Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

30 de abril de 2024*

«Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Confidencialidade das comunicações — Prestadores de serviços de comunicações eletrónicas — Diretiva 2002/58/CE — 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 — Acesso a esses dados pedido por uma autoridade nacional competente para efeitos de repressão de infrações de furtos com circunstâncias agravantes — Definição do conceito de "infração grave" cuja repressão é suscetível de justificar uma ingerência grave nos direitos fundamentais — Competência dos Estados-Membros — Princípio da proporcionalidade — Âmbito da fiscalização prévia do juiz sobre os pedidos de acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas»

No processo C-178/22,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, apresentado pelo Giudice delle indagini preliminari presso il Tribunale di Bolzano (Juiz de Instrução de Bolzano, Itália), por Decisão de 20 de fevereiro de 2022, que deu entrada no Tribunal de Justiça em 8 de março de 2022, nos processos penais contra

Desconhecidos,

sendo interveniente:

Procura della Repubblica presso il Tribunale di Bolzano,

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: K. Lenaerts, presidente, L. Bay Larsen, vice-presidente, A. Arabadjiev, A. Prechal, K. Jürimäe, T. von Danwitz e Z. Csehi, presidentes de secção, J.-C. Bonichot, S. Rodin, P. G. Xuereb (relator), D. Gratsias, M. L. Arastey Sahún e M. Gavalec, juízes,

advogado-geral: A. M. Collins,

secretário: C. Di Bella, administrador,

vistos os autos e após a audiência de 21 de março de 2023,

* Língua do processo: italiano.

vistas as observações apresentadas:

– em representação da Procura della Repubblica presso il Tribunale di Bolzano, por F. Iovene, sostituto procuratore della Repubblica,

– em representação do Governo Italiano, por G. Palmieri, na qualidade de agente, assistida por S. Faraci, avvocato dello Stato,

– em representação do Governo Checo, por A. Edelmannová, O. Serdula, M. Smolek, T. Suchá 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, Chief State Solicitor, A. Joyce e M. Tierney, na qualidade de agentes, assistidos por D. Fennelly, BL,

– em representação do Governo Francês, por A. Daniel, A.-L. Desjonquères, B. Fodda e J. Illouz, na qualidade de agentes,

– em representação do Governo Cipriota, por E. Neophytou, na qualidade de agente,

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

– em representação do Governo Neerlandês, por M. K. Bulterman, A. Hanje e J. Langer, na qualidade de agentes,

– em representação do Governo Austríaco, por A. Posch, J. Schmoll, C. Gabauer, K. Ibili e E. Samoilova, na qualidade de agentes,

– em representação do Governo Polaco, por B. Majczyna, D. Lutostańska e J. Sawicka, na qualidade de agentes,

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

ouvidas as conclusões do advogado-geral na audiência de 8 de junho 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»), 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 uma promoção junto do Giudice delle indagini preliminari presso il Tribunale di Bolzano (Juiz de Instrução de Bolzano, Itália) pela Procura della Repubblica presso il Tribunale di Bolzano (Ministério Público junto do Tribunal de Bolzano, Itália) (a seguir «Ministério Público»), no sentido de ser autorizado a aceder a dados pessoais conservados por prestadores de serviços de comunicações eletrónicas para identificar os autores de dois furtos de telemóvel com circunstâncias agravantes.

Quadro jurídico

Direito da União

Diretiva 2002/58

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 comunitário. 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 do Homem e das Liberdades Fundamentais.»

4 Nos termos do artigo 2.º desta diretiva, 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 O artigo 5.º da referida diretiva, sob a epígrafe «Confidencialidade das comunicações», prevê:

«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 mesma diretiva, 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, n.º 1, desta diretiva, sob a epígrafe «Aplicação de determinadas disposições da Diretiva [95/46]», enuncia:

«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 comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º [TUE].»

Direito italiano

Decreto Legislativo n.º 196/2003

9 O artigo 132.º, n.º 3, do decreto legislativo n.º 196 — Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE [Decreto Legislativo n.º 196, Código em matéria de Proteção de Dados Pessoais, que adapta o direito nacional ao Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE], de 30 de junho de 2003 (suplemento ordinário à GURI n.º 174, de 29 de julho de 2003), na sua redação aplicável ao litígio no processo principal (a seguir «Decreto Legislativo n.º 196/2003»), prevê o seguinte:

«Dentro do prazo de conservação imposto por lei, no caso de haver indícios suficientes de infrações para as quais a lei preveja pena de prisão perpétua ou pena máxima de prisão não inferior a três anos, determinada nos termos do artigo 4.º do [codice di procedura penale (Código de Processo Penal)], e de crimes de ameaça, assédio e perturbação das pessoas por meio de telefone, quando a ameaça, o assédio e a perturbação sejam graves, se forem relevantes para o apuramento dos factos, os dados são obtidos mediante autorização prévia emitida pelo juiz por despacho fundamentado, promovida pelo Ministério Público ou a requerimento da defesa do arguido, da pessoa sob investigação, do lesado ou de outros particulares.»

