Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Primeira Secção)

7 de setembro de 2023 *

«Reenvio prejudicial — Telecomunicações — Tratamento de dados pessoais no setor das comunicações eletrónicas — Diretiva 2002/58/CE — Âmbito de aplicação — Artigo 15.º, n.º 1 — Dados conservados pelos prestadores de serviços de comunicações eletrónicas e disponibilizados às autoridades titulares da ação penal — Utilização posterior desses dados num inquérito relativo a uma falta imputável ao serviço»

No processo C-162/22,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pelo Lietuvos vyriausiasis administracinis teismas (Supremo Tribunal Administrativo, Lituânia), por Decisão de 24 de fevereiro de 2022, que deu entrada no Tribunal de Justiça em 3 de março de 2022, no processo instaurado por

A. G.

sendo intervenientes:

Lietuvos Respublikos generalinė prokuratūra,

O TRIBUNAL DE JUSTIÇA (Primeira Secção),

composto por: A. Arabadjiev, presidente de secção, P. G. Xuereb (relator), T. von Danwitz, A. Kumin e I. Ziemele, juízes,

advogado-geral: M. Campos Sánchez-Bordona,

secretário: A. Lamote, administradora,

vistos os autos e após a audiência de 2 de fevereiro de 2023,

vistas as observações apresentadas:

– em representação de A. G., por G. Danėlius, advokatas,

– em representação do Governo lituano, por S. Grigonis, V. Kazlauskaitė-Švenčionienė e V. Vasiliauskienė, na qualidade de agentes,

* Língua do processo: lituano.

– em representação do Governo checo, por O. Serdula, M. Smolek e J. Vláčil, na qualidade de agentes,

– em representação do Governo estónio, por M. Kriisa, na qualidade de agente,

– em representação da Irlanda, por M. Browne, A. Joyce e M. Tierney, na qualidade de agentes, assistidos por D. Fennelly, BL,

– em representação do Governo francês, por R. Bénard, na qualidade de agente,

– em representação do Governo italiano, por G. Palmieri, na qualidade de agente, assistida por A. Grumetto, avvocato dello Stato,

– em representação do Governo húngaro, por Zs. Biró-Tóth e M. Z. Fehér, na qualidade de agentes,

– em representação da Comissão Europeia, por S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal e F. Wilman, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 30 de março de 2023,

profere o presente

Acórdão

1 O pedido de decisão prejudicial tem por objeto a interpretação do 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) (JO 2002, L 201, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO 2009, L 337, p. 11) (a seguir «Diretiva 2002/58»).

2 Este pedido foi apresentado no âmbito de um processo instaurado por A. G. a respeito da legalidade de decisões da Lietuvos Respublikos generalinė prokuratūra (Procuradoria-Geral da República da Lituânia; a seguir «Procuradoria-Geral») que o demitem das suas funções de procurador.

Quadro jurídico

Direito da União

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

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

[…]

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

4 O artigo 5.º desta diretiva, sob a epígrafe «Confidencialidade das comunicações», prevê, no seu n.º 1:

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

5 O artigo 15.º da referida diretiva, sob a epígrafe «Aplicação de determinadas disposições da Diretiva 95/46/CE», enuncia, no seu n.º 1:

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

Direito lituano

Lei relativa às Comunicações Eletrónicas

6 O artigo 65.º, n.º 2, da Lietuvos Respublikos elektroninių ryšių įstatymas (Lei da República da Lituânia relativa às Comunicações Eletrónicas), de 15 de abril de 2004 (Žin., 2004, n.º 69-2382), na versão aplicável aos factos no processo principal (a seguir «Lei relativa às Comunicações Eletrónicas»), impõe aos prestadores de serviços de comunicações eletrónicas a obrigação de conservarem os dados referidos no anexo 1 desta lei e, se necessário, de os disponibilizarem às autoridades competentes, para que os possam utilizar na luta contra a criminalidade grave.

