Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
ANTHONY MICHAEL COLLINS
apresentadas em 8 de junho de 2023 [1]

Processo C-178/22

Desconhecidos
sendo interveniente:
Procura della Repubblica presso il Tribunale di Bolzano,

[pedido de decisão prejudicial apresentado pelo Tribunale di Bolzano (Tribunal de Primeira Instância de Bolzano, Itália)]

«Pedido de decisão prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Confidencialidade das comunicações — Prestadores de serviços de comunicações eletrónicas — Diretiva 2002/58/CE — Artigos 1.º, n.º 3, e 15.º, n.º 1 — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.º, 8.º, 11.º e artigo 52.º, n.º 1 — Pedido do Ministério Público de acesso a dados para efeitos de investigação e repressão do furto qualificado de um telemóvel — Conceito de "infração grave" suscetível de justificar uma ingerência nos direitos fundamentais — Alcance da fiscalização prévia para assegurar o preenchimento do requisito de prática de uma infração grave — Princípio da proporcionalidade»

I. Introdução

1. A Procura della Repubblica presso il Tribunale di Bolzano [Ministério Público junto do Tribunal de Primeira Instância de Bolzano, Itália; a seguir «Ministério Público» (Bolzano)] pede ao Tribunale di Bolzano (Tribunal de Primeira Instância de Bolzano, Itália) que autorize o acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas ao abrigo do direito nacional que permitem, designadamente, detetar e identificar a origem e o destino das comunicações feitas a partir de telemóveis.

2. No âmbito desse pedido, o Tribunale di Bolzano (Tribunal de Primeira Instância de Bolzano) pede ao Tribunal de Justiça que interprete o artigo 15.º, n.º 1, da Diretiva 2002/58/CE [2]. Esta disposição permite que os Estados-Membros introduzam na lei exceções à obrigação, prevista nesta diretiva [3], de garantir a confidencialidade das comunicações eletrónicas. No Acórdão

[1] Língua original: inglês.

[2] Diretiva do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 201, p. 37), 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).

[3] V. artigo 5.º da Diretiva 2002/58. A proteção da confidencialidade das comunicações eletrónicas garantida pelo artigo 5.º, n.º 1, da Diretiva 2002/58 aplica-se às medidas adotadas por todas as pessoas que não sejam os utilizadores, independentemente de se tratar de entidades privadas ou de entidades estatais (Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 36 e jurisprudência referida).

Prokuratuur[4], o Tribunal de Justiça declarou que o acesso aos dados que permitem tirar conclusões precisas sobre a vida privada de um utilizador, em aplicação de medidas adotadas ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, constitui uma ingerência grave nos direitos e princípios fundamentais consagrados nos artigos 7.º, 8.º, 11.º e no artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»)[5]. Este acesso não pode ser autorizado para efeitos de prevenção, investigação, deteção ou repressão de «infrações penais» em geral. Apenas pode ser concedido no âmbito de processos e procedimentos destinados a lutar contra a «criminalidade grave»[6] e deve ser objeto de fiscalização prévia por um órgão jurisdicional ou por uma entidade administrativa independente, a fim de garantir o respeito deste requisito[7]. O Tribunale di Bolzano (Tribunal de Primeira Instância de Bolzano) pede ao Tribunal de Justiça que clarifique dois aspetos do Acórdão Prokuratuur: o conceito de «infração grave» e o alcance da fiscalização prévia que deve ser efetuada por um órgão jurisdicional por força de uma disposição nacional que exige que este autorize o acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas.

II. Regime jurídico

A. Direito da União

3. O artigo 5.º da Diretiva 2002/58, 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 […]

[…]»

4. 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.

[…]

[4] Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152 (a seguir «Acórdão Prokuratuur»).

[5] Independentemente da duração do período para o qual o acesso aos referidos dados é pedido, bem como da quantidade e da natureza dos dados disponíveis em relação a esse período.

[6] V. Acórdão Prokuratuur, n.ºs 35, 39 e 45. V. igualmente Acórdãos de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 56, 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 140.

[7] Acórdão Prokuratuur, n.ºs 48 a 52.

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.

[…]»

5. O artigo 9.º da Diretiva 2002/58, sob a epígrafe «Dados de localização para além dos dados de tráfego», prevê:

«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. Os utilizadores ou assinantes devem dispor da possibilidade de retirar em qualquer momento o seu consentimento para o tratamento dos dados de localização, para além dos dados de tráfego.

[…]»

6. Nos termos do artigo 15.º, n.º 1, da Diretiva 2002/58:

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

B. Direito nacional

7. O artigo 132.º, n.º 3, do decreto legislativo 30 giugno 2003, n.º 196, Codice in materia di protezione dei dati personali (Decreto Legislativo n.º 196, de 30 de junho de 2003, que aprova o Código de Proteção de Dados)[9], conforme alterado recentemente pelo artigo 1.º do decreto-legge

[8] Diretiva do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31).

[9] Suplemento ordinário n.º 123 ao GURI n.º 174, de 29 de julho de 2003, p. 11.

30 settembre 2021 n.º 132 - Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP, convertito con modificazioni nella legge 23 novembre 2021 n.º 178 (Decreto-Lei n.º 132, de 30 de setembro de 2021[10], convertido, com alterações, na Lei n.º 178, de 23 de novembro de 2021)[11] (a seguir «artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003»), dispõe:

«n.º 3: Dentro do prazo de conservação imposto por lei (isto é: 24 meses a contar da data da comunicação), no caso de haver indícios suficientes de crimes para os 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 Codice di procedura penale (a seguir "Código de Processo Penal"), e de crimes de ameaça, assédio e perturbação das pessoas por meio de telefone, quando a ameaça 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;

[…]

n.º 3-*quater*: Os dados obtidos em violação do disposto nos n.ºs 3 e 3-*bis* não podem ser utilizados.»

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

«Para determinar a competência, deve ser tida em conta a 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 o crime e das penas especialmente agravadas».

9. Segundo o órgão jurisdicional de reenvio, o Ministério Público pode instaurar oficiosamente um processo penal quando esteja em causa o crime de furto qualificado[12]. De acordo com o artigo 625.º do Codice Penale (a seguir «Código Penal»), o crime de furto qualificado é punível com uma pena especialmente agravada de prisão de dois a seis anos e com uma pena de multa de 927 a 1 500 euros. O artigo 624.º do Código Penal prevê que o crime de furto simples, que pode ser objeto de um processo penal na sequência de queixa do lesado, é punível com uma pena de prisão de seis meses a três anos e com uma pena de multa de 154 a 516 euros.