10 O n.º 3-*bis* deste artigo dispõe:

«Quando houver motivo de urgência e fundamento para considerar que do atraso possa decorrer grave prejuízo para a investigação, o Ministério Público ordena a obtenção dos dados por despacho fundamentado que será comunicado imediatamente, e em qualquer caso no prazo máximo de 48 horas, ao juiz competente para emitir a autorização na forma ordinária. O juiz, nas 48 horas seguintes, decide sobre a validação por despacho fundamentado.»

11 Por último, nos termos do n.º 3-*quater* do referido artigo: «[o]s dados obtidos em violação do disposto nos n.os 3 e 3-*bis* não podem ser utilizados.»

Código Penal

12 O artigo 624.º do codice penale (Código Penal), sob a epígrafe «Furto», dispõe:

«Quem se apropriar de coisa móvel alheia, subtraindo-o ao seu detentor, com o objetivo de obter lucro para si próprio ou para outrem, é punido com pena de prisão de seis meses a três anos e multa de 154 a 516 euros.

[…]

O crime é punível mediante queixa da pessoa lesada, exceto se estiverem reunidos um ou mais pressupostos referidos no artigo 61.º, n.º 7, e no artigo 625.º»

13 O artigo 625.º, primeiro parágrafo, do Código Penal, sob a epígrafe «Circunstâncias agravantes», prevê:

«O ato referido no artigo 624.º é punível com pena de prisão de dois a seis anos e multa de 927 a 1 500 euros:

[…]

2) se o culpado utilizar a violência contra os bens ou utilizar qualquer meio fraudulento;

3) se o culpado tiver consigo armas ou estupefacientes, sem os utilizar;

4) se se tratar de carteirismo;

5) se o ato for cometido por três ou mais pessoas, ou mesmo por uma única pessoa disfarçada ou que se faça passar por funcionário público ou por uma pessoa que exerce funções públicas;

6) se o ato disser respeito à bagagem de passageiros em qualquer veículo, nas estações ferroviárias, nos aeroportos ou nos cais, nos hotéis ou em qualquer estabelecimento que comercialize alimentos ou bebidas;

7) se o ato disser respeito a bens presentes em serviços públicos ou em estabelecimentos públicos, ou perdidos a favor do Estado ou apreendidos, ou expostos por necessidade ou costume ou com destino à fé pública, ou destinados ao serviço público ou de utilidade pública, à defesa ou à veneração;

7-*bis*) se o ato disser respeito a componentes metálicos ou a outros materiais retirados de infraestruturas destinadas ao fornecimento de energia, de serviços de transporte, de telecomunicações ou de outros serviços públicos e operados por entidades públicas ou privadas no âmbito de uma concessão pública;

8) se o ato disser respeito a três ou mais cabeças de gado em manada, ou a bovinos ou equídeos, mesmo não reunidos em manada;

8-*bis*) se o ato for cometido em meios de transporte público;

8-*ter*) se o ato for cometido em relação a uma pessoa que esteja a utilizar ou que acabe de utilizar os serviços de uma instituição de crédito, de uma estação de correios ou de um caixa-automático.»

Código de Processo Penal

14 Nos termos do artigo 4.º do Código de Processo Penal, sob a epígrafe «Regras de determinação da competência»:

«A competência é determinada em função da pena prevista por lei para cada crime consumado ou tentado. A continuação, a reincidência e as circunstâncias do crime não são tidas em conta, com

exceção das circunstâncias agravantes para as quais a lei preveja uma pena de tipo diferente da pena ordinária para a infração e das penas especialmente agravadas.»

15 O artigo 269.º, n.º 2, deste código prevê:

«[…] As gravações são conservadas até ser proferida sentença definitiva. Todavia, para proteger a confidencialidade, os interessados podem, quando os documentos não sejam necessários para efeitos do processo, requerer ao juiz que autorizou ou validou a interceção a destruição das gravações.»

