Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

2 de março de 2021 *

«Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Diretiva 2002/58/CE — Prestadores de serviços de comunicações eletrónicas — Confidencialidade das comunicações — Limitações — Artigo 15.º, n.º 1 — Artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia — Legislação que prevê a conservação generalizada e indiferenciada dos dados relativos ao tráfego e dos dados de localização pelos prestadores de serviços de comunicações eletrónicas — Acesso das autoridades nacionais aos dados conservados para efeitos de inquéritos — Luta contra a criminalidade em geral — Autorização dada pelo Ministério Público — Utilização dos dados no âmbito do processo penal enquanto elementos de prova — Admissibilidade»

No processo C-746/18,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pelo Riigikohus (Supremo Tribunal, Estónia), por Decisão de 12 de novembro de 2018, que deu entrada no Tribunal de Justiça em 29 de novembro de 2018, no processo penal contra

H. K.,

sendo interveniente:

Prokuratuur,

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: K. Lenaerts, presidente, R. Silva de Lapuerta, vice-presidente, J.-C. Bonichot, A. Arabadjiev, A. Prechal e L. Bay Larsen, presidentes de secção, T. von Danwitz (relator), M. Safjan, K. Jürimäe, C. Lycourgos e P. G. Xuereb, juízes,

advogado-geral: G. Pitruzzella,

secretário: C. Strömholm, administradora,

vistos os autos e após a audiência de 15 de outubro de 2019,

considerando as observações apresentadas:

– em representação de H. K., por S. Reinsaar, vandeadvokaat,

* Língua do processo: estónio.

– em representação do Prokuratuur, por T. Pern e M. Voogma, na qualidade de agentes,

– em representação do Governo estónio, por N. Grünberg, na qualidade de agente,

– em representação do Governo dinamarquês, por J. Nymann-Lindegren e M. S. Wolff, na qualidade de agentes,

– em representação da Irlanda, por M. Browne, G. Hodge, J. Quaney e A. Joyce, na qualidade de agentes, assistidos por D. Fennelly, barrister,

– em representação do Governo francês, inicialmente, por D. Dubois, D. Colas, E. de Moustier e A.-L. Desjonquères, em seguida, por D. Dubois, E. de Moustier e A.-L. Desjonquères, na qualidade de agentes,

– em representação do Governo letão, inicialmente, por V. Kalniņa e I. Kucina, em seguida, por V. Soņeca e V. Kalniņa, na qualidade de agentes,

– em representação do Governo húngaro, por M. Z. Fehér e A. Pokoraczki, na qualidade de agentes,

– em representação do Governo polaco, por B. Majczyna, na qualidade de agente,

– em representação do Governo português, por L. Inez Fernandes, P. Barros da Costa, L. Medeiros e I. Oliveira, na qualidade de agentes,

– em representação do Governo finlandês, por J. Heliskoski, na qualidade de agente,

– em representação do Governo do Reino Unido, por S. Brandon e Z. Lavery, na qualidade de agentes, assistidos por G. Facenna, QC, e por C. Knight, barrister,

– em representação da Comissão Europeia, inicialmente, por H. Kranenborg, M. Wasmeier, P. Costa de Oliveira e K. Toomus, em seguida, por H. Kranenborg, M. Wasmeier e E. Randvere, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 21 de janeiro de 2020,

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»), lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

2 Este pedido foi apresentado no âmbito de um processo penal instaurado contra H. K. por furto, utilização do cartão bancário de um terceiro e violência contra pessoas que participavam num processo judicial.

Quadro jurídico

Direito da União

3 Os considerandos 2 e 11 da Diretiva 2002/58 enunciam:

«(2) A presente diretiva visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela [Carta]. Visa, em especial, assegurar o pleno respeito pelos direitos consignados nos artigos 7.º e 8.º [desta].

[…]

(11) Tal como a 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)], a presente diretiva não trata questões relativas à proteção dos direitos e liberdades fundamentais relacionadas com atividades não reguladas pelo direito [da União]. Portanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.º 1 do artigo 15.º da presente diretiva, necessários para a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal. Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, [assinada em Roma, em 4 de novembro de 1950,] segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais.»

4 Nos termos do artigo 2.º da Diretiva 2002/58, sob a epígrafe «Definições»:

«Salvo disposição em contrário, são aplicáveis as definições constantes da Diretiva [95/46] e da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (Diretiva-Quadro) [(JO 2002, L 108, p. 33)].

São também aplicáveis as seguintes definições:

a) "Utilizador" é qualquer pessoa singular que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

b) “Dados de tráfego” são quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma;

c) “Dados de localização” [são] quaisquer dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público;

d) “Comunicação” é qualquer informação trocada ou enviada entre um número finito de partes, através de um serviço de comunicações eletrónicas publicamente disponível; não se incluem aqui as informações enviadas no âmbito de um serviço de difusão ao público em geral, através de uma rede de comunicações eletrónicas, exceto na medida em que a informação possa ser relacionada com o assinante ou utilizador identificável que recebe a informação;

[…]»

5 Nos termos do artigo 5.º da Diretiva 2002/58, sob a epígrafe «Confidencialidade das comunicações»:

«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.

[…]

3. Os Estados-Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Diretiva [95/46], nomeadamente sobre os objetivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.»

