Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
MANUEL CAMPOS SÁNCHEZ-BORDONA
apresentadas em 20 de abril de 2023 [1]

Processo C-548/21

C. G.
contra
Bezirkshauptmannschaft Landeck

[pedido de decisão prejudicial apresentado pelo Landesverwaltungsgericht Tirol (Tribunal Administrativo Regional do Tirol, Áustria)]

«Reenvio prejudicial — Telecomunicações — Proteção de dados pessoais — Diretiva (UE) 2016/680 — Processo penal — Tentativa de acesso das autoridades públicas aos dados registados num telemóvel sem autorização judicial ou de uma autoridade administrativa independente»

1. Este pedido de decisão prejudicial tem por objeto, em substância, as condições que as autoridades policiais devem respeitar para aceder aos dados armazenados no telemóvel da pessoa visada por um inquérito penal.

2. Como procurarei explicar, o reenvio prejudicial apresenta insuficiências significativas no que respeita à sua admissibilidade. Se, todavia, o Tribunal de Justiça decidir proceder a uma análise quanto ao mérito, deverá pronunciar-se sobre os âmbitos de aplicação respetivos da Diretiva 2002/58/CE [2] e da Diretiva (UE) 2016/680 [3].

[1] Língua original: espanhol.

[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).

[3] Diretiva do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO 2016, L 119, p. 89).

I. Quadro jurídico

A. Direito da União

1. Regulamento (UE) 2016/679 [4]

3. O artigo 2.º («Âmbito de aplicação material»), n.º 2, prevê:

«O presente regulamento não se aplica ao tratamento de dados pessoais:

[…]

d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.»

2. Diretiva 2016/680

4. No considerando 2 afirma-se:

«Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar […] os seus direitos e liberdades fundamentais, particularmente o direito à proteção dos dados pessoais. A presente diretiva destina-se a contribuir para a realização de um espaço de liberdade, segurança e justiça.»

5. O considerando 46 enuncia:

«As restrições dos direitos do titular dos dados devem respeitar a Carta e a CEDH, de acordo com a interpretação na jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem [5], respetivamente, e devem respeitar, em particular, o conteúdo essencial desses direitos e liberdades.»

6. O considerando 49 tem a seguinte redação:

«Caso os dados pessoais sejam tratados no âmbito de uma investigação criminal ou de um processo judicial em matéria penal, os Estados-Membros deverão poder dispor que o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou apagamento, bem como à limitação do tratamento, seja feito nos termos das regras nacionais aplicáveis aos processos judiciais.»

7. O artigo 1.º («Objeto e objetivos») dispõe:

«1. A presente diretiva estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de

[4] Regulamento do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO 2016, L 119, p. 1, a seguir «RGPD».

[5] A seguir «TEDH».

prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública.

2. Nos termos da presente diretiva, os Estados-Membros asseguram:

a) A proteção dos direitos e das liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais; e

[…]

3. A presente diretiva não obsta a que os Estados-Membros prevejam garantias mais elevadas do que as nela estabelecidas para a proteção dos direitos e liberdades do titular dos dados no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes.»

8. O artigo 2.º («Âmbito de aplicação»), n.º 1, prevê:

«A presente diretiva aplica-se ao tratamento de dados pessoais pelas autoridades competentes para os efeitos estabelecidos no artigo 1.º, n.º 1.»

9. O artigo 3.º («Definições») dispõe:

«Para efeitos da presente diretiva, entende-se por:

[…]

2) "Tratamento", uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

[…]

7) "Autoridade competente":

   a) Uma autoridade pública competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; ou

[…]»

10. O artigo 4.º («Princípios relativos ao tratamento de dados pessoais»), n.º 1, prevê:

«Os Estados-Membros preveem que os dados pessoais sejam:

a) Objeto de um tratamento lícito e leal;

b) Recolhidos para finalidades determinadas, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades;

c) Adequados, pertinentes e limitados ao mínimo necessário relativamente às finalidades para as quais são tratados;

[…]

e) Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados;

f) Tratados de uma forma que garanta a sua segurança adequada, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas.»

11. O artigo 8.º («Licitude do tratamento») dispõe:

«1. Os Estados-Membros preveem que o tratamento só seja lícito se e na medida em que for necessário para o exercício de uma atribuição pela autoridade competente para os efeitos previstos no artigo 1.º, n.º 1, e tiver por base o direito da União ou de um Estado-Membro.

2. O direito de um Estado-Membro que rege o tratamento no âmbito da presente diretiva especifica pelo menos os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento.»

12. O artigo 13.º («Informações a facultar ou a fornecer ao titular dos dados») prevê:

«1. Os Estados-Membros preveem que o responsável pelo tratamento faculte ao titular dos dados pelo menos as seguintes informações:

[…]

d) O direito de apresentar reclamação à autoridade de controlo e de obter os contactos dessa autoridade;

[…]

3. Os Estados-Membros podem adotar medidas legislativas que prevejam o adiamento, a limitação ou a não prestação aos titulares dos dados das informações a que se refere o n.º 2 se e enquanto tais medidas constituírem medidas necessárias e proporcionadas numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de:

a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;

b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais;

c) Proteger a segurança pública;

d) Proteger a segurança nacional;

e) Proteger os direitos e as liberdades de terceiros.

