicações tiveram lugar ou a frequência destas com determinadas pessoas durante um dado período. Os referidos dados não permitem, assim, tirar conclusões precisas a respeito da vida privada das pessoas cujos dados estão em causa» [66].

66. No processo resolvido pelo Acórdão Ministério Fiscal não se questionava se os dados pessoais objeto de acesso tinham sido conservados pelos prestadores de serviços de comunicações eletrónicas em conformidade com os requisitos previstos no artigo 15.º, n.º 1, da Diretiva 2002/58, interpretados à luz dos artigos 7.º e 8.º da Carta [67]. Também não foi abordada a questão de saber se cumpriam ou não os restantes requisitos de acesso decorrentes daquele artigo.

67. Por este motivo, a leitura do Acórdão Ministério Fiscal não permite deduzir qualquer alteração na jurisprudência do Tribunal de Justiça sobre a incompatibilidade com o direito da União de um regime nacional que autoriza o armazenamento generalizado e indiferenciado dos dados, no sentido do Acórdão Tele2 Sverige e Watson e o.

62 Acórdão Ministério Fiscal, n.º 53.

63 *Ibidem*, n.º 56.

64 *Ibidem*, n.º 57.

65 *Ibidem*, n.º 59. Tratava-se do acesso «aos números de telefone correspondentes aos cartões SIM ativados com o código IMEI do telemóvel roubado e aos dados relativos à identidade civil dos titulares desses cartões, tais como o seu apelido, o nome próprio e, sendo caso disso, o endereço, excluindo os dados relativos às comunicações efetuadas com os referidos cartões SIM e os dados de localização relativos ao telemóvel roubado».

66 *Ibidem*, n.º 60.

67 Acórdão Ministério Fiscal, n.º 49.

68. Creio, todavia, que o Tribunal de Justiça, reconhecendo a validade do regime de acesso limitado a determinados dados pessoais (os relativos à identidade civil dos titulares de cartões SIM), aceita implicitamente a conservação desses mesmos dados pelos prestadores do serviço.

Principais críticas à jurisprudência do Tribunal de Justiça

69. Tanto o órgão jurisdicional de reenvio como a maioria dos Estados-Membros que apresentaram observações pedem ao Tribunal de Justiça que esclareça, mitigue ou até reconsidere vários aspetos da sua jurisprudência nesta matéria, sobre a qual fazem incidir as suas críticas.

70. A maior parte dessas críticas, veladas ou frontais, já foram expressas a respeito do Acórdão Digital Rights Ireland e o. e foram rejeitadas no Acórdão Tele 2 Sverige e Watson e o. Surgem novamente agora para evidenciar, em síntese, que seriam suficientes algumas normas rigorosas sobre o acesso aos dados detidos pelos prestadores de serviços de comunicações eletrónicas, que pudessem compensar, de certo modo, a gravidade da ingerência que representa a conservação generalizada e indiferenciada desses mesmos dados.

71. Algumas dessas críticas também sublinham a necessidade de adotar medidas realmente eficazes na luta contra as ameaças graves à segurança e contra a criminalidade em geral, e pedem ao Tribunal de Justiça que tenha em conta o direito à segurança (artigo 6.º da Carta), bem como a margem de apreciação dos Estados-Membros para salvaguardar a segurança nacional. Eventualmente, acresce o facto de o Tribunal de Justiça não ter ponderado o caráter preventivo da intervenção dos serviços de informações e de segurança.

Apreciação dessas críticas e dos aperfeiçoamentos suscetíveis de ser introduzidos na jurisprudência do Tribunal de Justiça

72. Na minha opinião, o Tribunal de Justiça devia manter a posição de princípio que consagrou nos seus acórdãos anteriores: uma obrigação generalizada e indiferenciada de conservar todos os dados de tráfego e os dados de localização de todos assinantes e utilizadores registados viola desproporcionalmente os direitos fundamentais consagrados nos artigos 7.º, 8.º e 11.º da Carta.

73. *A sensu contrario*, uma legislação nacional que estabelecesse restrições adequadas à conservação de alguns desses dados, gerados no âmbito da prestação de serviços de comunicações eletrónicas, poderia ser compatível com o direito da União. O cerne da questão está, assim, na *conservação limitada* desses dados.

74. Pelas razões que passo a expor, essa conservação limitada não deve ser apenas a que tem por objeto uma zona geográfica ou uma categoria concreta de pessoas: os debates sobre esses critérios de conservação revelam que tanto podem ser irrealizáveis, ou ineficazes para os fins que se pretendem, como converterem-se mesmo numa fonte de discriminação.

75. Desde logo, não concordo com a argumentação crítica que defende o binómio «conservação mais extensa em contrapartida de um acesso mais limitado». O entendimento do Tribunal de Justiça, com o qual estou de acordo, é que a conservação e o acesso aos dados constituem dois tipos diferentes de ingerência. Mesmo que a conservação de dados faça sentido tendo em vista um eventual acesso posterior das autoridades competentes, cada uma dessas ingerências deve ser justificada separadamente, através de uma análise específica à luz do objetivo prosseguido.

76. Assim, um sistema nacional que preveja o armazenamento generalizado e indiferenciado de dados não pode justificar-se com base no facto de, simultaneamente, as respetivas normas consagrarem requisitos rigorosos, materiais e processuais, para o acesso a esses dados.

77. Devem existir, pois, normas especificamente relacionadas com a conservação de dados que a sujeitem a algumas condições para evitar o seu caráter generalizado e indiferenciado. Só assim ficará garantida a sua compatibilidade com o artigo 15.º, n.º 1, da Diretiva 2002/58, à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta.

78. Esta é, além do mais, a abordagem adotada pelos grupos de trabalho reunidos no âmbito do Conselho para definir normas de conservação e acesso compatíveis com a jurisprudência do Tribunal de Justiça, analisando em paralelo os dois tipos de ingerência [68].