6 O artigo 6.º da Diretiva 2002/58, sob a epígrafe «Dados de tráfego», dispõe:

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

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

3. Para efeitos de comercialização dos serviços de comunicações eletrónicas ou para a prestação de serviços de valor acrescentado, o prestador de um serviço de comunicações eletrónicas acessível ao público pode tratar os dados referidos no n.º 1 na medida do necessário e pelo tempo necessário para a prestação desses serviços ou essa comercialização, se o assinante ou utilizador a quem os dados dizem respeito tiver dado o seu consentimento prévio. Deve ser dada a possibilidade aos utilizadores ou assinantes de retirarem a qualquer momento o seu consentimento para o tratamento dos dados de tráfego.

[…]

5. O tratamento de dados de tráfego, em conformidade com o disposto nos n.os 1 a 4, será limitado ao pessoal que trabalha para os fornecedores de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis encarregado da faturação ou da gestão do tráfego, das informações a clientes, da deteção de fraudes, da comercialização dos serviços de comunicações eletrónicas publicamente disponíveis, ou da prestação de um serviço de valor acrescentado, devendo ser limitado ao necessário para efeitos das referidas atividades.

[…]»

7 O artigo 9.º da Diretiva 2002/58, sob a epígrafe «Dados de localização para além dos dados de tráfego», prevê, no seu n.º 1:

«Nos casos em que são processados dados de localização, para além dos dados de tráfego, relativos a utilizadores ou assinantes de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis, esses dados só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado. O prestador de serviços deve informar os utilizadores ou assinantes, antes de obter o seu consentimento, do tipo de dados de localização, para além dos dados de tráfego, que serão tratados, dos fins e duração do tratamento e da eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado. […]»

8 O artigo 15.º da referida diretiva, sob a epígrafe «Aplicação de determinadas disposições da Diretiva [95/46]», 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]. 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 [da União], incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do Tratado da União Europeia.»

Direito estónio

Lei Relativa às Comunicações Eletrónicas

9 O artigo 111[1] da elektroonilise side siadus (Lei Relativa às Comunicações Eletrónicas, RT I 2004, 87, 593; RT I, 22.05.2018, 3), na redação aplicável aos factos no processo principal (a seguir «Lei Relativa às Comunicações Eletrónicas»), sob a epígrafe «Obrigação de conservar os dados», prevê:

«[…]

(2) Os [prestadores] de serviços de telefonia fixa e de telefonia móvel e da rede de serviços de telefonia fixa e de telefonia móvel [devem] conservar os dados seguintes:

1) O número [da pessoa que] faz a chamada, o nome e a morada do assinante;

2) O número [da pessoa que] recebe a chamada, o nome e a morada do assinante;

3) Em caso de serviços complementares, como o reenvio ou a transferência da chamada, o número composto, o nome e a morada do assinante;

4) A data e a hora do início e do fim da chamada;

5) O serviço de telefonia fixa ou móvel utilizado;

6) A identificação internacional de assinante móvel (*International Mobile Subscriber Identity — IMSI*) [da pessoa que] faz a chamada e [da pessoa que a recebe];

7) A identificação internacional de equipamento móvel (*International Mobile Equipment Identity — IMEI*) [da pessoa que] faz a chamada e [da pessoa que a recebe];

8) O identificador celular no momento do início da chamada;

9) Os dados que identificam a localização geográfica da célula por referência ao identificador [celular] no período durante o qual os dados são conservados;

10) Em caso de serviços de telefonia móvel anónimos de pré-pagamento, a data e a hora da primeira ativação do serviço e a identidade de localização de onde o serviço foi ativado.

[…]

(4) Os dados referidos nos n.os 2 e 3 do presente artigo são conservados por um ano a contar da data da comunicação, se forem gerados ou tratados durante o fornecimento do serviço de comunicação. […]

[…]

(11) Os dados referidos nos n.os 2 e 3 do presente artigo são transferidos:

1) Em conformidade com o kriminaalmenetluse seadustik [(Código de Processo Penal)], para a autoridade encarregada do inquérito, para a autoridade habilitada a adotar medidas de vigilância, para o Ministério Público, para o tribunal;

[…]»

Código de Processo Penal

10 O artigo 17.º do kriminaalmenetluse seadustik (Código de Processo Penal, RT I 2003, 27, 166; RT I, 31.05.2018, 22) dispõe:

«(1) São partes no processo: o Ministério Público, […].

[…]»

11 O artigo 30.º deste código tem a seguinte redação:

«(1) O Ministério Público dirige a […] instrução do processo, garantindo a legalidade e a eficácia da mesma, e representa a ação pública no processo.

(2) As competências do Ministério Público no quadro do processo penal são exercidas em seu nome por um procurador que age de modo independente e que está unicamente sujeito à lei.»

12 O artigo 90[1] do referido código prevê:

«[…]

(2) A autoridade encarregada do inquérito pode, mediante autorização do Ministério Público durante a […] instrução do processo ou mediante autorização do tribunal durante o processo que nele decorre, pedir a uma empresa de comunicações eletrónicas que forneça os dados enumerados no artigo 111[1], n.os 2 e 3, da Lei Relativa às Comunicações Eletrónicas que não são referidos no n.º 1 do presente artigo. Esta autorização indica de forma precisa as datas relativas ao período durante o qual é possível exigir dados.