[…]»

13. Em conformidade com o artigo 15.º («Limitações do direito de acesso»), n.º 1:

«Os Estados-Membros podem adotar medidas legislativas para limitar, total ou parcialmente, o direito de acesso do titular dos dados, se e enquanto tal limitação, total ou parcial, constituir uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de:

a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;

b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais;

c) Proteger a segurança pública;

d) Proteger a segurança nacional;

e) Proteger os direitos e as liberdades de terceiros.»

14. Nos termos do artigo 27.º («Avaliação de impacto sobre a proteção de dados»):

«1. Caso um tipo de tratamento, em particular que utilize novas tecnologias, e tendo em conta a sua natureza, âmbito, contexto e finalidades, seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, os Estados-Membros preveem que o responsável efetue, antes de iniciar o tratamento, uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais.

2. A avaliação a que se refere o n.º 1 inclui pelo menos uma descrição geral das operações de tratamento de dados previstas, uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados, as medidas previstas para fazer face a esses riscos, as garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade com a presente diretiva, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.»

15. O artigo 28.º («Consulta prévia da autoridade de controlo») prevê:

«1. Os Estados-Membros preveem que o responsável pelo tratamento ou o subcontratante consulte a autoridade de controlo antes de proceder ao tratamento de dados pessoais que farão parte de um novo ficheiro a criar caso:

a) A avaliação de impacto sobre a proteção de dados prevista no artigo 27.º indique que o tratamento resultaria num elevado risco na ausência das medidas a tomar pelo responsável pelo tratamento para atenuar o risco; ou

b) O tipo de tratamento envolva, especialmente no caso de se utilizarem novas tecnologias, mecanismos ou procedimentos, um elevado risco para os direitos e liberdades dos titulares dos dados.

[…]»

16. O artigo 54.º («Direito de intentar uma ação judicial contra um responsável pelo tratamento de dados ou um subcontratante») dispõe:

«Sem prejuízo de qualquer via de recurso administrativo ou extrajudicial disponível, nomeadamente o direito de apresentar reclamação junto de uma autoridade de controlo nos termos do artigo 52.º, os Estados-Membros preveem que os titulares dos dados têm o direito de intentar ação judicial se considerarem ter havido violação dos direitos que lhes assistem nos termos das disposições adotadas por força da presente diretiva na sequência de um tratamento dos seus dados pessoais que não cumpra tais disposições.»

B. Direito nacional

17. O § 18 do Strafprozessordnung[6] confere à Polícia Judiciária funções ao serviço da administração da justiça penal (n.º 1). As investigações da Polícia Judiciária são da responsabilidade das autoridades de segurança (n.º 2). Os órgãos do serviço de segurança pública asseguram o serviço executivo da Polícia Judiciária, que consiste em investigar e reprimir as infrações penais (n.º 3).

18. Nos termos do § 99 do StPO, a Polícia Judiciária investiga oficiosamente ou com base numa queixa, devendo acatar as ordens do Ministério Público e dos órgãos jurisdicionais (n.º 1). Quando uma medida de investigação exija uma ordem do Ministério Público, a Polícia Judiciária pode exercer o poder correspondente, mesmo na falta dessa ordem, em caso de perigo iminente. Nessa situação, deve pedir imediatamente a autorização (n.º 2).

19. Em conformidade com o § 111, n.º 2, do StPO, quando as informações armazenadas em suportes de dados devam ser objeto de recolha de dados, qualquer pessoa é obrigada a facultar o acesso a essas informações e, a pedido, a entregar ou a permitir a obtenção de um suporte de dados eletrónico num formato de arquivo correntemente utilizado. Além disso, deve permitir que seja feita uma cópia de segurança das informações armazenadas nos suportes de dados.

II. Matéria de facto, litígio e questões prejudiciais

20. C. G. é um cidadão alemão que trabalha e vive na Áustria.

21. Em 23 de fevereiro de 2021, no âmbito de um controlo de estupefacientes, os funcionários da alfândega de Innsbruck (Áustria) apreenderam uma encomenda dirigida a C. G. que continha 85 gramas de canábis.

22. Em 6 de março de 2021, dois agentes da polícia interrogaram C. G. sobre o remetente da encomenda e revistaram a sua residência. Durante essa busca, apreenderam o seu telemóvel (com um cartão SIM e outro SD) e entregaram-lhe o auto de apreensão.

23. Tenso sido convidado a dar acesso aos dados de ligação do seu telemóvel, C. G. recusou-se a fazê-lo e recusou-se também a revelar o código de acesso do telefone.

[6] Código de Processo Penal (BGBl nº 631/1975), na versão aplicável à data dos factos (BGBl I nº 24/2020) (a seguir «StPO»).