III. Litígios nos processos principais e questão prejudicial

10. O Ministério Público (Bolzano) instaurou dois processos penais contra desconhecidos pelo furto qualificado de telemóveis em conformidade com os artigos 624.º e 625.º do Código Penal[13]. A fim de identificar os autores, apresentou ao órgão jurisdicional de reenvio um pedido, com base no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003, de «([…]) autorização para obter

[10] GURI n.º 234 de 30 de setembro de 2021, p.1.

[11] GURI n.º 284 de 29 de novembro de 2021, p.1.

[12] O direito italiano define como «qualificados» os furtos que são objeto de uma investigação em cujo âmbito intervém o órgão jurisdicional de reenvio.

[13] O primeiro furto ocorreu em 27 de outubro de 2021 (número RGNR 9228/2021), ao passo que o segundo ocorreu em 20 de novembro de 2021 (número RGNR 9794/2021). Os furtos dos telemóveis tiveram lugar em Bolzano e os respetivos proprietários apresentaram queixa aos Carabinieri (força de segurança).

junto de todas as companhias telefónicas todos os dados na sua posse, com o método de tráfego e localização (em especial, utilizações e eventualmente números IMEI chamados/recebidos, sítios visitados/acedidos, horário e duração da chamada/ligação e indicação das células e/ou repetidores em questão, utilizações e IMEI dos emitentes/destinatários dos SMS ou MMS e, sempre que possível, informações gerais sobre os respetivos titulares) das conversas/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».

11. O órgão jurisdicional de reenvio tem dúvidas 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 conforme interpretado no Acórdão Prokuratuur. Assinala que, em 7 de setembro de 2021, a Corte suprema di cassazione (Supremo Tribunal de Cassação, Itália)[14] declarou que, atenta a margem de apreciação dos órgãos jurisdicionais nacionais na determinação das infrações que constituem «ameaças graves à segurança nacional e criminalidade grave», o Acórdão Prokuratuur não vincula diretamente estes órgãos. Na sequência do Acórdão da Corte suprema di cassazione (Supremo Tribunal de Cassação), o legislador italiano adotou o Decreto-Lei n.º 132, de 30 de setembro de 2021, cujo artigo 132.º, n.º 3, qualifica como infrações penais graves, para efeitos de obtenção de registos telefónicos, nomeadamente, as infrações para as quais a lei prevê «uma pena máxima de prisão não inferior a três anos […]».

12. Segundo o órgão jurisdicional de reenvio, a moldura prevista no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 para infrações penais graves abrange infrações que causam pouco alarme social e que apenas podem ser objeto de um processo penal na sequência da queixa de um particular[15]. Assim, o acesso aos registos telefónicos pode ser obtido ao abrigo desta disposição para os casos de furto de bens de valor irrisório, como telemóveis ou bicicletas. Por conseguinte, a moldura prevista no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 viola o princípio da proporcionalidade, à luz do artigo 52.º, n.º 1, da Carta, que exige que se proceda, em todos os casos, a uma ponderação entre a gravidade do crime objeto de investigação e a restrição do gozo de um direito fundamental. A instauração de processos penais por tais crimes de menor gravidade não justifica a restrição do gozo dos direitos fundamentais ao respeito pela vida privada, à proteção de dados pessoais e à liberdade de expressão e de informação[16].

13. O órgão jurisdicional de reenvio esclarece que os órgãos jurisdicionais italianos têm uma margem de apreciação muito limitada para recusar o acesso aos registos telefónicos, uma vez que a autorização deve ser concedida quando existam «indícios suficientes [da prática de] [crimes]» e se a referida autorização for «relevante para o apuramento dos factos». Em particular, os órgãos jurisdicionais não têm competência para avaliar a gravidade do crime objeto de investigação. O legislador procedeu a esta avaliação quando previu, em termos gerais e sem distinguir entre diferentes tipos de infrações, que o acesso aos registos telefónicos deve ser concedido, nomeadamente, para efeitos de investigação de todos os crimes puníveis com uma pena máxima de prisão não inferior a três anos.

[14] Cass. Pen. Sez. II, n.º 33116, ud. 7.9.2021, est. Pellegrino.

[15] De acordo com o órgão jurisdicional de reenvio «é o caso, por exemplo, do crime de violação do domicílio, punido pelo artigo 614.º do Código Penal com uma pena de prisão de um a quatro anos. Outras infrações, cujas molduras legais das penas não impedem a obtenção dos registos telefónicos, punidas mediante queixa por gerarem pouco alarme social, são as infrações referidas no artigo 633.º do Código Penal (invasão de terrenos e edifícios: pena de prisão de um a três anos e multa de 103,00 euros a 1 032,00 euros) ou no artigo 640.º deste código (fraude simples: pena de prisão de seis meses a três anos e multa de 51,00 euros a 1 032,00 euros)».

[16] V. artigos 7.º, 8.º e 11.º da Carta.

14. Nestas circunstâncias, o Tribunale di Bolzano (Tribunal de Primeira Instância 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 do [artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003], que na sua versão atual dispõe o seguinte:

Dentro do prazo de conservação imposto por lei, no caso de haver indícios suficientes de [crimes] para [os] 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 [crimes] de ameaça, assédio e perturbação das pessoas por meio de telefone, quando a ameaça 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?»

IV. Tramitação processual no Tribunal de Justiça

15. Foram apresentadas observações escritas pelos Governos checo, estónio, francês, italiano, cipriota, húngaro, neerlandês, austríaco e polaco, bem como pela Irlanda e pela Comissão Europeia.

16. Na audiência de 21 de março de 2023, as partes supramencionadas e o Ministério Público (Bolzano) apresentaram alegações orais e responderam às questões colocadas pelo Tribunal de Justiça.

V. Análise

A. Quanto à admissibilidade

17. O Governo italiano e a Irlanda sustentam que o pedido de decisão prejudicial é parcialmente inadmissível. De acordo com os factos expostos no despacho de reenvio, o pedido de acesso foi apresentado no âmbito da investigação de furtos qualificados de telemóveis. A Irlanda sublinha que o Ministério Público pode instaurar oficiosamente um processo penal quando esteja em causa este tipo penal. Esta competência é um reflexo da ideia de que a natureza e os efeitos da infração afetam a sociedade em geral. Deste modo, o pedido de decisão prejudicial apresenta um caráter hipotético uma vez que incide igualmente sobre infrações penais que apenas podem ser objeto de um processo penal na sequência da queixa de um particular. O Governo italiano sublinha que o órgão jurisdicional de reenvio faz referência a uma série de infrações que são irrelevantes para os processos que lhe foram submetidos. O Governo italiano e a Comissão alegam que, ao contrário do que é referido no pedido a respeito da «pena máxima de prisão não inferior a três anos», o artigo 625.º do Código Penal prevê uma pena de prisão de dois a seis anos para o crime de furto qualificado. Por conseguinte, a Comissão propõe ao Tribunal de Justiça que reformule a questão. O Governo francês pede igualmente ao Tribunal de Justiça que reformule a questão. Considera que, embora o Tribunal de Justiça possa interpretar disposições de direito da União, não tem competência para apreciar a compatibilidade das disposições do direito nacional com o direito da União.