(3) Os pedidos de fornecimento de dados na aceção do presente artigo só podem ser feitos se forem absolutamente necessários para se alcançar o objetivo do processo penal.»

13 O artigo 211.º do mesmo código dispõe:

«(1) O objetivo da […] instrução do processo é a recolha de elementos de prova e a criação das outras condições necessárias à [organização] de um processo.

(2) Durante a […] instrução, a autoridade encarregada do inquérito e o Ministério Público verificam os elementos [incriminatórios] e os elementos [ilibatórios] recolhidos contra o suspeito ou contra o acusado.»

Lei Relativa ao Ministério Público

14 O artigo 1.º da prokuratuuriseadus (Lei Relativa ao Ministério Público, RT I 1998, 41, 625; RT I, 06.07.2018, 20), na redação aplicável aos factos no processo principal, prevê:

«(1) O Ministério Público é uma autoridade governamental que faz parte do Ministério da Justiça, que participa no planeamento das medidas de vigilância necessárias para combater e detetar infrações penais, dirige a […] instrução do processo penal, garantindo a legalidade e a eficácia desta, representa a ação [pública] no processo e executa as outras missões que lhe incumbem por força da lei.

(1[1]) O Ministério Público cumpre de modo independente as missões que lhe incumbem por força da lei e age baseando-se na presente lei, nas restantes leis e nos atos adotados ao abrigo das mesmas.

[…]»

15 O artigo 2.º, n.º 2, desta lei dispõe:

«O procurador cumpre as suas missões de forma independente e age unicamente nos termos da lei e segundo a sua convicção.»

Litígio no processo principal e questões prejudiciais

16 Por Decisão de 6 de abril de 2017, H. K. foi condenada pelo Viru Maakohus (Tribunal de Primeira Instância de Viru, Estónia) numa pena privativa de liberdade de dois anos, por ter cometido, entre 17 de janeiro de 2015 e 1 de fevereiro de 2016, vários furtos de bens (de valor entre 3 e 40 euros) e de dinheiro (de montantes entre 5,20 e 2 100 euros), utilizado um cartão bancário de um terceiro, causando a este último um prejuízo de 3 941,82 euros, e praticado atos de violência contra pessoas que participavam num processo judicial a seu respeito.

17 Para declarar H. K. culpada desses atos, o Viru Maakohus (Tribunal de Primeira Instância de Viru) baseou-se, designadamente, em vários relatórios elaborados a partir de dados relativos às comunicações eletrónicas, na aceção do artigo 111[1], n.º 2, da Lei Relativa às Comunicações Eletrónicas, que a autoridade encarregada do inquérito tinha recolhido junto de um prestador de serviços de telecomunicações eletrónicas, no decurso da instrução do processo, após ter obtido, ao abrigo do artigo 90[1] do Código de Processo Penal, várias autorizações, para esse efeito, do Viru Ringkonnaprokuratuur (Ministério Público do distrito de Viru, Estónia). Estas autorizações, concedidas em 28 de janeiro e 2 de fevereiro de 2015, em 2 de novembro de 2015 e em 25 de fevereiro de 2016, tinham por objeto os dados de vários números de telefone de H. K. e diferentes identidades internacionais de equipamento móvel desta, relativos ao período de 1 de janeiro a 2 de fevereiro de 2015, de 21 de setembro de 2015, bem como ao período de 1 de março de 2015 a 19 de fevereiro de 2016.

18 H. K. interpôs recurso da decisão do Viru Maakohus (Tribunal de Primeira Instância de Viru) para o Tartu Ringkonnakohus (Tribunal de Recurso de Tartu, Estónia), que lhe negou provimento por Decisão de 17 de novembro de 2017.

19 H. K. interpôs recurso de cassação desta última decisão para o Riigikohus (Supremo Tribunal, Estónia), contestando, designadamente, a admissibilidade dos relatórios elaborados a partir dos dados obtidos junto do prestador de serviços de comunicações eletrónicas. Em seu entender, decorre do Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, a seguir «Acórdão Tele2», EU:C:2016:970), que as disposições do artigo 111[1] da Lei Relativa às Comunicações Eletrónicas que preveem a obrigação dos prestadores de serviços de conservarem dados relativos às comunicações, bem como a utilização desses dados para efeitos da sua condenação, são contrárias ao artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º, e 52.º, n.º 1, da Carta.

20 Segundo o órgão jurisdicional de reenvio, coloca-se a questão de saber se se pode considerar que os relatórios elaborados a partir dos dados referidos no artigo 111[1], n.º 2, da Lei Relativa às Comunicações Eletrónicas constituem elementos de prova admissíveis. Esse órgão jurisdicional observa que a admissibilidade dos relatórios em causa no processo principal enquanto elementos de prova depende da questão de saber em que medida a recolha dos dados a partir dos quais esses relatórios foram elaborados foi feita em conformidade com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta.