79. Ao aplicar limitações a cada um desses dois tipos de ingerências, pode avaliar-se se o seu eventual efeito cumulativo, combinado com garantias sólidas, é suficiente para mitigar o impacto da conservação de dados nos direitos fundamentais consagrados nos artigos 7.º, 8.º e 11.º da Carta, além de assegurar a eficácia das investigações.

80. Para proteger esses direitos, o sistema deve:

– Prever uma conservação de dados com determinadas limitações e diferenças em função do objetivo prosseguido;

– Regular o acesso a esses dados apenas na medida estritamente necessária para o fim prosseguido e sob o controlo de um tribunal ou de uma autoridade administrativa independente.

81. A justificação de os prestadores de serviços de comunicações eletrónicas conservarem determinados dados, e não apenas para a gestão das suas obrigações contratuais com o utilizador, aumenta paralelamente à evolução tecnológica. Admitindo que essa conservação seja útil para prevenir e combater a criminalidade (o que é de difícil refutação [69]) não pareceria lógico circunscrever o respetivo alcance à mera exploração dos dados conservados pelos operadores para levarem a cabo a suas atividades comerciais e só durante o tempo necessário para essas atividades.

82. Uma vez reconhecida a utilidade de uma obrigação de conservação de dados para salvaguardar a segurança nacional e lutar contra a criminalidade, além da que os operadores podem levar a cabo para as suas necessidades técnicas e comerciais, é indispensável definir os contornos dessa obrigação.

[68] Os Estados-Membros participam desde 2017 num grupo de trabalho cuja finalidade consiste em adequar as suas legislações aos critérios fixados na jurisprudência do Tribunal de Justiça sobre esta matéria [Groupe Échange d'informations et protection des données (DAPIX)].

[69] De qualquer forma, a determinação das técnicas de investigação e a apreciação da sua eficácia enquadram-se na margem de apreciação dos Estados-Membros.

83. Cada regime de conservação deve ser estritamente adaptado à finalidade prosseguida, de modo a que não possa transformar-se numa conservação indiferenciada [70]. Além disso, deve excluir a possibilidade de a soma desses dados proporcionar um *retrato* da pessoa em causa (isto é, das suas atividades habituais e das suas relações sociais) próximo ou semelhante ao que seria obtido conhecendo o conteúdo das comunicações.

84. Para esclarecer alguns mal-entendidos e determinados equívocos, é importante ter em conta o que o Tribunal de Justiça *não declarou* nos seus Acórdãos Digital Rigths Ireland e o. e Tele2 Sverige e Watson e o. Não se censurou aí a existência, enquanto tal, de um regime de conservação de dados como instrumento útil na luta contra a criminalidade. Pelo contrário, foi reconhecida a legitimidade do objetivo de prevenir e reprimir os atos criminosos, bem como a utilidade de um regime de conservação de dados para conseguir esse objetivo.

85. O que, repito, então se rejeitou, e firmemente, é que a União ou os seus Estados-Membros pudessem, invocando esse objetivo, impor a conservação indiferenciada de *todos* os dados gerados no âmbito da prestação de serviços de comunicações eletrónicas e o acesso generalizado a esses dados.

86. Por conseguinte, é necessário encontrar formas de conservação dos dados que a afastem dos qualificativos («generalizada e indiferenciada») incompatíveis com a proteção exigida pelos artigos 7.º, 8.º e 11.º da Carta.

87. Uma dessas modalidades seria a conservação *seletiva* de dados, relativos quer a um público específico (em teoria, o que apresentasse determinados vínculos, mais ou menos diretos, com as ameaças mais graves) quer a uma zona geográfica determinada.

88. No entanto, esta abordagem apresenta algumas dificuldades:

– A identificação de um grupo de potenciais agressores será provavelmente insuficiente se estes utilizarem técnicas de anonimização ou falsificarem a sua identidade. A escolha desses grupos pode levar, além do mais, a instaurar um regime de suspeição geral sobre alguns segmentos da população e ser considerada discriminatória, em função do algoritmo utilizado;

– A seleção mediante critérios geográficos (que, para ser eficaz, não pode incidir sobre áreas muito reduzidas) suscita esses mesmos problemas e acrescenta outros, como referiu na audiência a Autoridade Europeia para a Proteção de Dados, na medida em que pode levar a estigmatizar certas zonas.

89. Além disso, pode existir uma certa contradição entre o caráter preventivo da conservação destinada a um público específico ou a uma zona geográfica e o facto de não se conhecerem antecipadamente os autores dos crimes, nem sequer o local e o momento da sua prática.

90. De qualquer maneira, importa não excluir que se encontrem fórmulas de conservação seletiva baseadas nesses critérios, que sejam úteis para atingir os objetivos já expostos. Cabe ao poder legislativo, em cada um dos Estados-Membros ou para toda a União, conceber essas fórmulas, conformes com a proteção dos direitos fundamentais que o Tribunal de Justiça salvaguarda.

[70] Acórdão Digital Rights Ireland e o., n.º 57, e Acórdão Tele2 Sverige e Watson e o., n.º 105.

91. Seria um erro acreditar que a conservação seletiva de dados pertencentes a um público específico ou a uma zona geográfica determinada é a única fórmula que o Tribunal de Justiça considera compatível com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º e 8.º da Carta.

92. É possível, insisto, encontrar outras modalidades de conservação seletiva de dados, além das centradas em grupos específicos de pessoas ou áreas geográficas. De facto, assim o entenderam os grupos de trabalho do Conselho aos quais me referi anteriormente: consideraram, em particular, como meios de exploração, a limitação das categorias de dados conservados [71], a pseudonimização dos dados [72], a previsão de períodos de conservação limitados [73], a exclusão de determinadas categorias de prestadores de serviços de comunicações eletrónicas [74], as autorizações de armazenamento renováveis [75], a obrigação de conservar os dados armazenados dentro da União ou o controlo sistemático e periódico por parte de uma autoridade administrativa independente das garantias oferecidas pelos prestadores de serviços de comunicações eletrónicas contra a utilização indevida dos dados.