18. Através da sua questão, o órgão jurisdicional de reenvio pede literalmente ao Tribunal de Justiça que se pronuncie sobre a compatibilidade de uma disposição de direito nacional com o direito da União. Isto não impede que seja facultada uma interpretação do direito da União ao órgão jurisdicional de reenvio, neste caso do artigo 15.º, n.º 1, da Diretiva 2002/58, que lhe permita decidir sobre a compatibilidade, com esta disposição, das normas nacionais em causa no litígio que lhe foi submetido [17].

19. Resulta claro do pedido de decisão prejudicial que o Ministério Público (Bolzano) requereu o acesso a dados, nomeadamente, para investigar e instaurar processos penais a título de dois furtos qualificados de telemóveis em aplicação do artigo 625.º do Código Penal. Neste contexto, as referências a outros tipos penais que figuram neste pedido, nomeadamente o crime previsto no artigo 624.º do Código Penal (furto simples) [18], não são relevantes para decidir sobre os pedidos pendentes no órgão jurisdicional de reenvio [19]. Tendo em conta que a questão prejudicial tem por objeto o pedido do Ministério Público (Bolzano) de acesso a dados para efeitos de investigação de crimes de furto qualificado, a mesma não é hipotética. Consequentemente, a minha análise sobre a aplicação do artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 limitar-se-á aos factos descritos pelo órgão jurisdicional de reenvio que se reportam a furtos qualificados de telemóveis.

B. Quanto ao mérito

1. Considerações preliminares

20. O presente reenvio resulta de um pedido do Ministério Público (Bolzano) de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas. Não tem por objeto a conservação dos dados ou a licitude da mesma, nomeadamente, ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58 [20]. Os dados dizem respeito, particularmente, a registos de chamadas recebidas e efetuadas [21] a partir dos telemóveis furtados e a dados de localização [22]. Embora estes dados não contemplem o conteúdo das comunicações, permitem tirar conclusões precisas sobre a vida privada dos titulares dos dados em causa, cujo acesso parece constituir uma ingerência «grave» nos seus direitos fundamentais [23]. A ingerência que resulta do acesso a estes dados pode ser

[17] V., por analogia, Acórdão de 17 de março de 2021, Consulmarketing, C-652/19, EU:C:2021:208, n.º 33. É jurisprudência constante que, ao abrigo do artigo 267.º TFUE, cabe ao Tribunal de Justiça dar ao órgão jurisdicional de reenvio uma resposta útil que lhe permita decidir o litígio que lhe foi submetido e que, nesta ótica, incumbe ao Tribunal de Justiça, se necessário, reformular as questões que lhe são submetidas (v., neste sentido, Acórdão de 25 de julho de 2018, Dyson, C-632/16, EU:C:2018:599, n.º 47 e jurisprudência referida).

[18] O crime de furto simples é punível com uma pena de prisão de seis meses a três anos, o que significa que está abrangido pelo âmbito de aplicação do artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003.

[19] Uma vez que tais referências indicam que o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 pode ser aplicado no contexto da investigação de infrações que não constituem criminalidade grave, v. n.ºs 35 a 39 das presentes conclusões.

[20] Por conseguinte, o pedido de decisão prejudicial baseia-se na premissa de que a conservação dos dados requeridos é lícita. A conservação e o acesso a dados abrangidos pela Diretiva 2002/58 constituem ingerências distintas nos direitos fundamentais garantidos nos artigos 7.º, 8.º e 11.º da Carta e necessitam de uma justificação distinta nos termos do artigo 52.º, n.º 1, da mesma (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 47). O Acórdão Prokuratuur contém, nos seus n.ºs 29 a 33, um panorama das normas que regulam a conservação deste tipo de dados.

[21] O artigo 2.º, alínea d), da Diretiva 2002/58 define «comunicação» como «qualquer informação trocada ou enviada entre um número finito de partes, através de um serviço de comunicações eletrónicas publicamente disponível […]».

[22] O artigo 2.º, alínea c), da Diretiva 2002/58 define «dados de localização» como «quaisquer dados […] que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público».

[23] V., neste sentido, Acórdão Prokuratuur, n.ºs 34 e 35. V., por analogia, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.ºs 59 a 62. Cabe ao órgão jurisdicional nacional avaliar se o acesso aos dados constitui uma ingerência «grave» nos direitos fundamentais das pessoas cujos dados estão em causa. As presentes conclusões assentam na premissa de que a ingerência que o acesso aos dados descritos no n.º10 das presentes conclusões implica é grave.

justificada pelo objetivo [24], mencionado no artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58, de investigação, deteção e repressão de «infrações penais graves», mas não de infrações penais em geral. Ao interpretar o artigo 15.º, n.º 1, da Diretiva 2002/58, o Tribunal de Justiça associa a gravidade da ingerência nos direitos fundamentais de uma pessoa à gravidade da infração penal objeto de investigação [25].

2. Quanto à competência dos Estados-Membros para definir as «infrações penais graves»

21. A Diretiva 2002/58 regula as atividades dos prestadores de serviços de comunicações eletrónicas em matéria de tratamento de dados pessoais [26]. O artigo 1.º, n.º 3, exclui expressamente do seu âmbito de aplicação as atividades do Estado em determinados domínios como a segurança pública, a defesa, a segurança do Estado e o direito penal. As atividades previstas no artigo 15.º, n.º 1, da Diretiva 2002/58 coincidem substancialmente com as atividades descritas no artigo 1.º, n.º 3, da mesma, e abrangem as atividades em matéria de direito penal que estão expressamente excluídas do âmbito de aplicação da Diretiva 2002/58 [27]. Por conseguinte, há uma ligação clara entre as atividades do Estado que estão excluídas do âmbito de aplicação da Diretiva 2002/58 por força do seu artigo 1.º, n.º 3 e as medidas legislativas que os Estados-Membros podem adotar em aplicação do artigo 15.º, n.º 1, da mesma [28].