Litígio no processo principal e questão prejudicial

16 Na sequência de duas queixas apresentadas por furtos de telemóvel cometidos em 27 de outubro e 20 de novembro de 2021, respetivamente, o Ministério Público instaurou, nos termos dos artigos 624.º e 625.º do Código Penal, dois processos penais contra autores desconhecidos por crimes de furto com circunstâncias agravantes.

17 Para identificar os autores desses furtos, o Ministério Público pediu, com base no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003, ao Giudice delle indagini preliminari presso il Tribunale di Bolzano (Juiz de Instrução de Bolzano), o órgão jurisdicional de reenvio, em 7 de dezembro e 30 de dezembro de 2021, respetivamente, autorização para recolher, junto de todas as companhias telefónicas, os extratos telefónicos dos telefones furtados. Estes pedidos visavam «todos os dados na [posse das companhias telefónicas], com o método de tráfego e localização (em especial, os assinantes e eventualmente os números [relativos à Identidade Internacional do Equipamento Móvel (IMEI) dos equipamentos] chamados ou recebidos, sítios visitados e acedidos, horário e duração da chamada ou da ligação e indicação das células ou repetidores em questão, assinantes e números IMEI [dos equipamentos] emitentes e destinatários dos SMS ou MMS e, sempre que possível, informações gerais sobre os respetivos titulares) das conversas e comunicações telefónicas e ligações efetuadas, incluindo em *roaming*, de entrada e saída igualmente no caso de chamadas sem faturação (toques) desde a data do furto até à data de elaboração do pedido».

18 O órgão jurisdicional de reenvio tem dúvidas quanto à compatibilidade do artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 com o artigo 15.º, n.º 1, da Diretiva 2002/58, conforme interpretado pelo Tribunal de Justiça no seu Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152).

19 Recorda que, nos termos do n.º 45 desse acórdão, as disposições nacionais que permitem o acesso das autoridades públicas a registos telefónicos, que contenham um conjunto de dados de tráfego ou de dados de localização suscetíveis de permitir tirar conclusões específicas sobre a vida privada do utilizador em causa, não são justificáveis, tendo em conta o princípio da proporcionalidade previsto no artigo 52.º, n.º 1, da Carta e a gravidade da ingerência nos direitos fundamentais à vida privada, à proteção dos dados pessoais e à liberdade de expressão e de informação, conforme garantidos, respetivamente, nos artigos 7.º, 8.º e 11.º da Carta, se se destinarem a punir crimes graves, como as ameaças graves contra a segurança pública, entendida como a do Estado, e outras formas de criminalidade grave.

20 A este respeito, o órgão jurisdicional de reenvio indica que, no seu Acórdão n.º 33116, de 7 de setembro de 2021, a Corte suprema di cassazione (Supremo Tribunal de Cassação, Itália) considerou que, atenta a margem de interpretação em torno da determinação dos crimes que

constituem ameaças graves contra a segurança pública ou outras formas de criminalidade grave na aceção da jurisprudência do Tribunal de Justiça, esta jurisprudência não apresentava as características exigidas para ser diretamente aplicada pelos tribunais nacionais. Consequentemente, o legislador italiano alterou o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 para qualificar de infrações graves, relativamente aos quais podem ser obtidos os extratos telefónicos, os crimes que a lei pune com uma pena de prisão máxima «não inferior a três anos».

21 Segundo o órgão jurisdicional de reenvio, este limiar de três anos a partir do qual a pena máxima de prisão com que um crime é punível justifica que esse crime possa dar origem à comunicação de extratos telefónicos às autoridades públicas é de tal ordem que esses registos lhes podem ser comunicados para punir os crimes que apenas causem uma perturbação social limitada e que só sejam puníveis com base numa queixa de um particular, nomeadamente os furtos de baixo valor como os furtos de telemóvel ou de bicicleta.

22 A disposição nacional em causa viola, assim, o princípio da proporcionalidade previsto no artigo 52.º, n.º 1, da Carta, que exige que seja ponderada a gravidade do crime a ser punido com os direitos fundamentais que são lesados para o punir. Com efeito, este princípio opõe-se a que uma violação dos direitos fundamentais garantidos pelos artigos 7.º, 8.º e 11.º da Carta seja justificada por um processo relativo a um crime como o furto.