93. Na minha opinião, para ser compatível com a jurisprudência do Tribunal de Justiça, deve dar-se preferência a uma conservação temporária de algumas *categorias* de dados de tráfego e de localização, limitadas em função de estritas necessidades de segurança, que não permitam, no seu conjunto, obter uma imagem específica e detalhada da vida das pessoas em causa.

94. Na prática, isto significa que, em relação às duas categorias principais (dados de tráfego e dados de localização) devem apenas conservar-se, com os filtros adequados, os dados *mínimos* que se considerem absolutamente imprescindíveis para a prevenção e o controlo eficazes da criminalidade e para salvaguardar a segurança nacional.

95. Cabe aos Estados-Membros ou às instituições da União realizar, por via legislativa (com a colaboração dos seus próprios peritos), este exercício de seleção, abandonando qualquer tentativa de impor um armazenamento generalizado e indiferenciado de todos os dados de tráfego e de localização.

96. Além desta limitação por categorias, os dados conservados só o poderão ser durante um período de armazenamento, para que não permitam proporcionar uma imagem detalhada da vida das pessoas em causa. Esse período de conservação deve, além do mais, ser adequado em

71 Os dados que não sejam estritamente indispensáveis e objetivamente necessários para a prevenção e investigação de infrações penais e a proteção da segurança pública ficarão excluídos da obrigação de conservação. Em particular, será conveniente salientar, de acordo com o objetivo prosseguido, que tipos de dados de assinantes, dados de tráfego e dados de localização devem ser obrigatoriamente conservados para atingir esse objetivo. Em particular, ficarão excluídos os dados que não se considerem imprescindíveis para a investigação e ação penal.

72 Método pelo qual os nomes são substituídos por um pseudónimo, de modo que os dados já não se relacionem com um nome. Contrariamente à anonimização, a pseudonimização permite voltar a relacionar os dados com o nome do interessado.

73 Pode estudar-se a possibilidade de limitar os períodos de conservação em função das diferentes categorias de dados, tendo em conta o seu caráter mais ou menos intrusivo na privacidade das pessoas. Deverá ainda prever-se que os dados sejam eliminados de forma permanente no final do período de conservação.

74 Pode considerar-se a possibilidade de não impor uma obrigação de conservação de dados a todos os prestadores de serviços de comunicações eletrónicas, mas introduzir esta obrigação em função da sua dimensão e do tipo de serviços que ofereçam, excluindo, por exemplo, os que ofereçam serviços altamente especializados.

75 Os sistemas de autorização podem basear-se em avaliações periódicas das ameaças em cada Estado-Membro. Deve garantir-se que o vínculo entre os dados conservados e o objetivo prosseguido seja criado e adaptado à situação específica de cada Estado-Membro. Por conseguinte, será possível que as autorizações de conservação concedidas aos prestadores possa dar lugar à conservação de certos tipos de dados durante um período de tempo determinado, dependendo da avaliação da ameaça. Estas autorizações podem ser dadas por um juiz ou por uma autoridade administrativa independente e darão lugar a um controlo periódico da imprescindibilidade dessa conservação.

função da natureza dos dados, para que os que proporcionem informação mais específica sobre os estilos de vida e os hábitos dessas pessoas sejam armazenados durante um período de tempo mais curto [76].

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

98. A Autoridade Europeia para a Proteção de Dados pronunciou-se neste sentido na audiência: quantas mais categorias de metadados forem armazenadas e mais longo for o período de armazenamento, mais fácil será definir o perfil pormenorizado de uma pessoa, e inversamente [77].

99. Além disso, como também se verificou na audiência, é difícil estabelecer a fronteira entre determinados metadados das comunicações eletrónicas e o conteúdo dessas mesmas comunicações. Alguns metadados podem ser tão ou mais reveladores do que o próprio conteúdo dessas comunicações: é o que pode acontecer com os endereços (URL) das páginas Web visitadas [78]. Por conseguinte, a esse género de dados e a outros idênticos deve ser prestada uma atenção especial para limitar ao máximo a necessidade da sua conservação e a duração desta.

100. Encontrar uma solução equilibrada não é fácil, uma vez que a técnica de cruzar e correlacionar os dados armazenados permite aos serviços de investigação e vigilância identificar um suspeito ou uma ameaça, consoante o caso. Ainda assim, há uma diferença de grau entre a conservação de dados para detetar esse suspeito ou essa ameaça e a que resulta numa descrição pormenorizada da vida de uma pessoa.

101. Enquanto se aguarda por uma regulamentação comum para toda a União nesta matéria específica, não creio que se possa pedir ao Tribunal de Justiça que assuma funções reguladoras e preveja minuciosamente quais as categorias de dados que se podem conservar e durante quanto tempo. Cabe às instituições da União e aos Estados-Membros, uma vez definidos os limites que, segundo o Tribunal de Justiça, decorrem da Carta, colocar o cursor no lugar correto para conseguir um equilíbrio entre a preservação da segurança e os direitos fundamentais consagrados na Carta.

102. É certo que prescindir das informações extraídas de um maior número de dados conservados pode tornar mais difícil, em alguns casos, a luta contra as potenciais ameaças. Mas esse é um tributo, como outros, que os poderes públicos devem pagar quando impõem a si próprios a obrigação de salvaguardar os direitos fundamentais.

76 Este é, aparentemente, o sistema aplicado na República Federal da Alemanha, cujo Governo referiu na audiência que, nos termos da sua legislação, o prazo de conservação dos dados de tráfego é de dez semanas, ao passo que o prazo de conservação dos dados de localização é de apenas quatro semanas. Pelo contrário, para a República Francesa é imprescindível um período de um ano de armazenamento dos dados de tráfego e de localização. Segundo este Estado-Membro, a redução deste prazo a menos de um ano levaria a reduzir a eficácia dos serviços da Polícia Judiciária.

77 Naturalmente, deve garantir-se que os prestadores de serviços de comunicações eletrónicas eliminem de modo permanente os dados no termo do período de conservação (com exceção dos que possam continuar a armazenar para fins comerciais, em conformidade com a Diretiva 2002/58).