22. Não obstante essa ligação clara, o Tribunal de Justiça tem reiteradamente declarado que, uma vez que o artigo 15.º, n.º 1, da Diretiva 2002/58 autoriza expressamente os Estados-Membros a adotarem as medidas legislativas nacionais aí descritas, tais medidas estão abrangidas pelo âmbito de aplicação desta diretiva. Resulta desta jurisprudência que o conceito de «atividades», incluindo as «atividades do Estado em matéria de direito penal», que figura no artigo 1.º, n.º 3, da Diretiva 2002/58, não abrange as medidas legislativas previstas no artigo 15.º, n.º 1, da mesma [29].

[24] O elenco de objetivos do artigo 15.º, n.º 1, da Diretiva 2002/58 é taxativo (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 90).

[25] V., neste sentido, Conclusões do advogado-geral H. Saugmandsgaard Øe no processo Ministerio Fiscal, C-207/16, EU:C:2018:300, n.ºs 79 a 82 e jurisprudência referida. Em relação ao objetivo de luta contra a criminalidade, este acesso só poderá, em princípio, ser concedido aos dados de pessoas que se suspeita estarem a planear, a cometer ou terem cometido uma infração grave ou, ainda, estarem envolvidas de uma maneira ou de outra nessa infração (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 105).

[26] V., neste sentido, artigo 3.º da Diretiva 2002/58, que dispõe que a diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas. V.,igualmente, Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. C-203/15 e C-698/15, EU:C:2016:970, n.ºs 70 e 74) e, por analogia, Conclusões do advogado-geral M. Szpunar no processo La Quadrature du Net e o. (Dados pessoais e combate à contrafação), C-470/21, EU:C:2022:838, n.º 38.

[27] 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 97.

[28] Para efeitos de salvaguarda da segurança nacional, a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de inflações penais ou a utilização não autorizada do sistema de comunicações eletrónicas.

[29] Acórdãos 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 98, e de 6 de outubro de 2020, Privacy International, C-623/17, EU:C:2020:790, n.º 38 e jurisprudência referida.

23. Nem o artigo 2.º da Diretiva 2002/58, que contém várias definições para efeitos de aplicação da diretiva, nem nenhuma outra disposição da mesma, incluindo o seu artigo 15.º, n.º 1, definem o conceito de «infrações penais». A Diretiva 2002/58 não contém uma enumeração das «infrações penais» [30]. Além disso, a jurisprudência relativa à interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58 não define este conceito [31].

24. Apesar de não existirem tais definições, a Diretiva 2002/58 não prevê que cada Estado-Membro defina as «infrações penais» em conformidade com o respetivo direito nacional [32]. Segundo jurisprudência constante do Tribunal de Justiça, decorre das exigências tanto da aplicação uniforme do direito da União como do princípio da igualdade que uma disposição do direito da União que não contenha uma remissão expressa para o direito dos Estados-Membros para efeitos da determinação do seu sentido e alcance, deve normalmente ter, em toda a União, uma interpretação autónoma e uniforme. No âmbito da interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, o conceito de «infrações penais» pode, pelo menos em princípio, ser considerado um conceito autónomo do direito da União que deve ser uniformemente interpretado no território de todos os Estados-Membros [33].

25. Os dez Estados-Membros que apresentaram observações ao Tribunal de Justiça e a Comissão consideram unanimemente que compete a cada Estado-Membro definir as «infrações penais», incluindo as infrações graves, para as quais remete o artigo 15.º, n.º 1, da Diretiva 2002/58, por referência ao seu direito nacional.

26. Partilho desta opinião pelas seguintes razões.

27. Em primeiro lugar, o Tribunal de Justiça já esclareceu que, no âmbito do artigo 15.º, n.º 1, da Diretiva 2002/58, incumbe aos Estados-Membros definir os seus interesses essenciais de segurança e adotar as medidas adequadas para garantir a sua segurança interna e externa [34]. Embora não o tenha expressamente declarado, o Tribunal de Justiça parece ter considerado, deste modo, que o conceito de «segurança nacional» que figura no artigo 15.º, n.º 1, da Diretiva 2002/58 não é um conceito autónomo de direito da União, apesar da ausência de definição deste conceito

30 V., em contrapartida, artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO 2002, L 190, p. 1), conforme alterada pela Decisão-Quadro 2009/299/JAI, de 26 de fevereiro de 2009 (JO 2009, L 81, p. 24), que enumera as infrações penais que determinam a entrega com base num mandado de detenção europeu, e o anexo II da Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave (JO 2016, L 119, p. 132), que contém uma enumeração dos tipos de «criminalidade grave» conforme definida no artigo 3.º, n.º 9, desta diretiva.

31 A Diretiva 2002/58 não faz referências a «infrações penais em geral», a «infrações penais graves» nem a «infração» ou «infrações». O Tribunal de Justiça remete para estes conceitos na sua jurisprudência sem os definir e sem fornecer elementos que permitam aos legisladores nacionais fazê-lo. V., por exemplo, Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.ºs 115 e 125, e de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.ºs 54, 56 e 63. V. também, sobre este aspeto, Acórdão Prokuratuur, n.º 45.

32 V., em contrapartida, artigo 1.º, n.º 1, da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO 2006, L 105, p. 54) que previa que «a presente diretiva visa harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro» (o sublinhado é meu). No Acórdão de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, o Tribunal de Justiça declarou a Diretiva 2006/24/CE inválida.

33 V., por analogia, Acórdão de 7 de setembro de 2022, Staatssecretaris van Justitie en Veiligheid (Natureza do direito de residência baseado no artigo 20.º TFUE), C-624/20, EU:C:2022:639, n.ºs 19 e 20.

34 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 99 e 136.

ou de remissão expressa para o direito dos Estados-Membros [35]. Não vejo nenhuma razão para que esta abordagem não se aplique à competência dos Estados-Membros para definir «infrações penais» ou «criminalidade grave» para efeitos do artigo 15.º, n.º 1, da Diretiva 2002/58. Os conceitos de «infrações penais», «segurança pública» e «segurança nacional» que figuram nesta disposição podem ser considerados como *noscitur a sociis* uma vez que se afigura que o legislador da União pretendeu que cada um destes conceitos fosse tratado de modo semelhante, incluindo no que respeita à forma como são definidos [36].