7 Em conformidade com o anexo 1 da Lei relativa às Comunicações Eletrónicas, as categorias de dados que devem ser conservados são as seguintes:

«1. Dados necessários para encontrar e identificar a fonte de uma comunicação: […] 2. Dados necessários para identificar o destino de uma comunicação: […] 3. Dados necessários para identificar a data, a hora e a duração de uma comunicação: […] 4. Dados necessários para identificar o tipo de comunicação: […] 5. Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento: […] 6. Dados necessários para identificar a localização do equipamento de comunicação móvel: […]»

8 De acordo com o artigo 77.º, n.º 4, desta lei, perante uma decisão judicial fundamentada ou outra base jurídica prevista por lei, os prestadores de serviços de comunicações eletrónicas devem viabilizar tecnicamente, em especial aos órgãos responsáveis pelo inquérito e pelo exercício da ação penal, de acordo com as modalidades previstas no Lietuvos Respublikos baudžiamojo proceso kodeksas (Código de Processo Penal da República da Lituânia; a seguir «Código de Processo Penal»), o controlo do conteúdo das informações difundidas nas redes de comunicações eletrónicas.

Lei relativa à Informação Criminal

9 O artigo 6.º, n.º 3, ponto 1, da Lietuvos Respublikos kriminalinės žvalgybos Įstatymas (Lei da República da Lituânia relativa à Informação Criminal), de 2 de outubro de 2012 (Žin., 2012, n.º 122-6093), na versão aplicável aos factos no processo principal (a seguir «Lei relativa à Informação Criminal»), dispõe que, quando estejam preenchidos os requisitos previstos nesta lei para justificar uma operação de informação criminal e mediante autorização de um membro do Ministério Público ou de um órgão jurisdicional, os órgãos de informação criminal têm o poder, além dos enumerados nos n.ºs 1 e 2 do mesmo artigo, de obter informações junto dos prestadores de serviços de comunicações eletrónicas.

10 O artigo 8.º, n.º 1, da referida lei prevê a realização de um inquérito pelos organismos de informação em matéria penal quando, nomeadamente, estejam disponíveis informações sobre a preparação ou a prática de uma infração muito grave, grave, ou relativamente grave ou sobre as pessoas que preparem, pratiquem ou tenham praticado tal infração. O artigo 8.º, n.º 3, da mesma lei especifica que, se esse inquérito revelar a existência de indícios de infração penal, é imediatamente aberta uma instrução penal.

11 De acordo com o artigo 19.º, n.º 1, ponto 5, da Lei relativa à Informação Criminal, as informações procedentes de operações de informação criminal podem ser utilizadas nos casos definidos nos n.ºs 3 e 4 deste artigo e noutros casos previstos na lei. Por força do n.º 3 do referido artigo, as informações procedentes de operações de informação criminal relativas a um facto com características de infração afim à corrupção podem ser desclassificadas, com o consentimento do Ministério Público, e utilizadas no âmbito de um inquérito sobre faltas disciplinares ou imputáveis ao serviço.

Código de Processo Penal

12 O artigo 154.º do Código de Processo Penal prevê que, por decisão de um juiz de instrução proferida a pedido de um membro do Ministério Público, o responsável pelo inquérito pode ouvir as conversas difundidas nas redes de comunicações eletrónicas, transcrevê-las, controlar

outras informações enviadas pelas redes de comunicações eletrónicas, registá-las e conservá-las, se existirem, nomeadamente, razões para crer que tal permitirá obter dados sobre uma infração muito grave ou grave em fase de preparação ou de execução ou já executada, ou sobre uma infração relativamente grave ou sem gravidade.

13 O artigo 177.º, n.º 1, deste código dispõe que os dados da instrução são confidenciais e que, até à apreciação judicial do processo, esses dados só podem ser divulgados mediante autorização do Ministério Público e apenas na medida em que tal se justifique.

14 Para efeitos da aplicação do artigo 177.º do referido código, são aplicáveis as Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos (Recomendações para o fornecimento e a utilização de dados da instrução para fins não judiciais e para a proteção desses dados), aprovadas pela Decisão n.º I-279 do Procurador-Geral, de 17 de agosto de 2017 (TAR, 2017, n.º 2017-13413), conforme alteradas em último lugar pela Decisão n.º I-211, de 25 de junho de 2018.

15 O ponto 23 destas recomendações prevê que, ao receber um pedido de acesso aos dados resultantes da instrução, o procurador decide se há que fornecer esses dados. Se for tomada a decisão de os fornecer, o procurador deve especificar em que medida podem ser fornecidos os dados referidos no pedido.

Litígio no processo principal e questão prejudicial

16 A Procuradoria-Geral abriu um inquérito administrativo contra o recorrente no processo principal, que na época exercia as funções de procurador do Ministério Público lituano, com o fundamento de que existiam indícios de que este, no âmbito de uma instrução que dirigia, tinha ilegalmente fornecido informações pertinentes para essa instrução ao suspeito e ao seu advogado.