23 O órgão jurisdicional de reenvio especifica que os tribunais italianos dispõem de uma margem de apreciação muito restrita para recusar a autorização para obter registos telefónicos, uma vez que, nos termos da disposição em causa, a autorização deve ser concedida se existirem «indícios suficientes de infrações» e se os dados solicitados forem «relevantes para o apuramento dos factos». Os tribunais italianos não dispõem, portanto, de nenhuma margem de apreciação quanto à gravidade concreta da infração objeto do inquérito. Esta apreciação foi efetuada a título definitivo pelo legislador italiano quando estabeleceu que a autorização para obter os dados devia ser concedida, nomeadamente, para todos os crimes puníveis com pena de prisão máxima não inferior a três anos.

24 Nestas condições, o Giudice delle indagini preliminari presso il Tribunale di Bolzano (Juiz de Instrução de Bolzano) decidiu suspender a instância e submeter ao Tribunal de Justiça a seguinte questão prejudicial:

«O artigo 15.º, n.º 1, da [Diretiva 2002/58] opõe-se à disposição nacional constante do artigo 132.º[, n.º 3,] do Decreto Legislativo [n.º 196/2003], que […] dispõe o seguinte:

"3. Dentro do prazo de conservação imposto por lei, no caso de haver indícios suficientes de infrações penais para as quais a lei prevê pena de prisão perpétua ou pena máxima de prisão não inferior a 3 anos, determinada nos termos do artigo 4.º do Código de Processo Penal, e de infrações de ameaça, assédio e perturbação das pessoas por meio de telefone, quando a ameaça[, o assédio] e a perturbação sejam graves, se forem relevantes para o apuramento dos factos, os dados são obtidos mediante autorização prévia emitida pelo juiz por despacho fundamentado, requerida pelo Ministério Público ou a pedido do advogado de defesa do arguido, da pessoa sob investigação, da pessoa lesada ou de outros particulares"?»

Quanto à admissibilidade do pedido de decisão prejudicial

25 O Governo Italiano e a Irlanda sustentam que o pedido de decisão prejudicial é parcialmente inadmissível. Referem que os pedidos de acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas foram apresentados pelo Ministério Público, com base no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003, para punir os crimes de furto de telemóvel com circunstâncias agravantes. Ora, com a sua questão prejudicial, o órgão jurisdicional de reenvio pergunta também ao Tribunal de Justiça se o artigo 15.º, n.º 1, da Diretiva 2002/58 se opõe a uma disposição nacional que permite obter acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas para punir outras infrações abrangidas pelo artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 diferentes das que estão em causa no processo principal, como o furto simples ou o assédio grave por telefone. Por conseguinte, o pedido de decisão prejudicial apresenta um caráter hipotético na parte que visa essas outras infrações.

26 A este respeito, recorde-se que, segundo jurisprudência constante, no âmbito da cooperação entre o Tribunal de Justiça e os órgãos jurisdicionais nacionais instituída pelo artigo 267.º TFUE, o juiz nacional, a quem foi submetido o litígio e que deve assumir a responsabilidade pela decisão judicial a tomar, tem competência exclusiva para apreciar, tendo em conta as especificidades do processo, tanto a necessidade de uma decisão prejudicial para poder proferir a sua decisão como a pertinência das questões que submete ao Tribunal de Justiça. Consequentemente, quando as questões submetidas sejam relativas à interpretação do direito da União, o Tribunal de Justiça é, em princípio, obrigado a pronunciar-se [Acórdão de 21 de março de 2023, Mercedes-Benz Group (Responsabilidade dos fabricantes de veículos munidos de dispositivos manipuladores), C-100/21, EU:C:2023:229, n.º 52 e jurisprudência referida].

27 Daqui se conclui que as questões relativas ao direito da União gozam de uma presunção de pertinência. O Tribunal de Justiça só pode recusar pronunciar-se sobre uma questão prejudicial submetida por um órgão jurisdicional nacional se for manifesto que a interpretação do direito da União solicitada não tem nenhuma relação com a realidade ou com o objeto do litígio no processo principal, quando o problema for hipotético ou ainda quando o Tribunal de Justiça não dispuser dos elementos de facto e de direito necessários para dar uma resposta útil às questões que lhe são submetidas [Acórdão de 21 de março de 2023, Mercedes-Benz Group (Responsabilidade dos fabricantes de veículos munidos de dispositivos manipuladores), C-100/21, EU:C:2023:229, n.º 53 e jurisprudência referida].

28 Ora, ao reproduzir integralmente o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003, a questão prejudicial, embora não distinga os tipos de infrações aos quais esta disposição se aplica, abrange, necessariamente, os crimes de furto com circunstâncias agravantes relativamente aos quais os pedidos de autorização de acesso aos dados pessoais foram apresentados no processo principal.