78 Na audiência, o Governo francês alegou que os URL estavam excluídos dos dados de conexão para os quais a sua legislação prevê um dever geral de conservação.

103. Da mesma forma que ninguém preconizaria uma obrigação *ex ante* de conservação generalizada e indiferenciada dos *conteúdos* das comunicações eletrónicas privadas (nem sequer se as leis garantissem o acesso posterior restrito a esses conteúdos), também os metadados dessas comunicações, suscetíveis de revelar informações tão sensíveis como os próprios conteúdos, não podem ser objeto de armazenamento indiferenciado e generalizado.

104. A dificuldade legislativa — que reconheço — de configurar com precisão os casos e as condições em que é necessário efetuar uma conservação seletiva não justifica que os Estados-Membros, fazendo da exceção uma regra, convertam a conservação generalizada de dados pessoais no princípio essencial das suas legislações. Se assim acontecesse, estaria a admitir-se a vigência indefinida de uma importante violação do direito à proteção dos dados pessoais.

105. Importa acrescentar que nada impede que, em situações verdadeiramente *excecionais*, caracterizadas por uma ameaça iminente ou por um risco extraordinário que justifiquem a declaração oficial do estado de emergência num Estado-Membro, a legislação nacional preveja, por um período limitado, a possibilidade de impor uma obrigação de conservação de dados com a amplitude e a generalidade consideradas imprescindíveis.

106. Nessa conjuntura, pode ser aprovada legislação que permita especificamente uma conservação de dados (e o acesso a eles) mais ampla, segundo condições e procedimentos que assegurem a essas medidas um caráter extraordinário, no que respeita ao seu alcance material e ao seu prolongamento no tempo, bem como as correspondentes garantias jurisdicionais.

107. A análise comparada dos regimes jurídicos que regulamentam o estado constitucional de emergência revela que não é impossível definir hipóteses factuais suscetíveis de desencadear a aplicação de um regime jurídico específico, estabelecendo qual a autoridade que pode adotar essa decisão, em que condições e sob que controlo [79].

Respostas específicas às três questões prejudiciais

Consideração preliminar

108. O órgão jurisdicional de reenvio pede uma interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58 relativamente a vários direitos consagrados pela Carta: o direito ao respeito pela vida privada e familiar (artigo 7.º), o direito à proteção de dados pessoais (artigo 8.º) e o direito à liberdade de expressão e de informação (artigo 11.º).

109. Como exponho nas Conclusões dos processos apensos C-511/18 e C-512/18, La Quadrature du Net e o., esses são, com efeito, os direitos que, segundo o Tribunal de Justiça, podem ser afetados nestes casos.

110. No entanto, a Cour constitutionnelle (Tribunal Constitucional) traz igualmente à colação os artigos 4.º e 6.º da Carta, aos quais se referem, respetivamente, a segunda e a primeira questão prejudicial.

[79] Ackerman, B., «The Emergency Constitution», *Yale Law Journal*, vol. 113, 2004, pp. 1029 a 1092; Ferejohn, J., e Pasquino, P., «The Law of the Exception: A typology of Emergency Powers», *International Journal of Constitutional Law*, vol. 2, 2004, pp. 210 a 239.

111. No que respeita ao artigo 6.º da Carta, que consagra o direito à liberdade e à segurança, foi igualmente invocado nos processos apensos C-511/18 e C-512/18, La Quadrature du Net e o., e quanto à sua pertinência pronunciei-me nas correspondentes conclusões, para as quais remeto [80].

112. Quanto ao artigo 4.º da Carta, uma vez que a resposta depende mais da respetiva interpretação do que da apreciação da legislação nacional para a confrontar com o direito da União, julgo oportuno responder-lhe em primeiro lugar.

Segunda questão prejudicial

113. A referência à proibição da tortura e dos tratos ou penas desumanos ou degradantes, consagrada no artigo 4.º da Carta, é, com efeito, exclusiva deste reenvio prejudicial, pelo que é necessário considerá-la.

114. Ao recorrer ao artigo 4.º da Carta, o órgão jurisdicional de reenvio pretende salientar que a legislação nacional também tem por objeto o cumprimento da *obrigação positiva* que recai sobre os poderes públicos de preverem «um quadro legal que permita uma fase de inquérito efetiva e uma repressão efetiva do abuso sexual de menores e que permita efetivamente identificar o autor do crime, mesmo quando são utilizados meios de comunicações eletrónicos» [81].

115. Na minha opinião, essa concreta *obrigação positiva* não é muito diferente de cada um dos deveres específicos em que se traduz, para o Estado, a consagração de um catálogo de direitos fundamentais. Dos direitos à vida (artigo 2.º da Carta), à integridade física (artigo 3.º da Carta) ou à proteção de dados (artigo 8.º da Carta), tal como das liberdades de expressão (artigo 11.º da Carta) ou de pensamento, de consciência e de religião (artigo 10.º da Carta), decorre a obrigação do Estado de prever um quadro legal que garanta o seu gozo efetivo, eventualmente através do uso da força monopolizado pelos poderes públicos, contra quem quer que seja que pretenda impedi-lo ou dificultá-lo [82].

116. Quanto ao abuso sexual de menores, o TEDH entende que as crianças e outras pessoas vulneráveis têm um direito qualificado à proteção do Estado, mediante a adoção de disposições em matéria penal que reprimam eficazmente e com efeito dissuasor a prática desses crimes [83].

117. Este direito qualificado à proteção não se enquadra apenas no artigo 4.º da Carta, podendo naturalmente invocar-se o artigo 1.º (dignidade do ser humano) ou o artigo 3.º (direito à integridade física e psíquica).