17 No relatório desse inquérito, a Comissão da Procuradoria-Geral constatou que o recorrente no processo principal tinha efetivamente cometido uma falta imputável ao serviço.

18 Segundo este relatório, esta falta imputável ao serviço era demonstrada pelos elementos recolhidos durante o inquérito administrativo. Em especial, as informações obtidas em operações de informação criminal e os dados recolhidos em duas instruções penais confirmavam a existência de comunicações telefónicas entre o recorrente no processo principal e o advogado do suspeito no âmbito da instrução respeitante a este último, que o recorrente no processo principal dirigia. O referido relatório salientou, além disso, que um despacho judicial tinha autorizado a interceção e o registo do conteúdo das informações difundidas em redes de comunicações eletrónicas relativas ao advogado em causa e que outro despacho judicial tinha autorizado a mesma medida relativamente ao recorrente no processo principal.

19 Com base no mesmo relatório, a Procuradoria-Geral adotou duas decisões através das quais, por um lado, aplicou ao recorrente no processo principal uma sanção que consistia na destituição das suas funções e, por outro, demitiu-o das suas funções.

20 O recorrente no processo principal interpôs no Vilniaus apygardos administracinis teismas (Tribunal Administrativo Regional de Vílnius, Lituânia) um recurso de anulação dessas duas decisões.

21 Por Sentença de 16 de julho de 2021, esse órgão jurisdicional negou provimento ao recurso interposto pelo recorrente no processo principal, com o fundamento, nomeadamente, de que as operações de informação criminal efetuadas no caso em apreço eram legais e que as informações recolhidas em conformidade com as disposições da Lei relativa à Informação Criminal tinham sido utilizadas legalmente para apreciar a existência de uma falta imputável ao serviço eventualmente cometida pelo recorrente no processo principal.

22 O recorrente no processo principal interpôs recurso no Lietuvos vyriausiasis administracinis teismas (Supremo Tribunal Administrativo, Lituânia), o órgão jurisdicional de reenvio, alegando que o acesso pelos órgãos de informação, no âmbito de uma operação de informação criminal, aos dados de tráfego e ao próprio conteúdo das comunicações eletrónicas constituía uma violação dos direitos fundamentais de tal gravidade, que, tendo em conta as disposições da Diretiva 2002/58 e da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»), esse acesso só podia ser concedido para efeitos de luta contra infrações graves. Ora, o artigo 19.º, n.º 3, da Lei relativa à Informação Criminal prevê que esses dados podem ser utilizados para investigar não só infrações graves mas também faltas disciplinares ou faltas imputáveis ao serviço afins a atos de corrupção.

23 Segundo o órgão jurisdicional de reenvio, as questões suscitadas pelo recorrente no processo principal têm por objeto dois elementos, a saber, por um lado, o acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas para fins diferentes da luta contra as infrações graves e a prevenção de ameaças graves à segurança pública e, por outro, obtido esse acesso, a utilização desses dados para investigar faltas imputáveis ao serviço afins à corrupção.

24 Esse órgão jurisdicional recorda que resulta da jurisprudência do Tribunal de Justiça, nomeadamente do Acórdão de 6 de outubro de 2020, Privacy International (C-623/17, EU:C:2020:790, n.º 39), que, por um lado, o artigo 15.º, n.º 1, da Diretiva 2002/58, lido em conjugação com o seu artigo 3.º, deve ser interpretado no sentido de que está abrangida pelo âmbito de aplicação desta diretiva não só uma medida legislativa que impõe aos fornecedores de serviços de comunicações eletrónicas a conservação dos dados de tráfego e dos dados de localização, mas também uma medida legislativa que os obriga a conceder às autoridades nacionais competentes o acesso a esses dados. Por outro lado, decorre desta jurisprudência, nomeadamente do Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152, n.ºs 33 e 35), que, no que respeita ao objetivo de prevenção, de investigação, de deteção e de perseguição de infrações penais, em conformidade com o princípio da proporcionalidade, só a luta contra a criminalidade grave e a prevenção de ameaças graves contra a segurança pública são suscetíveis de justificar ingerências graves nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, como as que implicam a conservação dos dados de tráfego e dos dados de localização, seja ela generalizada e indiferenciada ou seletiva.