29 Por conseguinte, esta questão não tem caráter hipotético e é, portanto, admissível.

Quanto à questão prejudicial

30 Como refere o Governo Francês nas suas observações escritas, a questão submetida pelo órgão jurisdicional de reenvio, tal como foi formulada, convida o Tribunal de Justiça a pronunciar-se sobre a compatibilidade do artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 com o artigo 15.º, n.º 1, da Diretiva 2002/58.

31 A este respeito, importa lembrar que, no âmbito do processo instituído pelo artigo 267.º TFUE, o Tribunal de Justiça não é competente para se pronunciar sobre a interpretação de disposições legislativas ou regulamentares nacionais nem sobre a conformidade de tais disposições com o direito da União. Com efeito, resulta de jurisprudência constante que, no âmbito de um reenvio prejudicial ao abrigo do artigo 267.º TFUE, o Tribunal de Justiça apenas pode interpretar o direito da União dentro dos limites das competências atribuídas à União [Acórdão de 14 de dezembro de 2023, Getin Noble Bank (Prazo de prescrição das ações de restituição), C-28/22, EU:C:2023:992, n.º 53 e jurisprudência referida].

32 No entanto, decorre de jurisprudência constante que, perante questões formuladas de maneira inadequada ou que ultrapassem o âmbito das funções que são atribuídas ao Tribunal de Justiça pelo artigo 267.º TFUE, cabe a este último extrair do conjunto dos elementos fornecidos pelo órgão jurisdicional nacional, designadamente da fundamentação da decisão de reenvio, os elementos do direito da União que requerem uma interpretação, tendo em conta o objeto do litígio. Nesta ótica, incumbe ao Tribunal de Justiça, se necessário, reformular as questões que lhe foram submetidas (Acórdão de 14 de dezembro de 2023, Sparkasse Südpfalz, C-206/22, EU:C:2023:984, n.º 20 e jurisprudência referida).

33 Além disso, o Tribunal de Justiça pode ser levado a tomar em consideração normas de direito da União a que o juiz nacional não fez referência no enunciado da sua questão (Acórdão de 17 de novembro de 2022, Harman International Industries, C-175/21, EU:C:2022:895, n.º 31 e jurisprudência referida).

34 Em face do exposto, há que considerar que, 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, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma disposição nacional que impõe ao juiz nacional, que intervém no âmbito de uma fiscalização prévia efetuada na sequência de um pedido fundamentado de acesso a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de permitir tirar conclusões específicas sobre a vida privada de um utilizador de um meio de comunicação eletrónica, conservados pelos prestadores de serviços de comunicações eletrónicas, apresentado por uma autoridade nacional competente no âmbito de um inquérito penal, que autorize esse acesso se for pedido para efeitos da investigação de infrações penais puníveis, pelo direito nacional, com uma pena máxima de prisão não inferior a três anos, desde que existam indícios suficientes de tais infrações e esses dados sejam relevantes para o apuramento dos factos.

35 A título preliminar, importa recordar que, no que respeita aos pressupostos para o acesso aos dados de tráfego e aos dados de localização conservados pelos prestadores de serviços de comunicações eletrónicas poder, para efeitos de prevenção, de investigação, de deteção e de repressão de infrações penais, ser concedido a autoridades públicas, em aplicação de uma medida legislativa adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, o Tribunal de Justiça declarou que esse acesso só pode ser concedido se esses dados tiverem sido conservados por esses prestadores em conformidade com esta diretiva [v., neste sentido, Acórdão hoje proferido, La Quadrature du Net e o. (Dados pessoais e combate à contrafação), C-470/21, n.º 65 e jurisprudência referida]. O Tribunal de Justiça declarou igualmente que este 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 [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 30 e jurisprudência referida].

36 Também importa recordar a jurisprudência do Tribunal de Justiça segundo a qual só os objetivos de luta contra a criminalidade grave ou de prevenção de ameaças graves para a segurança pública podem justificar a ingerência grave nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que 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 permitam tirar conclusões específicas sobre a vida privada das pessoas em causa, 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 pedido, possam ter por efeito que o objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral seja suscetível de justificar esse acesso [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 35 e jurisprudência referida].

37 Com a sua questão prejudicial, o órgão jurisdicional de reenvio pretende saber, em substância, se essa ingerência grave pode ser autorizada para infrações como as visadas pela regulamentação nacional em causa no processo principal.