80 Conclusões nos processos apensos C-511/18 e C-512/18, La Quadrature du Net e o., n.ºs 95 e segs.

81 Enunciado da segunda questão, *in fine*. Esta alusão aos meios de comunicação eletrónicos explica que a questão mencione a existência de uma segunda *obrigação positiva* que recai sobre os Estados, a imposta pelo artigo 8.º da Carta quanto à proteção de dados pessoais. A dupla referência ao artigo 8.º da Carta revela que o órgão jurisdicional de reenvio atribui aos direitos da Carta, em função da respetiva natureza, uma dupla função: como *limite* da obrigação controvertida e como *justificação* dessa obrigação.

82 Esta obrigação de eficácia traduz-se numa obrigação de resultado para os poderes públicos no Estado social ou providência, em que, além do reconhecimento formal dos direitos, é necessária a realização prática do seu conteúdo material.

83 Acórdão TEDH, 2 de dezembro de 2008, K.U. c. Finlândia (ECHR:2008:1202JUD000287202, § 46).

118. Embora a obrigação positiva dos poderes públicos de garantir a proteção às crianças e a outras pessoas vulneráveis não possa afastar-se na ponderação dos bens jurídicos afetados pela legislação nacional [84], também não se pode traduzir em «cargas não razoáveis» para os poderes públicos [85] nem ser cumprida à margem da lei ou do respeito pelos outros direitos fundamentais [86].

Primeira questão prejudicial

119. O órgão jurisdicional de reenvio pretende saber, em síntese, se o direito da União se opõe à lei nacional sobre a qual deve proferir decisão no âmbito de um recurso de constitucionalidade.

120. Como o Tribunal de Justiça já proporcionou uma interpretação da Diretiva 2002/58 que se adequa às disposições correspondentes da Carta, a resposta à questão prejudicial deve ter em conta a jurisprudência assente no Acórdão Tele2 Sverige e Watson e o., eventualmente com os aperfeiçoamentos que agora se acrescentem.

121. Partindo dessa premissa, as linhas interpretativas que se podem proporcionar à Cour constitutionnelle (Tribunal Constitucional) para que, por si mesma, efetue a fiscalização que lhe permita verificar a conformidade da legislação nacional com o direito da União devem incidir, separadamente, sobre a conservação e sobre o acesso aos dados, tal como se encontram regulamentados na referida legislação nacional.

Condições da conservação dos dados

122. O Governo belga sublinha que pretendia prever um quadro legal claro, que incluísse as garantias necessárias à proteção da privacidade, em vez de se basear na prática dos operadores de serviços de comunicações eletrónicas relativamente à conservação dos dados com vista à faturação e tratamento dos pedidos de informação dos clientes.

123. Para esse Governo, a obrigação geral e preventiva de conservação dos dados não só tem como finalidade a instrução, a investigação e a instauração do procedimento criminal relativamente aos atos de delinquência grave mas também a salvaguarda da segurança nacional, a defesa do território e a segurança pública, a investigação, a deteção e a instauração de procedimento criminal relativamente a atos que não sejam de delinquência grave ou a prevenção da utilização proibida dos sistemas de comunicações eletrónicas [87], ou qualquer outro objetivo identificado no artigo 23.º, primeiro parágrafo, do Regulamento 2016/679.

84 A este respeito, considero que aos direitos invocados pelo órgão jurisdicional de reenvio (como *limites* da obrigação controvertida, não como *justificação* da mesma) podem acrescentar-se o direito à ação (artigo 47.º da Carta) ou os direitos de defesa (artigo 48.º da Carta), cuja eventual violação também foi objeto de debate nos processos principais. No entanto, o dispositivo do despacho de reenvio refere-se apenas aos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta.

85 Acórdão TEDH, 28 de outubro de 1998, Osman c. Reino Unido (CE:ECHR:1998:1028JUD002345294, § 116).

86 *Ibidem*, § 116 *in fine*: «[é necessário] garantir que a polícia exerce o seu poder de repressão e prevenção da criminalidade respeitando integralmente a legalidade e as demais garantias que limitam legitimamente o alcance dos seus atos no âmbito do inquérito penal». V., também, o Acórdão TEDH, 2 de dezembro de 2008, K.U. c. Finlândia (CE:ECHR:2008:1202JUD000287202, § 48). Nesta mesma linha, o Tribunal de Justiça declarou no Acórdão de 29 de julho de 2019, Gambino e Hyka (C-38/18, EU:C:2019:628, n.º 49), que os direitos previstos a favor da vítima de uma infração não podem afetar o gozo efetivo dos direitos reconhecidos ao arguido.

87 Igualmente se justifica para responder a uma chamada feita para um serviço de emergência ou para encontrar uma pessoa desaparecida, cuja integridade física esteja em perigo iminente.

124. Segundo o Governo belga:

– A conservação de dados, como tal, não permite extrair conclusões muito específicas sobre a vida privada das pessoas em causa: a possibilidade de extrair tais conclusões só surgiria na medida em que também se facilitasse o aceso aos dados conservados;

– A lei contém cuidados destinados a proteger a privacidade, nomeadamente, a conservação de dados não afeta o conteúdo das comunicações; as garantias quanto à justificação da conservação, o direito de acesso, o direito de retificação e outros são integralmente aplicáveis; os prestadores de serviços e os operadores devem submeter os dados guardados às mesmas obrigações e medidas de segurança e proteção aplicáveis aos dados na rede, impedindo a sua destruição fortuita ou ilícita, a sua perda ou alteração acidentais;

– Os dados podem ser armazenados durante doze meses (devendo ser destruídos no termo desse período) e apenas em território da União;

– Os prestadores de serviços e os operadores devem aplicar medidas de proteção tecnológica que façam com que os dados conservados, uma vez registados, sejam ilegíveis e inutilizáveis por qualquer pessoa que não tenha autorização para aceder aos mesmos;

– De qualquer forma, estas operações são levadas a efeito sob a supervisão da entidade reguladora belga dos setores postal e de telecomunicações e da Autoridade de proteção de dados.