25 Todavia, o Tribunal de Justiça ainda não se terá pronunciado sobre o impacto da utilização posterior dos dados em questão na ingerência nos direitos fundamentais. Nestas circunstâncias, o órgão jurisdicional de reenvio interroga-se sobre se se deve igualmente considerar que tal utilização posterior constitui uma ingerência dessa gravidade nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que apenas a luta contra a criminalidade grave e a prevenção das ameaças graves contra a segurança pública são suscetíveis de a justificar, o que exclui a possibilidade de utilizar esses dados em investigações relativas a faltas imputáveis ao serviço afins à corrupção.

26 Nestas condições, o Lietuvos vyriausiasis administracinis teismas (Supremo Tribunal Administrativo) decidiu suspender a instância e submeter ao Tribunal de Justiça a seguinte questão prejudicial:

«Deve o artigo 15.º, n.º 1, da [Diretiva 2002/58], lido em conjugação com os artigos 7.º, 8.º, 11.º, e 52.º, n.º 1, da [Carta], ser interpretado no sentido de que proíbe as autoridades públicas competentes de usarem, no âmbito de investigações por conduta ilícita relacionada com corrupção no exercício de funções, os dados conservados pelos prestadores de serviços de comunicações eletrónicas que podem fornecer informações sobre os dados de um utilizador de um meio de comunicação eletrónica e sobre as comunicações por este efetuadas, independentemente de ter sido concedido acesso a esses dados, no caso concreto, para fins de luta contra a criminalidade grave e de prevenção de ameaças graves à segurança pública?»

Quanto à questão prejudicial

27 Com a sua questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a que os dados pessoais relativos a comunicações eletrónicas que, em aplicação de uma medida legislativa adotada ao abrigo desta disposição, foram conservados pelos prestadores de serviços de comunicações eletrónicas e que, em seguida, em aplicação dessa medida, foram disponibilizados às autoridades competentes para efeitos de luta contra a criminalidade grave possam ser utilizados no âmbito de investigações relativas a faltas imputáveis ao serviço afins à corrupção.

28 A título preliminar, importa salientar que resulta da decisão de reenvio que, se é certo que o processo administrativo relativo ao procedimento que conduziu às decisões na causa principal, referidas no n.º 19 do presente acórdão, incluía igualmente informações que tinham sido recolhidas pelas autoridades competentes graças à interceção e ao registo de comunicações eletrónicas que tinham sido autorizadas, para efeitos de procedimento penal, por dois despachos judiciais, não deixa de ser verdade que o órgão jurisdicional de reenvio não se interroga sobre a utilização de dados pessoais que foram obtidos sem a intervenção dos prestadores de serviços de comunicações eletrónicas, mas sobre a utilização posterior de dados pessoais que foram conservados por esses prestadores com fundamento numa medida legislativa do Estado-Membro que lhes impunha essa obrigação de conservação, ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58.

29 A este respeito, resulta das indicações que figuram no pedido de decisão prejudicial que os dados visados na questão submetida são os considerados nos termos do artigo 65.º, n.º 2, da Lei relativa às Comunicações Eletrónicas, lido em conjugação com o anexo 1 desta lei, que impõe aos prestadores de serviços de comunicações eletrónicas a obrigação de conservar, de forma generalizada e indiferenciada, os dados de tráfego e os dados de localização relativos a essas comunicações para efeitos da luta contra a criminalidade grave.

30 No que respeita às condições em que estes dados podem ser utilizados num procedimento administrativo relativo a faltas de serviço afins à corrupção, importa, em primeiro lugar, recordar que, em aplicação de uma medida tomada nos termos do artigo 15.º, n.º 1, da Diretiva 2002/58, o acesso a esses dados só pode ser concedido se os mesmos dados tiverem sido conservados por esses fornecedores em conformidade com esta disposição [v., neste sentido, Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações

eletrónicas), C-746/18, EU:C:2021:152, n.º 29, e jurisprudência referida]. Em seguida, a utilização posterior dos dados de tráfego e dos dados de localização associados a tais comunicações com o propósito de combater a criminalidade grave só é possível na condição de, por um lado, a conservação destes dados pelos prestadores de serviços de comunicações eletrónicas estar em conformidade com o artigo 15.º, n.º 1, da Diretiva 2002/58, conforme interpretado pela jurisprudência do Tribunal de Justiça, e, por outro lado, o acesso a tais dados concedido às autoridades competentes também estar em conformidade com esta disposição.