38 No que respeita, antes de mais, à questão de saber se os acessos como os que estão em causa podem ser qualificados de ingerência grave nos direitos fundamentais garantidos nos artigos 7.º e 8.º da Carta, refira-se que, para identificar os presumíveis autores dos furtos que estão na origem desse litígio, o Ministério Público, para cada um dos telemóveis em causa, pediu ao órgão jurisdicional de reenvio, com base no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003, autorização para recolher todos os dados na posse das companhias telefónicas, obtidos através de um método de rastreio e de localização das conversas e comunicações telefónicas e das ligações efetuadas com esses telefones. Esses pedidos diziam respeito, mais especificamente, aos assinantes e aos números IMEI dos aparelhos chamados ou recebidos, aos sítios visitados e acedidos, horário e duração das chamadas ou da ligação e indicação das células ou repetidores em questão, bem como aos assinantes e aos números IMEI dos equipamentos emitentes e destinatários dos SMS ou MMS.

39 O acesso a esse conjunto de dados de tráfego ou de dados de localização parece suscetível de permitir tirar conclusões específicas 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 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 36 e jurisprudência referida]. A ingerência nos direitos fundamentais garantidos nos artigos 7.º e 8.º da Carta causada pelo acesso a esses dados parece, portanto, suscetível de ser qualificada de grave.

40 Como resulta do n.º 39 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), esta apreciação não pode ser afastada pelo simples facto de os dois pedidos de acesso aos dados de tráfego ou aos dados de localização em causa apenas dizerem respeito a curtos períodos, de menos de dois meses, compreendidos entre as datas dos presumíveis furtos dos telemóveis e as datas em que esses pedidos foram redigidos, uma vez que os referidos pedidos diziam respeito a um conjunto desses dados suscetível de fornecer informações específicas sobre a vida privada das pessoas que utilizam os telemóveis em causa.

41 Do mesmo modo, é irrelevante, para apreciar a existência de uma ingerência grave nos direitos garantidos nos artigos 7.º e 8.º da Carta, a circunstância de os dados aos quais o Ministério Público pediu acesso não serem os dos proprietários dos telemóveis em causa, mas sim os das pessoas que comunicaram umas com as outras utilizando esses telefones depois dos presumíveis furtos. Com efeito, resulta do artigo 5.º, n.º 1, da Diretiva 2002/58 que a obrigação de princípio de garantir a confidencialidade das comunicações eletrónicas efetuadas através de uma rede pública de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis, bem como a confidencialidade dos respetivos dados de tráfego, visa as comunicações efetuadas pelos utilizadores dessa rede. Ora, o artigo 2.º, alínea a), desta diretiva define o conceito de «utilizador» como qualquer pessoa singular que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou profissionais, não sendo necessariamente assinante desse serviço.

42 Por conseguinte, tendo em conta a jurisprudência referida no n.º 36 do presente acórdão, uma vez que as ingerências nos direitos fundamentais causadas pelo acesso aos dados, como as que estão em causa no processo principal, são suscetíveis de serem consideradas graves, só podem ser justificadas pelos objetivos de luta contra a criminalidade grave ou de prevenção de ameaças graves para a segurança pública.

43 Em seguida, embora caiba 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, essa regulamentação deve prever regras claras e precisas que regulem o alcance e os pressupostos de aplicação desse acesso. Este só poderá, em princípio, ser concedido, em relação com o objetivo de luta contra a criminalidade, aos dados de pessoas que se suspeita estarem envolvidas numa infração grave. A fim de garantir, na prática, o pleno respeito destes pressupostos que garanta que a ingerência seja limitada ao estritamente necessário, é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja sujeito a uma fiscalização prévia efetuada por um tribunal ou por uma entidade administrativa independente [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.os 48 a 51].

44 Por último, no que respeita à definição do conceito de «infração grave», resulta da jurisprudência que, na medida em que a União não tenha legislado na matéria, a legislação penal e as regras de processo penal são da competência dos Estados-Membros. Todavia, estes devem exercer essa competência no respeito do direito da União (v., neste sentido, Acórdão de 26 de fevereiro de 2019, Rimšēvičs e BCE/Letónia, C-202/18 e C-238/18, EU:C:2019:139, n.º 57 e jurisprudência referida).

45 A este respeito, há que observar que a definição de infrações penais, circunstâncias atenuantes e agravantes e sanções reflete tanto as realidades sociais como os costumes jurídicos que variam não só entre os Estados-Membros mas também no tempo. Ora, estas realidades e costumes têm uma certa importância para determinar as infrações consideradas de caráter grave.