21 O referido órgão jurisdicional considera que a resposta a esta questão implica que se determine se este artigo 15.º, n.º 1, lido à luz da Carta, deve ser interpretado no sentido de que o acesso das autoridades nacionais a dados que permitem identificar a origem e o destino de uma comunicação telefónica a partir do telefone fixo ou móvel de um suspeito, determinar a data, a hora, a duração e a natureza dessa comunicação, identificar o material de comunicação utilizado e localizar o material de comunicação móvel utilizado constitui uma ingerência de tal gravidade nos direitos fundamentais em causa, que esse acesso deveria ser limitado à luta contra a criminalidade grave, independentemente do período em relação ao qual as autoridades nacionais solicitaram o acesso aos dados conservados.

22 O órgão jurisdicional de reenvio considera, todavia, que a duração deste período é um elemento essencial para apreciar a gravidade da ingerência que consiste no acesso aos dados relativos ao tráfego e aos dados de localização. Assim, quando o referido período é muito curto ou a quantidade dos dados recolhidos é muito limitada, há que se interrogar se o objetivo de luta contra a criminalidade em geral, e não apenas de luta contra a criminalidade grave, é suscetível de justificar tal ingerência.

23 Por último, o órgão jurisdicional de reenvio tem dúvidas quanto à possibilidade de considerar o Ministério Público estónio como uma autoridade administrativa independente, na aceção do n.º 120 do Acórdão de 21 de dezembro de 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970), suscetível de autorizar o acesso da autoridade encarregada do inquérito a dados relativos às comunicações eletrónicas como os previstos no artigo 111[1], n.º 2, da Lei Relativa às Comunicações Eletrónicas.

24 O Ministério Público dirige a instrução do processo, garantindo a legalidade e a eficácia da mesma. Sendo o objetivo desse processo, designadamente, a recolha de provas, a autoridade encarregada do inquérito e o Ministério Público verificam os elementos incriminatórios e os elementos ilibatórios recolhidos contra qualquer suspeito ou acusado. Se o Ministério Público estiver convencido de que foram recolhidas todas as provas necessárias, exerce a ação pública contra o arguido. As competências do Ministério Público são exercidas em seu nome por um procurador que desempenha as suas missões de modo independente, como resulta do artigo 30.º, n.ºs 1 e 2, do Código de Processo Penal e dos artigos 1.º e 2.º da Lei Relativa ao Ministério Público.

25 Neste contexto, o órgão jurisdicional de reenvio salienta que as suas dúvidas quanto à independência exigida pelo direito da União se devem principalmente ao facto de o Ministério Público não só dirigir a instrução do processo mas também representar a ação pública durante o processo penal, sendo esta autoridade, por força do direito nacional, parte nesse processo.

26 Foi nestas circunstâncias que o Riigikohus (Supremo Tribunal) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) 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 o acesso das autoridades nacionais, no âmbito de um processo penal, a dados que permitem encontrar e identificar a origem e o destino de uma comunicação telefónica a partir do telefone fixo ou móvel do suspeito, determinar a data, a hora, a duração e a natureza, identificar o material de comunicação utilizado e localizar o material de comunicação móvel utilizado constitui uma ingerência de tal modo grave nos direitos fundamentais garantidos pelos artigos já referidos da Carta que, relativamente à prevenção, à investigação, à deteção e à [perseguição] de infrações penais, este acesso deve ser limitado à luta contra a criminalidade grave, independentemente do período em relação ao qual as autoridades nacionais têm acesso aos dados conservados?

2) Deve o artigo 15.º, n.º 1, da Diretiva [2002/58] ser interpretado a partir do princípio da proporcionalidade tal como formulado nos n.os 55 a 57 do [Acórdão de 2 de outubro de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788),] no sentido de que, se a quantidade de dados referidos na primeira questão, a que as autoridades nacionais têm acesso, não for muito significativa (quer do ponto de vista da natureza dos dados quer do ponto de vista da duração do período em causa), a ingerência nos direitos fundamentais que daí resulta pode ser justificada de forma geral pelo objetivo da prevenção, investigação, deteção e [perseguição] de infrações penais e de que, quanto maior for a quantidade dos dados a que as autoridades nacionais têm acesso mais graves devem ser as infrações penais contra as quais a ingerência se destina a lutar?

3) Deve considerar-se que a exigência constante do segundo ponto do dispositivo do [Acórdão de 21 de dezembro de 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970)], segundo a qual o acesso das autoridades nacionais competentes aos dados deve ser submetido a um controlo prévio por parte de um órgão jurisdicional ou por uma autoridade administrativa independente, significa que o artigo 15.º, n.º 1, da Diretiva [2002/58] deve ser interpretado no sentido de se poder considerar como autoridade administrativa independente o Ministério Público que dirige a […] instrução do processo e que, ao fazê-lo, é, por força da lei, obrigado a agir de modo independente, estando unicamente sujeito à lei e analisando, no âmbito da […] instrução, simultaneamente os elementos [incriminatórios] e os elementos [ilibatórios] relativos ao acusado, mas que representa a ação [pública] durante o processo judicial posterior?»

Quanto às questões prejudiciais

Quanto à primeira e à segunda questão

27 Com as suas primeira e segunda questões prejudiciais, que importa examinar conjuntamente, 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, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que permite o acesso de autoridades públicas a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados e de permitir tirar conclusões precisas sobre a sua vida privada, para fins de prevenção, de investigação, de deteção e de perseguição de infrações penais, sem que esse acesso esteja circunscrito a processos que visem a luta contra a criminalidade grave, independentemente da duração do período em relação ao qual o acesso aos referidos dados é solicitado, bem como da quantidade e da natureza dos dados disponíveis sobre tal período.