31 A este respeito, o Tribunal de Justiça já declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, e 11.º, bem como do artigo 52.º, n.º 1, da Carta, se opõe a medidas legislativas que preveem, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização (Acórdão de 20 de setembro de 2022, SpaceNet e Telekom Deutschland, C-793/19 e C-794/19, EU:C:2022:702, n.ºs 74 e 131 e jurisprudência referida). Em contrapartida, o Tribunal de Justiça precisou que o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,

– uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas renovável;

– uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

– uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos; e

– uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem,

desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito pelas respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso (Acórdão de 20 de setembro de 2022, SpaceNet e Telekom Deutschland, C-793/19 e C-794/19, EU:C:2022:702, n.º 75 e jurisprudência referida).

32 No que respeita aos objetivos suscetíveis de justificar a utilização, pelas autoridades públicas, dos dados conservados pelos prestadores de serviços de comunicações eletrónicas em aplicação de uma medida em conformidade com estas disposições, há que recordar que o artigo 15.º, n.º 1, da Diretiva 2002/58 permite que os Estados-Membros introduzam exceções à obrigação de princípio, prevista no artigo 5.º, n.º 1, desta diretiva, de garantir a confidencialidade dos dados pessoais e às obrigações correspondentes, mencionadas, nomeadamente, nos artigos 6.º e 9.º da referida diretiva, sempre que constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional, a defesa e 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. Para o efeito, os Estados-Membros podem, designadamente, adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, por uma destas razões (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 110).

33 O artigo 15.º, n.º 1, da Diretiva 2002/58 não pode, portanto, justificar que a derrogação da obrigação de princípio de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados e, em especial, da proibição de armazenar esses dados, prevista no artigo 5.º dessa diretiva, se converta em regra, sob pena de esvaziar em grande medida esta última disposição do seu alcance (Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 40).

34 Quanto aos objetivos suscetíveis de justificar uma restrição aos direitos e às obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58, o Tribunal de Justiça já declarou que a enumeração dos objetivos que figuram no artigo 15.º, n.º 1, primeira frase, desta diretiva tem caráter taxativo, de modo que uma medida legislativa adotada ao abrigo desta disposição tem de responder efetiva e estritamente a um desses objetivos (Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 41).

35 Relativamente aos objetivos de interesse geral suscetíveis de justificar uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, resulta da jurisprudência do Tribunal de Justiça que, em conformidade com o princípio da proporcionalidade, existe uma hierarquia entre estes objetivos em função da sua importância respetiva e que a importância do objetivo prosseguido por essa medida deve estar relacionada com a gravidade da ingerência daí resultante (Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 56).

36 A este respeito, a importância do objetivo de salvaguarda da segurança nacional, lido à luz do artigo 4.º, n.º 2, TUE, segundo o qual a salvaguarda da segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro, ultrapassa a dos outros objetivos referidos no artigo 15.º, n.º 1, da Diretiva 2002/58, nomeadamente os objetivos de luta contra a criminalidade em geral, incluindo grave, e de salvaguarda da segurança pública. Sem prejuízo dos outros requisitos previstos no artigo 52.º, n.º 1, da Carta, o objetivo de salvaguarda da segurança nacional é, por conseguinte, suscetível de justificar medidas que incluam ingerências nos direitos fundamentais mais graves do que aquelas que esses outros objetivos poderiam justificar (Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 57 e jurisprudência referida).

37 No que diz respeito ao objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais, o Tribunal de Justiça salientou que, em conformidade com o princípio da proporcionalidade, só a luta contra a criminalidade grave e a prevenção das ameaças graves contra a segurança pública são suscetíveis de justificar ingerências graves nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, tais como as que implicam a conservação de dados de tráfego e de dados de localização. Por conseguinte, só as ingerências sem caráter grave nos referidos direitos fundamentais podem ser justificadas pelo objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral (Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 59 e jurisprudência referida).

38 Resulta desta jurisprudência que, embora seja certo que a luta contra a criminalidade grave e a prevenção de ameaças graves à segurança pública têm uma importância menor, na hierarquia dos objetivos de interesse geral, do que a salvaguarda da segurança nacional (v., neste sentido, Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 99), a sua importância é, contudo, superior à da luta contra infrações penais em geral e à da prevenção de ameaças não graves à segurança pública.