46 Por conseguinte, tendo em conta a repartição de competências entre a União e os Estados-Membros nos termos do TFUE e as diferenças importantes que existem entre os sistemas jurídicos dos Estados-Membros no domínio penal, há que considerar que incumbe aos Estados-Membros definir as «infrações graves» para efeitos da aplicação do artigo 15.º, n.º 1, da Diretiva 2002/58.

47 Todavia, a definição de «infrações graves» pelos Estados-Membros deve respeitar as exigências que decorrem deste 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.

48 A este respeito, importa relembrar que, na medida em que permite aos Estados-Membros adotarem medidas legislativas destinadas a «restringir o âmbito» dos direitos e obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58, como os que decorrem dos princípios da confidencialidade das comunicações e da proibição de armazenamento dos respetivos dados, o artigo 15.º, n.º 1, desta diretiva enuncia uma exceção à regra geral prevista nomeadamente nestes artigos 5.º, 6.º e 9.º e deve, assim, em conformidade com jurisprudência constante, ser objeto de interpretação estrita. Tal disposição não pode, portanto, justificar que a exceção à obrigação de princípio de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados se converta em regra, sob pena de esvaziar em grande medida o artigo 5.º da referida diretiva do seu alcance (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 40).

49 Além disso, resulta do artigo 15.º, n.º 1, terceiro período, da Diretiva 2002/58 que as medidas tomadas pelos Estados-Membros ao abrigo desta disposição devem respeitar os princípios gerais do direito da União, entre os quais figura o princípio da proporcionalidade, e assegurar o respeito dos direitos fundamentais garantidos pelos artigos 7.º, 8.º e 11.º da Carta (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 42).

50 Daqui resulta que os Estados-Membros não podem desvirtuar o conceito de «infração grave» e, por extensão, o de «criminalidade grave», nele incluindo, para efeitos da aplicação desse artigo 15.º, n.º 1, infrações que manifestamente não são graves, tendo em conta as condições sociais prevalecentes no Estado-Membro em causa, apesar de o legislador desse Estado-Membro ter previsto puni-las com uma pena máxima de prisão de três anos.

51 É, nomeadamente, para verificar a inexistência de tal desvirtuação que é essencial que, quando o acesso das autoridades nacionais competentes aos dados conservados comporta o risco de uma ingerência grave nos direitos fundamentais da pessoa em causa, esse acesso esteja sujeito a uma fiscalização prévia efetuada por um tribunal ou por uma entidade administrativa independente [v., neste sentido, Acórdão proferido hoje, La Quadrature du Net e o. (Dados pessoais e combate à contrafação), C-470/21, n.ºs 124 a 131].

52 No caso vertente, resulta da decisão de reenvio que o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 fixa os pressupostos para o acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas poder ser concedido por um juiz chamado a pronunciar-se sobre um pedido fundamentado de uma autoridade pública. Esta disposição define as infrações, para cuja repressão pode ser concedido o acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas, com referência a uma pena de prisão máxima não inferior a três anos. A disposição condiciona esse acesso a um duplo pressuposto de existirem «indícios suficientes de crimes» e de esses dados serem «relevantes para o apuramento dos factos».

53 No entanto, o órgão jurisdicional de reenvio interroga-se sobre se a definição, resultante desta disposição, de «infrações graves», para cuja repressão pode ser concedido o acesso aos dados, não é demasiado ampla, uma vez que abrange infrações que causem apenas uma perturbação social limitada.

54 A este respeito, refira-se, primeiro, que uma definição no sentido de que as «infrações graves», para cuja repressão o acesso pode ser concedido, são aquelas para as quais a pena máxima de prisão, pelo menos igual a uma duração que a lei determina, se baseia num critério objetivo. Tal está em conformidade com o pressuposto de a legislação nacional em causa se basear 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 (Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 105 e jurisprudência referida).

55 Segundo, decorre da jurisprudência referida no n.º 48 do presente acórdão que a definição dada, no direito nacional, das «infrações graves» que podem permitir o acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas, que permitam tirar conclusões específicas sobre a vida privada das pessoas em causa, não deve ser de tal modo ampla que o acesso a esses dados se torne mais a regra do que a exceção. Assim, não pode abranger a grande maioria das infrações penais, o que aconteceria se o limiar a partir do qual a pena de prisão máxima com que é punível uma infração justificasse que esta fosse qualificada de infração grave, fosse fixado a um nível excessivamente baixo.