28 A este respeito, resulta do pedido de decisão prejudicial que, como confirmou o Governo estónio na audiência, os dados a que a autoridade nacional encarregada do inquérito teve acesso no processo principal são os obtidos ao abrigo do artigo 111[1], n.os 2 e 4, da Lei Relativa às Comunicações Eletrónicas, que impõe aos prestadores de serviços de comunicações eletrónicas uma obrigação de conservar de maneira generalizada e indiferenciada os dados de tráfego e os dados de localização no que respeita à telefonia fixa e móvel, durante um ano. Estes dados permitem, designadamente, encontrar e identificar a origem e o destino de uma comunicação a partir do telefone fixo ou móvel de uma pessoa, determinar a data, a hora, a duração e a natureza dessa comunicação, identificar o material de comunicação utilizado e localizar o telefone móvel sem que uma comunicação seja necessariamente enviada. Além disso, oferecem a possibilidade de determinar a frequência das comunicações do utilizador com certas pessoas durante um dado período. Por outro lado, como confirmou o Governo estónio na audiência, o acesso aos referidos dados pode, em matéria de luta contra a criminalidade, ser pedido relativamente a qualquer tipo de infração penal.

29 No que respeita às condições em que o acesso aos dados de tráfego e aos dados de localização conservados pelos prestadores de serviços de comunicações eletrónicas pode, para fins de prevenção, de investigação, de deteção e perseguição de infrações penais, ser concedido a autoridades públicas, em aplicação de uma medida tomada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, o Tribunal de Justiça declarou que tal acesso só pode ser concedido se esses dados tiverem sido conservados por esses prestadores em conformidade com o referido artigo 15.º, n.º 1 (v., neste sentido, 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 167).

30 A este respeito, o Tribunal de Justiça declarou igualmente 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, se opõe a medidas legislativas que prevejam, para tais fins, a título preventivo, a conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização (v., neste sentido, 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 168).

31 Quanto aos objetivos suscetíveis de justificar o acesso das autoridades públicas aos dados conservados pelos prestadores de serviços de comunicações eletrónicas em aplicação de uma medida conforme com essas disposições, resulta, por um lado, da jurisprudência do Tribunal de

Justiça que tal acesso só pode ser justificado pelo objetivo de interesse geral para o qual essa conservação foi imposta a esses prestadores de serviços (v., neste sentido, 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 166).

32 Por outro lado, o Tribunal de Justiça declarou que a possibilidade de os Estados-Membros justificarem uma limitação aos direitos e às obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58 deve ser apreciada medindo a gravidade da ingerência que essa limitação comporta e verificando se a importância do objetivo de interesse geral prosseguido por essa limitação tem relação com a gravidade dessa ingerência (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 e jurisprudência referida).

33 No que diz respeito ao objetivo de prevenção, de investigação, de deteção e de perseguição de infrações penais, prosseguido pela regulamentação em causa no processo principal, 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 implica a conservação dos dados de tráfego e dos dados de localização, quer esta seja generalizada e indiferenciada ou seletiva. Por conseguinte, só ingerências nos referidos direitos fundamentais que não apresentem caráter grave podem ser justificadas pelo objetivo, prosseguido pela regulamentação em causa no processo principal, de prevenção, de investigação, de deteção e perseguição de infrações penais em geral (v., neste sentido, 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.ºs 140 e 146).

34 A este respeito, foi, designadamente, declarado que as medidas legislativas que visam o tratamento de dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicas enquanto tais, designadamente a sua conservação e o acesso a estes, exclusivamente para efeitos de identificação do utilizador em causa, e sem que os referidos dados possam ser associados a informações relativas às comunicações efetuadas, podem ser justificadas pelo objetivo de prevenção, de investigação, de deteção e de perseguição de infrações penais em geral, ao qual se refere o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58. Com efeito, esses dados não permitem, por si sós, conhecer a data, a hora, a duração e os destinatários das comunicações efetuadas, nem os locais onde estas comunicações ocorreram ou a frequência destas com certas pessoas durante um dado período, pelo que não fornecem, com exceção das coordenadas dos utilizadores dos meios de comunicações eletrónicas, como os seus endereços, nenhuma informação sobre as comunicações efetuadas nem, consequentemente, sobre a sua vida privada. Assim, a ingerência que uma conservação destes dados comporta não pode, em princípio, ser qualificada de grave (v., neste sentido, 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.ºs 157 e 158 e jurisprudência referida).

35 Nestas condições, só os objetivos de luta contra a criminalidade grave ou de prevenção de ameaças graves para a segurança pública podem justificar o acesso das autoridades públicas a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados e que permitem tirar conclusões precisas sobre a vida privada das pessoas em causa (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 54), sem que outros fatores respeitantes à proporcionalidade de um pedido de acesso, como a duração do período em relação ao qual o

acesso a esses dados é solicitado, possam ter por efeito que o objetivo de prevenção, de investigação, de deteção e de perseguição de infrações penais em geral seja suscetível de justificar esse acesso.