28. Em segundo lugar, o artigo 4.º, n.º 2, TUE impõe à União Europeia que respeite a identidade nacional dos Estados-Membros refletida nas estruturas políticas e constitucionais fundamentais de cada um deles. O preâmbulo da Carta reconhece igualmente que a União contribui para a preservação e o desenvolvimento de valores comuns, no respeito, nomeadamente, pela diversidade das culturas e tradições dos povos da Europa. A definição de infrações penais e sanções [37] reflete as sensibilidades e tradições nacionais que variam consideravelmente não só em função dos Estados-Membros mas também ao longo do tempo, em paralelo com as mudanças sociais [38].

29. Neste contexto, é possível observar que, ao definirem as infrações penais e as sanções, os Estados-Membros têm em conta, em diferente medida, vários fatores. A avaliação por um Estado-Membro da «gravidade» de uma determinada infração reflete-se frequentemente, se não invariavelmente, na gravidade da sanção aplicada. A duração de uma pena privativa de liberdade pode refletir a análise de um certo número de fatores, entre os quais a «gravidade» intrínseca de uma infração e a sua «gravidade» relativa face a outras infrações. Não foram apresentados argumentos para explicar por que razão os Estados-Membros não deveriam exercer essa competência nem, aliás, por que razão se deveria adotar uma abordagem diferente relativamente à definição de «infrações penais», de «infrações penais graves» ou de «infrações penais em geral» no contexto específico em análise.

30. A competência dos Estados-Membros no domínio do direito penal não prejudica a competência da União, em certos casos, para estabelecer, por exemplo, regras mínimas relativas à definição das infrações penais e das sanções em domínios de criminalidade particularmente grave com dimensão transfronteiriça que resulte da natureza ou das incidências dessas infrações

[35] Além disso, o artigo 4.º, n.º 2, TUE, estabelece que a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro. O simples facto de uma medida nacional ter sido adotada para efeitos da proteção da segurança nacional não pode implicar a inaplicabilidade do direito da União e dispensar os Estados-Membros do respeito necessário desse direito (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 99 e 135).

[36] Embora o objetivo de salvaguarda da segurança nacional seja mais importante do que o objetivo de luta contra a criminalidade grave e seja, por conseguinte, suscetível de justificar ingerências mais graves nos direitos fundamentais, este objetivo não prejudica o direito dos Estados-Membros de definirem «infrações penais» ou «criminalidade 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.º 136).

[37] Bem como das circunstâncias atenuantes e agravantes.

[38] O Advogado-Geral H. Saugmandsgaard Øe considerou que a legislação penal e as normas do processo penal são da competência dos Estados-Membros, mesmo que a ordem jurídica destes últimos possa ser, no entanto, afetada pelas disposições do direito da União adotadas neste domínio com base, nomeadamente, no artigo 83.º, n.º 2, TFUE. Por conseguinte, não existe nenhuma disposição de alcance geral que dê uma definição harmonizada do conceito de «infração grave» (Conclusões no processo Ministerio Fiscal, C-207/16, EU:C:2018:300, n.º 95). O Advogado-Geral G. Pitruzzella referiu que a definição de «infração grave» deve ser deixada à apreciação dos Estados-Membros. A definição das circunstâncias agravantes pode igualmente variar consoante os Estados-Membros [Conclusões no processo Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2020:18, n.ºs 91 e 92]. Em contrapartida, o Advogado-Geral M. Szpunar considerou que «[o] conceito de "criminalidade grave" deve […] ser objeto de uma interpretação autónoma. Não pode depender das conceções de cada Estado-Membro sob pena de permitir contornar os requisitos do artigo 15.º, n.º 1, da Diretiva 2002/58 consoante os Estados-Membros adotem ou não uma conceção extensiva da luta contra a criminalidade grave [Conclusões no processo La Quadrature du Net e o. (Dados pessoais e combate à contrafação), C-470/21, EU:C:2022:838, n.º 74].

ou ainda da especial necessidade de as combater, assente em bases comuns [39]. Contudo, o legislador da União não estabeleceu regras relativas à definição das infrações penais no artigo 15.º, n.º 1, da Diretiva 2002/58 [40]. Com efeito, conforme indicado anteriormente [41], resulta claro do artigo 1.º, n.º 3, da Diretiva 2002/58 que, ao adotar esta diretiva, o legislador da União não pretendeu exercer nenhuma competência no domínio do direito penal.

31. Estas duas razões são suficientes para explicar por que motivo, não obstante as medidas legislativas nacionais adotadas ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58 para a investigação e repressão de infrações penais estarem abrangidas pelo âmbito de aplicação desta medida, os Estados-Membros mantêm a sua competência para definir as «infrações penais», incluindo as «infrações penais graves», e para estabelecer as respetivas sanções [42].

3. Quanto ao nível de fiscalização aplicável ao exercício da faculdade prevista no artigo 15.º, n.º 1, da Diretiva 2002/58 de derrogar o princípio da confidencialidade

32. O Tribunal de Justiça realçou que a faculdade de derrogar [43], nomeadamente, o princípio da confidencialidade previsto no artigo 5.º, n.º 1, da Diretiva 2002/58, deve ser interpretada em sentido estrito, para evitar que se converta na regra geral, esvaziando assim o referido princípio do seu alcance [44]. O exercício desta faculdade deve, assim, respeitar, particularmente, os princípios da equivalência [45] e da efetividade [46]. Deve igualmente respeitar os princípios gerais do direito da União, incluindo o princípio da proporcionalidade [47], os artigos 7.º, 8.º e 11.º [48] e o artigo 52.º, n.º 1, da Carta [49]. O objetivo de luta contra a criminalidade grave deve ser sempre conciliado com o gozo dos direitos fundamentais em causa. Os direitos consagrados nos artigos 7.º, 8.º e 11.º da Carta não são prerrogativas absolutas e o seu exercício deve ser tomado

[39] Artigo 83.º, n.º 1, primeiro parágrafo, TFUE. V.,igualmente, Acórdão de 21 de outubro de 2021, Okrazhna prokuratura — Varna, C-845/19 e C-863/19, EU:C:2021:864, n.º 32.

[40] V., por analogia, Acórdão Prokuratuur, n.ºs 41 e 42. O Tribunal de Justiça declarou que na falta de regras da União na matéria e por força do princípio da autonomia processual, «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». A Diretiva 2002/58 tem como base jurídica o artigo 114.º TFUE (anterior artigo 95.º TCE) e não, por exemplo, o artigo 83.º, n.º 1, primeiro parágrafo, TFUE. Pelo contrário, a Diretiva 2016/681 tem como bases jurídicas o artigo 82.º, n.º 1, segundo parágrafo, alínea d), TFUE (cooperação judiciária em matéria penal) e o artigo 87.º, n.º 2, alínea a), TFUE (cooperação policial).

[41] V. n.º 21 das presentes conclusões.