125. Apesar destas garantias, o certo é que a legislação belga impõe aos operadores e prestadores de serviços de comunicações eletrónicas a obrigação, geral e indiferenciada, de conservarem os dados de tráfego e de localização, na aceção da Diretiva 2002/58, tratados no âmbito da prestação desses serviços. O período de conservação é, em geral, como já se referiu, de doze meses: não se prevê nenhum limite temporal em função das categorias de dados conservados.

126. Esta obrigação de conservação geral e indiferenciada opera de forma permanente e continuada. Mesmo que a sua finalidade seja a prevenção, a investigação e a repressão de todo o tipo de infrações penais (desde as que dizem respeito à segurança nacional, à defesa ou as especialmente graves, até às que são punidas com uma pena de prisão de duração inferior a um ano), uma obrigação com estas características não está em conformidade com a jurisprudência do Tribunal de Justiça, pelo que não se pode considerar compatível com a Carta.

127. Para se adaptar a essa jurisprudência, o legislador belga tem de explorar outras vias (como as que anteriormente mencionei) que instituam modalidades de conservação limitada. Essas modalidades, variáveis consoante as categorias de dados, devem respeitar o princípio de que só se deve conservar o *mínimo* de dados imprescindível, em função do risco ou da ameaça, e por um período de tempo limitado, que dependerá da natureza da informação armazenada. Em todo o caso, a conservação não pode proporcionar uma *cartografia* específica da privacidade, dos hábitos, da conduta ou das relações sociais das pessoas em causa.

Condições de acesso das autoridades públicas aos dados conservados

128. Na minha opinião, as condições referidas no Acórdão Tele2 Sverige e Watson e o.[88] continuam a ser pertinentes também quanto ao acesso: a regulamentação nacional deve prever as condições materiais e processuais que regulam o acesso das autoridades nacionais competentes aos dados conservados[89].

129. O Governo belga especifica que o artigo 126.º, n.º 2, da Lei de 2005[90] prevê de forma restritiva quais as autoridades nacionais que podem receber os dados armazenados nos termos do n.º 1 do mesmo artigo.

130. Entre essas autoridades encontram-se: as judiciais propriamente ditas e o Ministério Público; as forças de segurança do Estado; o Serviço Geral de Informações e Segurança, sob controlo de comissões independentes; os agentes de Polícia Judiciária do Instituto Belga de Correios e Telecomunicações; os serviços de emergência; os agentes de Polícia Judiciária da Divisão de pessoas desaparecidas da polícia federal; o Serviço de Mediação das Telecomunicações e o órgão de supervisão do setor financeiro.

131. Genericamente, o Governo belga afirma que a legislação nacional não permite que os diversos serviços tenham acesso aos dados para exercer a ação penal concreta relativamente a ameaças não identificadas ou sem informações específicas. As autoridades nacionais não podem, assim, aceder indiscriminadamente aos dados das comunicações em bruto e tratá-los automaticamente para obter informações e prevenir ativamente os perigos para a segurança.

132. Segundo o mesmo Governo, o acesso aos dados está sujeito a condições estritas em função do estatuto de cada uma das autoridades nacionais competentes.

133. A resposta à primeira questão prejudicial não exige, na minha opinião, que o Tribunal de Justiça efetue uma apreciação exaustiva das condições aplicáveis para que cada uma dessas autoridades possa obter os dados conservados. É ao órgão jurisdicional de reenvio que incumbe essa tarefa, que deverá ser levada a cabo à luz das orientações da jurisprudência Tele2 Sverige e Watson e o. e Ministério Fiscal.

134. Além disso, segundo a informação disponibilizada pelo Governo belga, há diferenças consideráveis entre as condições de acesso que se aplicam às autoridades judiciais ou ao Ministério Público[91], com a finalidade de investigação, instrução e de repressão das infrações penais, nos termos dos artigos 46bis[92] e 88bis[93] do Código de Processo Penal belga, e as que são aplicáveis a outras autoridades.

88 V. n.º 60 das presentes conclusões.

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

90 Artigo 126.º, na redação dada pela Lei de 29 de maio de 2016.

91 A idoneidade do Ministério Fiscal para ordenar medidas deste tipo é objeto de debate no âmbito do reenvio prejudicial no Processo C-746/18, HK/Prokuratur (Condições de acesso aos dados relativos às comunicações eletrónicas), ainda pendente.

92 O Ministério Público tem competência para exigir aos operadores os dados de identificação, mediante decisão escrita e fundamentada (verbal em casos urgentes), que demonstre a proporcionalidade da medida quanto ao respeito pela privacidade e a sua subsidiariedade relativamente a qualquer outra obrigação de investigação. Para os crimes que não sejam punidos com pena principal de prisão de um ano ou mais grave, o Ministério Público só pode pedir os dados durante um período de seis meses anteriores à sua decisão.

93 Para exigir aos operadores a rastreabilidade das comunicações eletrónicas ou os dados de tráfego e de localização conservados é competente o juiz de instrução, que pode fixar essa medida se houver indícios sérios da prática de um crime punido com determinadas penas, mediante despacho escrito e fundamentado (verbal, em caso de urgência) sujeito às mesmas exigências de proporcionalidade e subsidiariedade aplicáveis ao Ministério Público. Há algumas exceções quando a medida visa determinadas categorias profissionais protegidas (advogados ou médicos, por exemplo).

135. Quanto aos serviços de informações e segurança, nos termos da Lei de 1998, o pedido de acesso aos dados de tráfego e de localização em poder dos operadores deve basear-se em critérios objetivos para garantir que se limita ao estritamente necessário, na sequência de uma ameaça previamente identificada [94]. São previstos diversos prazos de acesso (seis, nove ou doze meses) em função da ameaça potencial e o pedido deve respeitar os princípios da proporcionalidade e da subsidiariedade. Contudo, foi instituído um mecanismo de controlo a cargo de uma autoridade independente [95].

136. Quanto aos agentes da Polícia Judiciária do Instituto Belga de Correios e Telecomunicações (BIPT), têm a possibilidade de aceder aos dados em poder dos operadores de telecomunicações sob a supervisão do Ministério Público, em casos concretos muito limitados [96], sem que, segundo o Governo belga, a sua atividade atinja as pessoas cujos dados se conservam.