36 Há que salientar que o acesso a um conjunto de dados de tráfego ou de dados de localização, como os conservados ao abrigo do artigo 111[1] da Lei Relativa às Comunicações Eletrónicas, é efetivamente suscetível de permitir tirar conclusões precisas, ou mesmo muito precisas, sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os locais de residência permanentes ou temporários, as deslocações diárias ou outras, as atividades exercidas, as relações sociais dessas pessoas e os meios sociais frequentados por estas (v., neste sentido, 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 117).

37 É certo que, como sugere o órgão jurisdicional de reenvio, quanto mais longo for o período em relação ao qual o acesso é solicitado, mais importante é, em princípio, a quantidade de dados suscetíveis de ser conservados pelos prestadores de serviços de comunicações eletrónicas, relativos às comunicações eletrónicas passadas, aos locais de residência frequentados e às deslocações efetuadas pelo utilizador de um meio de comunicação eletrónica, permitindo, assim, tirar, a partir dos dados consultados, um maior número de conclusões sobre a vida privada desse utilizador. Uma conclusão análoga pode ser tirada no que respeita às categorias de dados solicitados.

38 Por conseguinte, é para satisfazer a exigência de proporcionalidade, segundo a qual as derrogações e as limitações à proteção dos dados pessoais devem ocorrer na estrita medida do necessário (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 130 e jurisprudência referida), que cabe às autoridades nacionais competentes assegurar, em cada caso concreto, que tanto a categoria ou as categorias de dados visados como a duração do período em relação ao qual o acesso a esses dados é solicitado sejam, consoante as circunstâncias do caso, limitadas ao estritamente necessário para os fins do inquérito em questão.

39 Todavia, a ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que comporta o acesso, por uma autoridade pública, a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados, apresenta, de qualquer modo, um caráter grave independentemente da duração do período em relação ao qual o acesso aos referidos dados é solicitado e da quantidade ou da natureza dos dados disponíveis em relação a esse período, quando, como no processo principal, esse conjunto de dados seja suscetível de permitir tirar conclusões precisas sobre a vida privada da pessoa ou das pessoas em causa.

40 A este respeito, mesmo o acesso a uma quantidade limitada de dados de tráfego ou de dados de localização ou o acesso a dados por um curto período pode ser suscetível de fornecer informações precisas sobre a vida privada de um utilizador de um meio de comunicação eletrónica. Além disso, a quantidade dos dados disponíveis e as informações concretas sobre a vida privada da pessoa em causa deles decorrentes são circunstâncias que só podem ser apreciadas após a consulta dos referidos dados. Ora, a autorização de acesso concedida pelo órgão jurisdicional ou pela autoridade independente competente ocorre, necessariamente, antes de os dados e as informações deles decorrentes poderem ser consultados. Assim, a apreciação da gravidade da ingerência que o acesso constitui é feita necessariamente em função do risco, para a

vida privada das pessoas em causa, que geralmente corresponde à categoria de dados solicitados, sem que seja necessário, por outro lado, saber se as informações relativas à vida privada deles decorrentes apresentam ou não, concretamente, caráter sensível.

41 Por último, tendo em conta que o órgão jurisdicional de reenvio é chamado a conhecer de um pedido que conclui pela inadmissibilidade dos relatórios elaborados a partir dos dados de tráfego e dos dados de localização, pelo facto de as disposições do artigo 111[1] da Lei Relativa às Comunicações Eletrónicas serem contrárias ao artigo 15.º, n.º 1, da Diretiva 2002/58 tanto no que respeita à conservação dos dados como ao acesso a estes, recorde-se que, no estado atual do direito da União, cabe, em princípio, exclusivamente ao direito nacional determinar as regras relativas à admissibilidade e à apreciação, no âmbito de um processo penal instaurado contra pessoas suspeitas de atos de criminalidade, de informações e de elementos de prova que foram obtidos mediante uma conservação generalizada e indiferenciada desses dados, contrária ao direito da União (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 222), ou ainda mediante um acesso das autoridades nacionais aos referidos dados, contrário a esse direito.

42 Com efeito, é jurisprudência constante que, na falta de regras da União na matéria, cabe à ordem jurídica interna de cada Estado-Membro, por força do princípio da autonomia processual, regular as modalidades processuais dos recursos judiciais destinados a assegurar a salvaguarda dos direitos conferidos aos litigantes pelo direito da União, desde que, no entanto, não sejam menos favoráveis do que as que regulam situações semelhantes sujeitas ao direito interno (princípio da equivalência) e não tornem impossível, na prática, ou excessivamente difícil o exercício dos direitos conferidos pelo direito da União (princípio da efetividade) (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 223 e jurisprudência referida).

43 Quanto, mais especificamente, ao princípio da efetividade, importa recordar que as regras nacionais relativas à admissibilidade e à exploração das informações e dos elementos de prova têm por objetivo, em razão das opções efetuadas pelo direito nacional, evitar que informações e elementos de prova que foram obtidos de maneira ilegal prejudiquem indevidamente uma pessoa suspeita de ter cometido infrações penais. Ora, este objetivo pode, segundo o direito nacional, ser alcançado não só através de uma proibição de explorar tais informações e tais elementos de prova mas igualmente através de regras e práticas nacionais que regulem a apreciação e a ponderação das informações e dos elementos de prova, ou mesmo através da tomada em consideração do seu caráter ilegal no âmbito da determinação da pena (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 225).