[42] V., por analogia, Acórdão de 23 de outubro de 2007, Comissão/Conselho, C-440/05, EU:C:2007:625, n.ºs 66, 70 e 71 e jurisprudência referida. V.,igualmente, Acórdão de 28 de abril de 2011, El Dridri, C-61/11 PPU, EU:C:2011:268, n.º 53.

[43] O artigo 15.º, n.º 1, da Diretiva 2002/58 enuncia que os Estados-Membros «podem adotar» medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nesta diretiva.

[44] Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 89. O Advogado-Geral H. Saugmandsgaard Øe referiu que «mesmo que cada Estado-Membro tenha a faculdade de apreciar qual é o limiar de pena adequado para caracterizar uma infração grave, tem, no entanto, o dever de não o escalonar a um nível de tal modo baixo, tendo em conta o nível habitual das penas aplicáveis nesse Estado, de tal modo que as exceções à proibição de armazenar e de utilizar os dados pessoais que estão previstos nesse artigo 15.º, n.º 1, seriam convertidos em princípios […]» (Conclusões no processo Ministerio Fiscal, C-207/16, EU:C:2018:300, n.º 114).

[45] Nada indica que o direito italiano não respeite este princípio.

[46] Acórdão de 5 de abril de 2022, Commissioner of An Garda Síochána e o., C-140/20, EU:C:2022:258, n.º 127.

[47] V., igualmente, considerando 11 da Diretiva 2002/58.

[48] V., igualmente, considerando 2 da Diretiva 2002/58.

[49] Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 89, 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.ºs 111 a 113. V., igualmente, Conclusões do Advogado-Geral H. Saugmandsgaard no processo Ministerio Fiscal, C-207/16, EU:C:2018:300, n.ºs 116 a 120. No Acórdão de 8 de março de 2022, Bezirkshauptmannschaft Hartberg-Fürstenfeld (Efeito direto), C-205/20, EU:C:2022:168, n.º 31, o Tribunal de Justiça recordou que o princípio da proporcionalidade vincula os Estados-Membros quando aplicam o direito da União. Nesse contexto, os Estados-Membros devem respeitar o artigo 49.º, n.º 3, da Carta quando adotam sanções, mesmo na ausência de legislação da União que harmonize essas sanções.

em consideração relativamente à sua função na sociedade [50]. O artigo 52.º, n.º 1, da Carta prevê, assim, que as restrições ao exercício destes direitos, conforme previstas por lei, devem respeitar o seu conteúdo essencial e que, na observância do princípio da proporcionalidade, devem ser necessárias e corresponder efetivamente a objetivos de interesse geral reconhecidos pela União Europeia ou à necessidade de proteção dos direitos e liberdades de terceiros. As medidas legislativas nacionais adotadas em aplicação do artigo 15.º, n.º 1, da Diretiva 2002/58 devem, assim, responder efetiva e estritamente a um dos objetivos enunciados nesta disposição. Devem basear-se em critérios objetivos, ser juridicamente vinculativas e estabelecer regras claras e precisas que indiquem as condições materiais e processuais em que os prestadores de serviços de comunicações eletrónicas devem permitir o acesso aos dados por parte das autoridades nacionais competentes [51].

33. Para assegurar o pleno respeito dessas condições na prática, o acesso das autoridades nacionais competentes aos dados conservados deve, em princípio [52], ser sujeito à fiscalização prévia de um órgão jurisdicional ou de uma entidade administrativa independente [53], na sequência de um pedido fundamentado dessas autoridades e da notificação das pessoas visadas [54]. É jurisprudência constante que, no âmbito dessa fiscalização prévia, um órgão jurisdicional ou uma entidade administrativa independente deve conciliar os diferentes interesses e direitos em causa, a fim de assegurar um justo equilíbrio entre as exigências do inquérito e a necessidade de garantir os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas visadas [55].

34. No caso em apreço, o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 fixa as condições com base nas quais um órgão jurisdicional nacional deve ordenar aos prestadores de serviços de comunicações eletrónicas que concedam ao Ministério Público o acesso aos dados a pedido deste último. É consensual [56] que o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 enuncia de forma clara e precisa as circunstâncias e as condições em que um órgão jurisdicional nacional pode ordenar aos prestadores de serviços de comunicações eletrónicas que concedam tal acesso. No entanto, o órgão jurisdicional de reenvio considera que a pena «de prisão máxima não inferior a três anos» é excessivamente ampla, uma vez que inclui no seu âmbito de aplicação infrações como o furto simples que causa pouco alarme social.

35. Embora o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 abranja, pelo menos potencialmente, um leque alargado de infrações penais, o Tribunal de Justiça não dispõe, no âmbito do presente processo, de elementos de prova que revelem um número de infrações tão significativo ao ponto de tornar o acesso aos dados a regra e não a exceção [57]. A moldura de uma

[50] Artigo 52.º, n.º 1, da Carta. 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 120.

[51] Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.os 117 a 119. V., igualmente, 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 110 e 129 a 133.

[52] Por exemplo, o artigo 132.º, n.º 3-*bis*, do Decreto Legislativo n.º 196/2003 prevê regras especiais de acesso a dados em situações urgentes. Nas suas Conclusões no processo La Quadrature du Net e o. (Dados pessoais e combate à contrafação), C-470/21, EU:C:2022:838, n.os 99 a 105, o Advogado-Geral M. Szpunar referiu que é necessário uma fiscalização prévia apenas nos casos que envolvam ingerências graves na vida dos utilizadores de serviços de comunicações eletrónicas. No presente processo, afigura-se necessário uma fiscalização prévia dado que a ingerência em causa é grave em razão da natureza dos dados a que o Ministério Público pretende aceder.

[53] A jurisprudência do Tribunal de Justiça, contrariamente à Diretiva 2002/58, estabelece o requisito da fiscalização prévia: Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.os 120 e 121 e jurisprudência referida.

[54] Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.os 120 e 121.

[55] Acórdão Prokuratuur, n.º 52.

[56] Sob reserva de verificação pelo órgão jurisdicional de reenvio.