39 Neste contexto, importa, contudo, lembrar que, como também resulta do n.º 31 do presente acórdão, a possibilidade de os Estados-Membros justificarem uma restrição aos direitos e às obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58 deve ser apreciada através da medição da gravidade da ingerência que tal restrição implica e da verificação de que a importância do objetivo de interesse geral prosseguido por esta restrição está relacionada com essa gravidade (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 131).

40 Além disso, como o Tribunal de Justiça já declarou, o acesso a dados de tráfego e a dados de localização conservados pelos prestadores em aplicação de uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, que deve ser efetuado no pleno respeito pelas condições resultantes da jurisprudência que interpretou esta diretiva, apenas pode, em princípio, ser justificado pelo objetivo de interesse geral pelo qual essa conservação foi imposta a esses prestadores. Só assim não será se a importância do objetivo prosseguido pelo acesso ultrapassar a do objetivo que justificou a conservação (Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 98 e jurisprudência referida).

41 Ora, estas considerações aplicam-se *mutatis mutandis* a uma utilização posterior dos dados de tráfego e dos dados de localização conservados por prestadores de serviços de comunicações eletrónicas em aplicação de uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58 para efeitos de luta contra a criminalidade grave. Com efeito, tais dados não podem, após terem sido conservados e disponibilizados às autoridades competentes com o propósito de combater a criminalidade grave, ser transmitidos a outras autoridades e utilizados para realizar objetivos, tais como, no caso em apreço, a luta contra faltas imputáveis ao serviço afins à corrupção, que, na hierarquia dos objetivos de interesse geral, têm menor importância do que a luta contra a criminalidade grave e a prevenção de ameaças graves contra a segurança pública. Com efeito, autorizar, em tal situação, um acesso aos dados conservados e a sua utilização iria contra essa hierarquia dos objetivos de interesse geral recordada nos n.os 33, 35 a 37 e 40 do presente acórdão (v., neste sentido, Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 99).

42 Quanto ao argumento invocado pelo Governo checo e pela Irlanda nas suas observações escritas, segundo o qual um processo disciplinar relativo a faltas imputáveis ao serviço afins à corrupção pode estar relacionado com a salvaguarda da segurança pública, basta salientar que, na sua decisão de reenvio, o órgão jurisdicional de reenvio não referiu uma ameaça grave à segurança pública.

43 Além disso, embora seja verdade que os inquéritos administrativos relativos a faltas disciplinares ou a faltas imputáveis ao serviço afins a atos de corrupção podem desempenhar um papel importante na luta contra esses atos, uma medida legislativa que prevê tais inquéritos não cumpre efetiva e estritamente o objetivo de repressão e de punição de infrações penais, previsto no artigo 15.º, n.º 1, primeira frase, da Diretiva 2002/58, que se refere apenas à ação penal.

44 Atendendo às considerações anteriores, há que responder à questão submetida que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a que os dados pessoais relativos a comunicações eletrónicas que, em aplicação de uma medida legislativa adotada ao abrigo desta disposição, foram conservados pelos prestadores de serviços de comunicações eletrónicas e que, em seguida, em aplicação dessa medida, foram disponibilizados às autoridades competentes para efeitos de luta contra a criminalidade grave possam ser utilizados no âmbito de investigações relativas a faltas imputáveis ao serviço afins à corrupção.

Quanto às despesas

45 Revestindo o processo, quanto às partes na causa principal, a natureza de incidente suscitado perante o órgão jurisdicional de reenvio, compete a este decidir quanto às despesas. As despesas efetuadas pelas outras partes para a apresentação de observações ao Tribunal de Justiça não são reembolsáveis.

Pelos fundamentos expostos, o Tribunal de Justiça (Primeira Secção) declara:

O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia,

deve ser interpretado no sentido de que:

se opõe a que os dados pessoais relativos a comunicações eletrónicas que, em aplicação de uma medida legislativa adotada ao abrigo desta disposição, foram conservados pelos prestadores de serviços de comunicações eletrónicas e que, em seguida, em aplicação dessa medida, foram disponibilizados às autoridades competentes para efeitos de luta contra a criminalidade grave possam ser utilizados no âmbito de investigações relativas a faltas imputáveis ao serviço afins à corrupção.

Assinaturas