44 A necessidade de excluir informações e elementos de prova obtidos em violação das disposições do direito da União deve ser apreciada tendo em conta, designadamente, o risco que a admissibilidade dessas informações e elementos de prova comporta para o respeito do princípio do contraditório e, portanto, do direito a um processo equitativo. Ora, um órgão jurisdicional que considera que uma parte não está em condições de comentar eficazmente um meio de prova abrangido por um domínio que escapa ao conhecimento dos juízes e que é suscetível de influenciar de modo preponderante a apreciação dos factos deve declarar uma violação do direito a um processo equitativo e excluir esse meio de prova a fim de evitar tal violação. Por conseguinte, o princípio da efetividade obriga o juiz penal nacional a afastar informações e elementos de prova que foram obtidos através de uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização incompatível com o direito da União ou ainda através de um acesso da autoridade competente a esses dados em violação desse direito, no âmbito de um processo penal

instaurado contra pessoas suspeitas de atos de criminalidade, se essas pessoas não estiverem em condições de comentar eficazmente essas informações e esses elementos de prova, provenientes de um domínio que escapa ao conhecimento dos juízes e que são suscetíveis de influenciar de modo preponderante a apreciação dos factos (v., neste sentido, 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.os 226 e 227).

45 Tendo em conta as considerações precedentes, há que responder à primeira e segunda questões que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que permite o acesso de autoridades públicas a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados e de permitir tirar conclusões precisas sobre a sua vida privada, para fins de prevenção, de investigação, de deteção e de perseguição de infrações penais, sem que esse acesso esteja circunscrito a processos que visem a luta contra a criminalidade grave ou a prevenção de ameaças graves à segurança pública, independentemente da duração do período em relação ao qual o acesso aos referidos dados é solicitado e da quantidade ou da natureza dos dados disponíveis sobre tal período.

Quanto à terceira questão

46 Com a sua terceira questão prejudicial, 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, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que atribui competência ao Ministério Público, cuja missão é dirigir a instrução penal e exercer, sendo caso disso, a ação pública num processo posterior, para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal.

47 O órgão jurisdicional de reenvio precisa, a este respeito, que, embora o Ministério Público estónio seja obrigado, em conformidade com o direito nacional, a agir de modo independente, esteja sujeito unicamente à lei e deva examinar os elementos incriminatórios e ilibatórios no decurso da instrução do processo, o objetivo desta não deixa de ser a recolha de elementos de prova e a reunião dos outros requisitos necessários à organização de um processo penal. É esta mesma autoridade que representa a ação pública num processo penal, sendo, portanto, igualmente parte no processo. Além disso, resulta dos autos de que dispõe o Tribunal de Justiça, como igualmente confirmaram o Governo estónio e o Prokuratuur na audiência, que o Ministério Público estónio está organizado hierarquicamente e que os pedidos de acesso aos dados de tráfego e aos dados de localização não estão sujeitos a uma exigência de forma especial e podem ser apresentados pelo próprio procurador. Por último, as pessoas a cujos dados pode ser concedido acesso não são apenas as pessoas suspeitas de estar envolvidas numa infração penal.

48 Como o Tribunal de Justiça já declarou, é verdade que cabe ao direito nacional determinar as condições em que os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes o acesso aos dados de que dispõem. No entanto, para satisfazer a exigência de proporcionalidade, tal regulamentação deve prever regras claras e precisas que regulem o alcance e a aplicação da medida em causa e imponham exigências mínimas, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente esses dados pessoais contra os riscos de abuso. Essa regulamentação deve ser legalmente vinculativa em direito interno e indicar em que circunstâncias e sob que condições uma medida que preveja o tratamento desses dados pode ser

tomada, garantindo, assim, que a ingerência seja limitada ao estritamente necessário (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.os 117 e 118; de 6 de outubro de 2020, Privacy International, C-623/17, EU:C:2020:790, n.º 68; e 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 132 e jurisprudência referida).

49 Em especial, uma regulamentação nacional que regula o acesso das autoridades competentes a dados de tráfego e a dados de localização conservados, adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, não se pode limitar a exigir que o acesso das autoridades aos dados responda à finalidade prosseguida por essa regulamentação, mas deve igualmente prever as condições materiais e processuais que regem essa utilização (Acórdãos de 6 de outubro de 2020, Privacy International, C-623/17, EU:C:2020:790, n.º 77, e 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 176 e jurisprudência referida).

50 Assim, e uma vez que um acesso geral a todos os dados conservados, independentemente de qualquer ligação, no mínimo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário, a regulamentação nacional em causa deve basear-se em critérios objetivos para definir as circunstâncias e as condições em que o acesso aos dados em causa deve ser concedido às autoridades nacionais competentes. A este respeito, tal acesso só poderá, em princípio, ser concedido, em relação com o objetivo de luta contra a criminalidade, aos dados de pessoas que se suspeita estarem a planear, irem cometer ou terem cometido uma infração grave ou, ainda, estarem envolvidas de uma maneira ou de outra nessa infração. Todavia, em situações especiais, como aquelas em que os interesses vitais da segurança nacional, da defesa ou da segurança pública sejam ameaçados por atividades terroristas, o acesso aos dados de outras pessoas poderia igualmente ser concedido quando existam elementos objetivos que permitam considerar que esses dados poderiam, num caso concreto, contribuir efetivamente para a luta contra essas atividades (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 119, e 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 188).