[57] V. Conclusões do advogado-geral H. Saugmandsgaard Øe no processo Ministerio Fiscal, C-207/16, EU:C:2018:300, n.os 116 a 120. Trata-se, em última análise, de uma questão a apreciar pelo órgão jurisdicional de reenvio.

pena máxima de prisão não inferior a três anos prevista nesta disposição não parece excessivamente reduzida [58]. Por analogia, o artigo 3.º, n.º 9, da Diretiva 2016/681 [59] define «criminalidade grave» como «as infrações enumeradas no anexo II puníveis com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos nos termos do direito nacional de um Estado-Membro» [60]. Contudo, o Tribunal de Justiça declarou que, uma vez que o artigo 3.º, ponto 9, da Diretiva 2016/681 não se refere à pena mínima aplicável, mas à pena máxima aplicável, não se pode excluir que os dados em causa possam ser objeto de um tratamento para efeitos de luta contra infrações que, embora preencham o critério previsto por esta disposição relativo ao limiar de gravidade, atendendo às especificidades do sistema penal nacional, não se enquadram na criminalidade grave mas na criminalidade comum [61].

36. A pena de três anos prevista no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 refere-se à pena máxima aplicável e pode, assim, aplicar-se a crimes como o furto simples [62]. Por conseguinte, há que examinar de que modo é que o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 é aplicado na prática. Sob reserva de verificação pelo órgão jurisdicional de reenvio, o artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 parece estabelecer dois critérios diferentes a propósito da fiscalização prévia por um órgão jurisdicional nacional em função da natureza das infrações objeto de investigação.

37. O primeiro destes critérios de fiscalização impõe [63] aos órgãos jurisdicionais nacionais que autorizem o acesso do Ministério Público aos dados conservados pelos prestadores de serviços de comunicações eletrónicas se tal for relevante para o apuramento dos factos e se houver indícios suficientes da prática de um crime que consiste em ameaçar e assediar ou perturbar pessoas por telefone, se a ameaça ou a perturbação for grave. Por conseguinte, o órgão jurisdicional nacional deve proceder a uma apreciação individual da gravidade da infração em causa e verificar se a investigação e a instauração de um processo penal a título dessa infração justificam a restrição dos direitos gerais consagrados nos artigos 7.º, 8.º e 11.º da Carta e dos direitos específicos previstos nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58. O critério permite apreciar individual e concretamente, num determinado caso, a proporcionalidade da ingerência nestes direitos em função do objetivo de interesse público de luta contra a criminalidade.

38. Em contrapartida, o segundo destes critérios de fiscalização, que é relevante no presente processo, exige [64] aos órgãos jurisdicionais nacionais que autorizem o Ministério Público a aceder aos dados conservados pelos prestadores de serviços de comunicações eletrónicas se isso for

[58] V., por analogia, Acórdão de 8 de julho de 2010, Sjöberg e Gerdin, C-447/08 e C-448/08, EU:C:2010:415, n.º 38.

[59] A Diretiva 2016/681 regula a transferência e o tratamento de dados dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

[60] O Tribunal de Justiça declarou que os requisitos resultantes desta disposição, que dizem respeito à natureza e à severidade da pena aplicável, podem, em princípio, limitar a aplicação do sistema estabelecido pela referida diretiva a infrações que apresentem um nível suficiente de gravidade suscetível de justificar a ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta (Acórdão de 21 de junho de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, n.º 150).

[61] O Tribunal de Justiça declarou, por conseguinte, que os Estados-Membros devem assegurar que o sistema estabelecido pela Diretiva 2016/681 se limita à luta contra a criminalidade grave, e não contra a criminalidade comum (Acórdão de 21 de junho de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, n.ºs 151 e 152). O objeto e o âmbito da aplicação da Diretiva 2016/681 que preveem, nomeadamente, a troca de dados dos registos de identificação dos passageiros (PNR) entre Estados-Membros, não se sobrepõem aos da Diretiva 2002/58. Daqui resulta que as disposições destas diretivas devem ser apreciadas separadamente e em função das suas características. A este propósito, e ao contrário do artigo 15.º, n.º 1, da Diretiva 2002/58, o conceito de «criminalidade grave» que figura na Diretiva 2016/681 é um conceito autónomo de direito da União. V., igualmente, a este respeito, considerando 12, artigo 3.º, n.º 9, e anexo II da Diretiva 2016/681.

[62] V., por analogia, Acórdão de 21 de junho de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, n.º 151.

[63] O texto na língua original utiliza a expressão «i dati sono acquisti».

[64] Sob reserva de verificação pelo órgão jurisdicional de reenvio, a utilização do indicativo no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 («i dati sono acquisti») implica que os órgãos jurisdicionais nacionais concedem o acesso aos dados em questão se os requisitos exigidos por esta disposição estiverem preenchidos.

relevante para o apuramento dos factos e se existirem indícios suficientes da prática de um crime punível, designadamente, com uma pena de prisão máxima não inferior a três anos. Neste caso, o órgão jurisdicional nacional limita-se a verificar se estes requisitos objetivos estão preenchidos, sem poder proceder a uma apreciação individualizada ou concreta dos interesses em causa [65]. A fiscalização efetuada pelo órgão jurisdicional nacional ao abrigo do artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 é, assim, alheia à existência de um nexo concreto com as circunstâncias específicas do processo que lhe é submetido.

39. Embora os órgãos jurisdicionais nacionais não tenham competência para fiscalizar a definição das infrações pelo legislador nem a decisão deste sobre a gravidade das mesmas [66], devem, todavia, ter competência para proceder a uma apreciação individualizada ou concreta no sentido de averiguar se a concessão de acesso, ao abrigo de medidas legislativas adotadas por referência ao artigo 15.º, n.º 1, da Diretiva 2002/58, a dados sensíveis que permitam tirar conclusões precisas sobre a vida privada de um utilizador, constituindo assim uma ingerência grave nos direitos fundamentais consagrados nos artigos 7.º, 8.º, 11.º e no artigo 52.º, n.º 1, da Carta, é proporcionada.

40. Daqui resulta que as medidas adotadas ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58 só podem permitir o acesso a dados sensíveis se (i) a infração em causa atingir o limiar de gravidade previamente determinado pelo legislador nacional (ii) e se um órgão jurisdicional ou uma entidade administrativa independente considerar, na sequência de uma apreciação ou de um exame individual, que a ingerência nos direitos fundamentais que tal acesso implica é proporcionada em relação ao objetivo de interesse geral de luta contra a criminalidade num caso específico. No entanto, em certos casos, o acesso a esses dados pode não ser concedido mesmo que a infração atinja o limiar de gravidade previsto no direito nacional.

41. O crime de furto qualificado em causa é considerado «grave» no direito nacional, uma vez que é punível, nomeadamente, com uma pena de prisão de dois a seis anos, pelo que atinge o limiar de gravidade previsto no artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003 [67]. Quando aplicam medidas adotadas por referência ao artigo 15.º, n.º 1, da Diretiva 2002/58, os órgãos jurisdicionais italianos não parecem ter competência para pôr em causa a qualificação do furto qualificado como «infração grave» no âmbito do direito nacional. Se o limiar fixado pelo direito nacional não for atingido, o órgão jurisdicional de reenvio não pode, assim, conceder o requerido acesso aos dados [68].