56 Ora, um limiar fixado por referência a uma pena máxima de prisão de três anos não se afigura, a este respeito, excessivamente baixo (v., neste sentido, Acórdão de 21 de junho de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, n.º 150).

57 É certo que, uma vez que a definição de «infrações graves», para as quais o acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas pode ser pedido, não é estabelecida por referência a uma pena mínima aplicável mas sim a uma pena máxima aplicável, não se exclui que um acesso a dados que constitua uma ingerência grave nos direitos fundamentais possa ser pedido para efeitos de repressão de infrações que, na realidade, não pertencem à criminalidade grave (v., por analogia, Acórdão de 21 de junho de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, n.º 151).

58 A fixação de um limiar a partir do qual a pena de prisão máxima com que é punida uma infração justifica que esta seja qualificada de infração grave não é, todavia, necessariamente contrária ao princípio da proporcionalidade.

59 Por um lado, parece ser esse o caso de uma disposição como a que está em causa no processo principal, uma vez que visa, como resulta da decisão de reenvio, de maneira geral, o acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas, sem especificar a natureza desses dados. Assim, esta disposição parece abranger, nomeadamente, casos em que o acesso não pode ser qualificado de ingerência grave uma vez que não visa um conjunto de dados suscetível de permitir tirar conclusões específicas sobre a vida privada das pessoas em causa.

60 Por outro lado, o tribunal ou a entidade administrativa independente, que intervém no âmbito de uma fiscalização prévia efetuada na sequência de um pedido de acesso fundamentado, deve estar habilitado a recusar ou a restringir esse acesso quando verifica que a ingerência nos direitos fundamentais que esse acesso constitui é grave quando é manifesto que a infração em causa não está efetivamente abrangida pela criminalidade grave (v., por analogia, Acórdão de 21 de junho de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, n.º 152).

61 Com efeito, o tribunal ou a entidade competente de fiscalização deve estar em condições de assegurar um justo equilíbrio entre, por um lado, os interesses legítimos 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 cujos dados são afetados pelo acesso [Acórdão proferido hoje, La Quadrature du Net e o. (Dados pessoais e combate à contrafação), C-470/21, n.º 125 e jurisprudência referida].

62 Em especial, no âmbito da sua análise da proporcionalidade da ingerência causada nos direitos fundamentais da pessoa a que o pedido de acesso diz respeito, esse tribunal ou essa entidade deve poder excluir esse acesso quando este último é requerido no âmbito de repressão de uma infração que manifestamente não é grave, na aceção do n.º 50 do presente acórdão.

63 Resulta do exposto que há que responder à questão prejudicial que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º, e do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que não se opõe a uma disposição nacional que impõe ao juiz nacional, que intervém no âmbito de uma fiscalização prévia efetuada na sequência de um pedido fundamentado de acesso a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de permitir tirar conclusões específicas sobre a vida privada de um utilizador de um meio de comunicação eletrónica, conservados pelos prestadores de serviços de comunicações eletrónicas, apresentado por uma autoridade nacional competente no âmbito de um inquérito penal, que autorize esse acesso se for pedido para efeitos da investigação de infrações penais puníveis, pelo direito nacional, com uma pena máxima de prisão não inferior a três anos, desde que existam indícios suficientes de tais infrações e esses dados sejam relevantes para o apuramento dos factos, na condição, todavia, de esse juiz poder indeferir o referido acesso se for requerido no âmbito de um inquérito de uma infração que manifestamente não é grave, tendo em conta as condições sociais prevalecentes no Estado-Membro em causa.

Quanto às despesas

64 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:

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:

não se opõe a uma disposição nacional que impõe ao juiz nacional, que intervém no âmbito de uma fiscalização prévia efetuada na sequência de um pedido fundamentado de acesso a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de permitir tirar conclusões específicas sobre a vida privada de um utilizador de um meio de comunicação eletrónica, conservados pelos prestadores de serviços de comunicações eletrónicas, apresentado por uma autoridade nacional competente no âmbito de um inquérito penal, que autorize esse acesso se for pedido para efeitos da investigação de infrações penais puníveis, pelo direito nacional, com uma pena máxima de prisão não inferior a três anos, desde que existam indícios suficientes de tais infrações e esses dados sejam relevantes para o apuramento dos factos, na condição, todavia, de esse juiz poder indeferir o referido acesso

se for requerido no âmbito de um inquérito de uma infração que manifestamente não é grave, tendo em conta as condições sociais prevalecentes no Estado-Membro em causa.

Assinaturas