137. Quanto aos serviços de emergência que prestem assistência *in situ*, podem pedir os dados do autor de uma chamada de emergência quando, após a receção desta, não obtenham do prestador de serviços ou do operador os dados de identificação da referida pessoa ou quando estes sejam incompletos ou incorretos.

138. Quanto aos agentes de Polícia Judiciária afetos à Divisão de pessoas desaparecidas da Polícia Federal, podem pedir ao operador os dados necessários para localizar um desaparecido cuja integridade física esteja em perigo iminente. O acesso, sujeito a condições estritas, é limitado aos dados que permitam identificar o utilizador e aos relativos ao acesso e ligação dos terminais à rede e ao serviço, bem como à localização desses equipamentos, circunscrevendo-se aos armazenados nas 48 horas imediatamente anteriores ao pedido.

139. Quanto ao Serviço de Mediação para as Telecomunicações, só pode pedir os dados de identificação da pessoa que tenha usado indevidamente uma rede ou um serviço de comunicações eletrónicas. Não existe, neste caso, um controlo prévio por uma autoridade judiciária ou administrativa independente (autónoma em relação ao próprio serviço).

140. Por último, visando a luta contra a criminalidade financeira, a autoridade de supervisão do setor financeiro pode requerer o acesso aos dados de tráfego e de localização, estando sujeita a autorização prévia do juiz de instrução.

141. A exposição destas modalidades e condições de acesso aos dados conservados, aplicáveis a cada uma das autoridades habilitadas a obtê-los, revela a existência de uma diversidade de casos e exceções, cuja conformidade pormenorizada com os critérios utilizados pelo Tribunal de Justiça na sua jurisprudência [97] cabe ao órgão jurisdicional de reenvio apreciar.

94 A decisão especificará, consoante os casos, as pessoas singulares ou coletivas, as associações de facto ou grupos, os objetos, os locais, os eventos ou as informações sujeitas ao método específico. Deve igualmente mencionar a relação entre a finalidade dos dados pedidos e a ameaça potencial que justifica especialmente este método.

95 A Comissão administrativa para a supervisão de métodos específicos e excecionais de recolha de dados pelos serviços de informações e segurança (Comissão BIM) e o Comité permanente para a fiscalização dos serviços de informações (Comité R). O Governo belga declara que a Comissão BIM é responsável pelo acompanhamento dos métodos de pesquisa utilizados pelos serviços de informações e segurança, sobre os quais exerce um controlo de primeira linha. Esta comissão, composta por juízes, leva a efeito os seus trabalhos com total independência. É igualmente estabelecido um controlo independente de segunda linha a cargo do Comité R.

96 O acesso é permitido para a investigação, instrução e repressão das infrações previstas nos artigos 114.º (segurança das redes), 124.º (confidencialidade das comunicações eletrónicas) e 126.º (conservação de dados e acesso) da Lei de 13 de junho de 2005 relativa às Comunicações Eletrónicas.

97 Remeto para o n.º 60 das presentes conclusões.

142. Observo, por exemplo, que, no âmbito da legislação impugnada, não é mencionado o dever de as autoridades nacionais competentes informarem sistematicamente as pessoas em causa (a não ser que essa informação comprometa o decurso do inquérito) de que seus dados foram consultados. Também não parece que se estabeleçam, pelo menos em alguns casos, como os relativos às infrações financeiras, quaisquer regras predeterminadas sobre a gravidade destas, para justificar o acesso aos dados correspondentes. A relação entre a intensidade da ingerência e a gravidade do crime investigado, na aceção do Acórdão Ministério Fiscal, não é evidente em todos os casos.

143. De qualquer modo, creio que as considerações relacionadas com o acesso das autoridades aos dados passam para um segundo plano quando, atento o que já foi exposto, a principal razão pela qual a legislação nacional objeto do presente reenvio não está em conformidade com o direito da União é a própria conservação generalizada e indiferenciada desses dados.

Terceira questão prejudicial

144. A Cour constitutionnelle (Tribunal Constitucional) pretende saber se, no caso de, à luz da resposta do Tribunal de Justiça, se declarar que a legislação nacional é incompatível com o direito da União, pode manter provisoriamente os efeitos dessa legislação. Seria assim evitada a insegurança jurídica e permitir-se-ia que os dados recolhidos e conservados pudessem continuar a ser utilizados ao serviço dos objetivos prosseguidos.

145. É jurisprudência assente que «apenas o Tribunal de Justiça pode, a título excecional e com base em considerações imperiosas de segurança jurídica, conceder uma suspensão provisória do efeito de exclusão exercido por uma norma de direito da União relativamente ao direito nacional a ela contrário». Se «os órgãos jurisdicionais nacionais pudessem, ainda que a título provisório, dar primazia sobre o direito da União a disposições nacionais a ele contrárias, ficaria comprometida a aplicação uniforme do direito da União» [98].

146. A Comissão entende que, como o Tribunal de Justiça não limitou no tempo os efeitos da interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, a resposta a esta questão do órgão jurisdicional de reenvio deve ser negativa [99].

147. No entanto, no Acórdão de 28 de fevereiro de 2012, Inter-Environnement Wallonie e Terre wallonne [100], o Tribunal de Justiça afirmou que, tendo em conta a existência de uma consideração imperiosa ligada à proteção do ambiente, um órgão jurisdicional nacional pode ser excecionalmente autorizado a fazer uso da sua disposição nacional que lhe permita manter certos efeitos de um ato nacional anulado por violação de uma norma do direito da União [101].

98 Acórdão de 28 de julho de 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, n.º 33).

99 N.º 100 das observações escritas da Comissão.

100 C-41/11, EU:C:2012:103.

101 Acórdão de 28 de fevereiro de 2012, Inter-Environnement Wallonie e Terre wallonne (C-41/11, EU:C:2012:103, n.º 58). No n.º 34 do Acórdão de 28 de julho de 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603), o Tribunal de Justiça inferiu dessa afirmação que «pretendeu […] casuisticamente e a título excecional, reconhecer a um órgão jurisdicional nacional a faculdade de fixar os efeitos de uma disposição nacional considerada incompatível com o direito da União».