42. Quando o limiar fixado pelo legislador nacional é atingido, o órgão jurisdicional de reenvio deve, em aplicação do artigo 15.º, n.º 1, da Diretiva 2002/58, verificar se, à luz de todas as circunstâncias específicas do caso em apreço, a ingerência nos direitos fundamentais que implica a concessão de acesso a dados sensíveis é proporcionada em relação ao objetivo de interesse geral da luta contra essa infração. A este respeito, o órgão jurisdicional de reenvio deve ter em conta e

[65] Na audiência, as posições do Ministério Público (Bolzano) e do Governo italiano divergiram, no que respeita ao papel dos órgãos jurisdicionais nacionais e ao alcance da fiscalização prévia ao abrigo do artigo 132.º, n.º 3, do Decreto Legislativo n.º 196/2003. Ao passo que o Ministério Público (Bolzano) alegou que, antes de concederem o acesso a esses dados, os órgãos jurisdicionais nacionais devem proceder a uma apreciação individual da proporcionalidade da concessão do acesso, o Governo italiano sublinhou, por seu turno, que, em conformidade com o artigo 101.º da Costituzione della Repubblica Italiana (Constituição da República Italiana) e o artigo 1.º do Código Penal, os órgãos jurisdicionais nacionais estão vinculados pelo princípio da legalidade, o que significa que não podem adotar o que descreveu como uma interpretação criativa da lei. Cabe ao órgão jurisdicional de reenvio interpretar as disposições do direito nacional aplicáveis.

[66] A menos que o direito nacional o permita e no respeito, nomeadamente, do artigo 49.º da Carta.

[67] Uma pena máxima de prisão não inferior a três anos.

[68] O artigo 52.º, n.º 1, da Carta dispõe que qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela Carta deve ser prevista por lei. Isto significa que os órgãos jurisdicionais nacionais estão, em princípio, vinculados pela legislação nacional que preveja estas restrições.

ponderar todos os direitos e interesses relevantes, incluindo, nomeadamente, os danos provocados ao direito de propriedade das vítimas protegido pelo artigo 17.º da Carta, bem como o facto de os telemóveis poderem conter informações muito sensíveis relativas à vida privada, profissional e financeira dos seus proprietários [69]. O acesso aos dados em causa pode ser o único meio eficaz disponível para investigar e reprimir as infrações em causa e para assegurar que os comportamentos dos autores, ainda desconhecidos, não permanecem impunes. Também devem ser tidos em conta os direitos de terceiros [70].

43. No que respeita aos direitos de terceiros, resulta [71] dos autos do órgão jurisdicional de reenvio que o Ministério Público (Bolzano) requereu o acesso aos dados relativos às comunicações provenientes dos telemóveis furtados a partir de 29 de outubro de 2021 a respeito do primeiro furto, cometido em 27 de outubro de 2021 [72], e de 20 de novembro de 2021, a propósito do segundo furto, cometido nesta data [73]. Estas datas demonstram que os pedidos de acesso têm um impacto muito limitado nos direitos das vítimas garantidos, designadamente, pelos artigos 7.º, 8.º e 11.º da Carta [74]. O Governo italiano referiu igualmente nas suas observações escritas que o processo nacional incide apenas sobre dados que são úteis para identificar o autor ou os autores dos furtos em causa. No caso de serem identificadas chamadas destinadas ou provenientes de terceiros não relacionados com o furto, tais dados são destruídos, em conformidade com o artigo 269.º do Código de Processo Penal [75]. Por último, o artigo 132.º, n.º 3, alínea c), do Decreto Legislativo n.º 196/2003 prevê que os dados recolhidos em violação dos n.ºs 3 ou 3-*bis* deste artigo não podem ser utilizados [76].

VI. Conclusão

44. Tendo em conta as considerações que precedem, proponho ao Tribunal de Justiça que responda à questão prejudicial submetida pelo Tribunale di Bolzano (Tribunal de Primeira Instância de Bolzano, Itália) do seguinte modo:

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

[69] Os telemóveis podem conter fotografias, dados de saúde, registos bancários, palavras-passe, etc. Como tal, o furto de um telemóvel pode comprometer a identidade digital do seu proprietário e as consequências deste ato podem superar consideravelmente as da perda do respetivo valor monetário. O órgão jurisdicional de reenvio deverá, por conseguinte, tomar em consideração e ponderar os eventuais danos aos direitos das vítimas, particularmente à luz dos artigos 7.º, 8.º e 17.º da Carta.

[70] Como as vítimas da alegada infração.

[71] Sob reserva de verificação pelo órgão jurisdicional de reenvio.

[72] Número RGNR 9228/2021.

[73] Número RGNR 9794/2021.

[74] Embora os dados estejam relacionados com comunicações destinadas à vítima após o furto, não são, na prática, relativos a comunicações feitas pela vítima ou à sua localização.

[75] Segundo o Governo italiano, a versão aplicável do artigo 269.º, n.º 2, do Código de Processo Penal prevê que «[…] os registos devem ser conservados até ao trânsito em julgado da decisão. No entanto, se os registos não forem relevantes para o processo, as partes interessadas podem, por razões de confidencialidade, requerer ao juiz que autorizou ou validou a interceção que ordene a destruição dos mesmos» (na medida em que sejam irrelevantes). Embora o acesso a dados de terceiros inocentes seja ilimitado, a utilização dos mesmos parece, sob reserva de verificação pelo órgão jurisdicional de reenvio, ser objeto de restrições pelo direito nacional.

[76] O pedido de decisão prejudicial não explica nem o sentido exato desta disposição nem como a mesma é aplicada na prática.

deve ser interpretado no sentido de que não se opõe a uma legislação nacional que exige que os órgãos jurisdicionais autorizem o acesso do Ministério Público a dados licitamente conservados pelos prestadores de serviços de comunicações eletrónicas que permitam tirar conclusões precisas sobre a vida privada de um utilizador, se estes dados forem relevantes para o apuramento dos factos e se houver indícios suficientes da prática de uma infração grave, na aceção do direito nacional, punível com uma pena máxima de prisão não inferior a três anos. Antes de concederem o acesso, os órgãos jurisdicionais nacionais devem proceder a uma apreciação individualizada para determinar se a ingerência nos direitos fundamentais que tal acesso implica é proporcionada em relação, nomeadamente, à gravidade da infração específica e aos factos do caso em apreço.