51 A fim de garantir, na prática, o pleno respeito destes requisitos, é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja, em princípio, sujeito a uma fiscalização prévia efetuada por um órgão jurisdicional ou por uma entidade administrativa independente e que a decisão desse órgão jurisdicional ou dessa entidade seja tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de perseguição penal. Em caso de urgência devidamente justificada, a fiscalização deve ser efetuada em prazos curtos (v., neste sentido, 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 189 e jurisprudência referida).

52 Essa fiscalização prévia exige, designadamente, como salientou, em substância, o advogado-geral no n.º 105 das suas conclusões, que o órgão jurisdicional ou a entidade encarregada de efetuar a referida fiscalização prévia disponha de todas as atribuições e apresente todas as garantias necessárias com vista a assegurar uma conciliação dos diferentes interesses e direitos em causa. Quanto, mais especificamente, a um inquérito penal, tal fiscalização exige que esse órgão jurisdicional ou essa entidade possa assegurar um justo equilíbrio entre, por um lado, os interesses ligados às necessidades do inquérito no âmbito da luta contra a criminalidade e, por outro, os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas às quais o acesso diz respeito.

53 Quando essa fiscalização não é efetuada por um órgão jurisdicional, mas por uma entidade administrativa independente, esta deve gozar de um estatuto que lhe permita agir, quando desempenha as suas missões, de maneira objetiva e imparcial e, para esse efeito, deve estar ao abrigo de qualquer influência externa [v., neste sentido, Acórdão de 9 de março de 2010, Comissão/Alemanha, C-518/07, EU:C:2010:125, n.º 25, e Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.ºs 229 e 230].

54 Resulta das considerações precedentes que a exigência de independência que a autoridade encarregada de exercer a fiscalização prévia, recordada no n.º 51 do presente acórdão, deve satisfazer impõe que essa autoridade tenha a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, de modo que a primeira esteja em condições de exercer essa fiscalização de maneira objetiva e imparcial, ao abrigo de qualquer influência externa. Em especial, no domínio penal, a exigência de independência implica, como salientou o advogado-geral, em substância, no n.º 126 das suas conclusões, que a autoridade encarregada dessa fiscalização prévia, por um lado, não esteja envolvida na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal.

55 Não é esse o caso de um Ministério Público que dirige o inquérito e exerce, sendo caso disso, a ação pública. Com efeito, o Ministério Público tem por missão, não decidir com total independência um litígio mas submetê-lo, se necessário, ao órgão jurisdicional competente, enquanto parte no processo que exerce a ação penal.

56 A circunstância de o Ministério Público ser obrigado, em conformidade com as regras que regulam as suas competências e o seu estatuto, a verificar os elementos incriminatórios e ilibatórios, a garantir a legalidade da instrução do processo e a agir unicamente nos termos da lei e segundo a sua convicção não basta para lhe conferir o estatuto de terceiro em relação aos interesses em causa na aceção descrita no n.º 52 do presente acórdão.

57 Daqui resulta que o Ministério Público não está em condições de efetuar a fiscalização prévia referida no n.º 51 do presente acórdão.

58 Tendo o órgão jurisdicional de reenvio suscitado, por outro lado, a questão de saber se a falta de fiscalização efetuada por uma autoridade independente pode ser suprida por uma fiscalização posterior, exercida por um órgão jurisdicional, da legalidade do acesso de uma autoridade nacional aos dados de tráfego e aos dados de localização, importa salientar que a fiscalização independente deve ser efetuada, como exige a jurisprudência recordada no n.º 51 do presente acórdão, previamente a qualquer acesso, salvo em caso de urgência devidamente justificada, devendo, nesse caso, a fiscalização ser efetuada em prazos curtos. Como salientou o advogado-geral no n.º 128 das suas conclusões, essa fiscalização posterior não permitiria responder ao objetivo de uma fiscalização prévia, que consiste em impedir que seja autorizado um acesso aos dados em causa que ultrapasse os limites do estritamente necessário.

59 Nestas condições, há que responder à terceira questão prejudicial que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que atribui competência ao Ministério Público, cuja missão é dirigir a instrução do processo penal e exercer, sendo caso disso, a ação pública num processo posterior, para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal.

Quanto às despesas

60 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 (Grande Secção) declara:

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), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que permite o acesso de autoridades públicas a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados e de permitir tirar conclusões precisas sobre a sua vida privada, para fins de prevenção, de investigação, de deteção e de perseguição de infrações penais, sem que esse acesso esteja circunscrito a processos que visem a luta contra a criminalidade grave ou a prevenção de ameaças graves à segurança pública, independentemente da duração do período em relação ao qual o acesso aos referidos dados é solicitado e da quantidade ou da natureza dos dados disponíveis sobre tal período.**

2) **O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que atribui competência ao Ministério Público, cuja missão é dirigir a instrução do processo penal e exercer, sendo caso disso, a ação pública num processo posterior, para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal.**

Assinaturas