148. Esta linha jurisprudencial foi confirmada pelo Acórdão de 29 de julho de 2019, Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen [102]. Adotada no âmbito da proteção do ambiente ou baseada na segurança do fornecimento de eletricidade, não encontro motivos para excluir a sua aplicação noutros domínios do direito da União, em especial no que aqui se encontra em apreço.

149. Se uma «consideração imperiosa ligada à proteção do ambiente» pode justificar que, excecionalmente, os tribunais nacionais preservem determinados efeitos de uma disposição nacional incompatível com o direito da União, isso fica a dever-se ao facto de a proteção do ambiente representar «um dos objetivos essenciais da União e te[r] caráter transversal e fundamental» [103].

150. Ora, entre os objetivos da União conta-se também a constituição de um espaço de segurança (artigo 3.º TUE), que inclui o respeito pelas funções essenciais do Estado, nomeadamente as que se destinam a manter a ordem pública e a salvaguardar a segurança nacional (artigo 4.º TUE, n.º 2). Este objetivo não é menos «transversal e fundamental» do que a proteção do ambiente, uma vez que a sua realização é a condição necessária para a instauração de um quadro legal capaz de garantir o gozo efetivo dos direitos e liberdades fundamentais.

151. Na minha opinião, razões imperiosas relacionadas com a proteção da segurança nacional podem justificar, neste processo, que o Tribunal de Justiça autorize, excecionalmente, o órgão jurisdicional de reenvio a manter, pelo menos, alguns dos efeitos da lei impugnada.

152. Essa subsistência exigirá que o órgão jurisdicional de reenvio, à luz da decisão do Tribunal de Justiça, considere a disposição nacional incompatível com o direito da União e julgue incomensuravelmente perturbadoras as repercussões que, para a segurança pública ou a segurança do Estado, possa ter a sua anulação imediata (caso a anulação fosse, no direito nacional, a consequência dessa incompatibilidade) ou a sua inaplicabilidade.

153. A subsistência provisória (total ou parcial) dos efeitos da disposição nacional dependerá ainda do seguinte:

– que a finalidade dessa prorrogação seja evitar uma lacuna de efeitos tão perniciosos como os decorrentes da aplicação da regulamentação impugnada, lacuna impossível de superar por outros meios e que implica privar as autoridades nacionais de um instrumento valioso para a garantia da segurança do Estado; e

– que se mantenha apenas pelo tempo estritamente necessário para adotar as medidas que permitam sanar a referida incompatibilidade com o direito da União [104].

154. Além do mais, advogam no sentido desta solução a dificuldade que representa adaptar as legislações nacionais à jurisprudência estabelecida no processo Tele2 Sverige e Watson e o. [105] e o facto de a vontade de o legislador belga expressar dar cumprimento ao Acórdão Digital Rights Ireland e o. ser evidenciada ao alterar a sua própria legislação. Este precedente leva a pensar que irá igualmente adequar a Lei de 29 de maio de 2016 (adotada antes da publicação do Acórdão Tele2 Sverige e Watson e o.) à jurisprudência assente neste último.

102 C-411/17, EU:C:2019:622 (n.º 178).

103 Acórdão de 28 de fevereiro de 2012, Inter-Environnement Wallonie e Terre wallonne (C-41/11, EU:C:2012:103, n.º 57).

104 Acórdão de 28 de fevereiro de 2012, Inter-Environnement Wallonie e Terre wallonne (C-41/11, EU:C:2012:103, n.º 62).

105 N.º 45 das observações escritas do Governo dinamarquês.

V. Conclusão

155. Em face do exposto, proponho ao Tribunal de Justiça que responda à Cour constitutionnelle (Tribunal Constitucional, Bélgica) nos seguintes termos:

1) O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conjugado com os 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:

   – Se opõe a uma legislação nacional que 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 e utilizadores, relativamente a todos os meios de comunicação eletrónica;

   – A isto não obsta que essa legislação nacional tenha por objetivos não apenas a investigação, a deteção e a instauração de procedimento criminal contra crimes, graves ou não, mas também a segurança nacional, a defesa do território, a segurança pública, a prevenção da utilização não autorizada dos sistemas de comunicação eletrónica, ou qualquer outro previsto no artigo 23.º, n.º 1, do Regulamento (UE) 2016/679 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 sobre a Proteção de Dados);

   – A isto também não obsta que o acesso aos dados conservados esteja sujeito a garantias regulamentadas de forma precisa. Cabe ao órgão jurisdicional de reenvio verificar se a legislação nacional que regulamenta as condições desse acesso por parte das autoridades competentes o limita a casos específicos cuja gravidade torne imprescindível a ingerência, se o condiciona ao controlo prévio (exceto em caso de urgência) de um órgão jurisdicional ou de uma autoridade independente e prevê que as pessoas em causa sejam informadas desse acesso, desde que essa comunicação não comprometa a atuação das referidas autoridades.

2) Os artigos 4.º e 6.º da Carta dos Direitos Fundamentais da União Europeia não influenciam a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, conjugado com os restantes já mencionados artigos da mesma Carta, de modo a impedir a determinação da incompatibilidade de uma regulamentação nacional como a impugnada no litígio principal com o direito da União.

3) Um órgão jurisdicional nacional pode, caso o direito nacional o permita, manter excecional e provisoriamente os efeitos de uma legislação como a impugnada no litígio principal, mesmo que seja incompatível com o direito da União, se essa subsistência se justificar por considerações imperiosas relacionadas com as ameaças à segurança pública ou à segurança nacional, que não pudessem ser combatidas por outros meios e outras alternativas. Essa subsistência só pode manter-se durante o tempo estritamente necessário para sanar a referida incompatibilidade com o direito da União.