24. Na sede da polícia distrital em Landeck (Áustria) não foi possível desbloquear o telemóvel. Foi transferido para Viena para o Bundeskriminalamt (Departamento Federal de Polícia Criminal, Áustria), onde tentaram novamente, sem sucesso, desbloquear o telemóvel e aceder aos dados aí armazenados.

25. No que se refere a essas medidas, à data em foram tomadas pela polícia, não havia ordem do Ministério Público nem uma decisão judicial.

26. Em 31 de março de 2021, C. G. apresentou um recurso no Landesverwaltungsgericht Tirol (Tribunal Administrativo Regional do Tirol, Áustria) contra a medida de coação que lhe tinha sido aplicada, contestando a apreensão do seu telemóvel. Este foi-lhe devolvido em 20 de abril de 2021.

27. C. G. não foi informado sobre as tentativas de análise do conteúdo do telemóvel; teve conhecimento dessas tentativas quando o agente da polícia que efetuou a apreensão e subsequentemente iniciou a análise digital foi interrogado como testemunha sob juramento. Essas tentativas também não foram documentadas no processo de investigação criminal.

28. Neste contexto, o Landesverwaltungsgericht Tirol (Tribunal Administrativo Regional do Tirol, Áustria) submeteu ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Deve o artigo 15.º, n.º 1 (eventualmente em conjugação com o artigo 5.º), da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136/CE, lido à luz dos artigos 7.º e 8.º da Carta […], ser interpretado no sentido de que o acesso das autoridades públicas a dados armazenados em telemóveis constitui uma ingerência nos direitos fundamentais consagrados nestes artigos da Carta de tal modo grave que, no domínio da prevenção, investigação, deteção e repressão de infrações penais, esse acesso deve ser limitado à luta contra a criminalidade grave?

2) Deve o artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º, 11.º, bem como do artigo 52.º, n.º 1, da Carta […], ser interpretado no sentido de que se opõe a uma regulamentação nacional como o § 18, em conjugação com o § 99, n.º 1, [da StPO], que permite às autoridades de segurança obterem por si próprias, durante um inquérito penal e sem autorização de um tribunal ou de uma autoridade administrativa independente, um acesso total e não controlado a todos os dados digitais armazenados num telemóvel?

3) Deve o artigo 47.º da Carta […], em conjugação com o artigo 41.º e com o artigo 52.º da mesma Carta, na perspetiva do princípio da igualdade de armas e do direito a uma tutela jurisdicional efetiva, ser interpretado no sentido de que se opõe a uma regulamentação de um Estado-Membro que, como o § 18, em conjugação com o § 99, n.º 1, [da StPO], permite que um telemóvel seja analisado digitalmente, sem que o interessado seja informado previamente ou, pelo menos, depois de a medida ter sido tomada?»

III. Tramitação do processo no Tribunal de Justiça

29. O pedido de decisão prejudicial foi registado no Tribunal de Justiça em 6 de setembro de 2021.

30. Em 20 de outubro de 2021, o Tribunal de Justiça convidou o órgão jurisdicional de reenvio a indicar se a Diretiva 2016/680 poderia ser relevante para o presente processo.

31. Em 11 de novembro de 2021, o órgão jurisdicional de reenvio respondeu que a Diretiva 2016/680 deve ser aplicada no processo principal.

32. Apresentaram observações escritas os Governos alemão, austríaco, cipriota, dinamarquês, estónio, francês, húngaro, irlandês, neerlandês, norueguês, polaco e sueco, e a Comissão Europeia.

33. Na audiência realizada em 16 de janeiro de 2023, compareceram, com exceção dos Governos alemão, húngaro e polaco, todos os que tinham apresentado observações escritas e o Governo finlandês. Todos foram convidados pelo Tribunal de Justiça a concentrar os seus argumentos na Diretiva 2016/680 e a responder oralmente a determinadas questões relacionadas com esta.

IV. Análise

A. Inadmissibilidade

34. O órgão jurisdicional de reenvio formulou inicialmente as suas questões pedindo apenas a interpretação da Diretiva 2002/58. Todavia, praticamente todos os que intervieram no reenvio concordam quanto ao facto de essa diretiva não ser aplicável a este processo e, por conseguinte, a sua interpretação não ser necessária para dirimir o litígio.

35. Nos termos do seu artigo 3.º, a Diretiva 2002/58 regula o «[…] tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na [União], nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação».

36. O Tribunal de Justiça já declarou que «quando os Estados-Membros aplicam diretamente medidas que derrogam a confidencialidade das comunicações eletrónicas, sem imporem obrigações de tratamento aos prestadores de serviços de tais comunicações, a proteção dos dados das pessoas em causa não está abrangida pela Diretiva 2002/58, mas apenas pelo direito nacional, sem prejuízo da aplicação da [Diretiva 2016/680]» [7].

37. No presente processo, a tentativa de acesso aos dados foi efetuada diretamente pelas autoridades policiais no âmbito de um inquérito penal. Não houve intervenção dos prestadores de serviços de comunicações eletrónicas a quem não foi pedida a divulgação de dados pessoais. Por conseguinte, a Diretiva 2002/58 não é aplicável.

38. A legislação do direito da União que regula esta situação é a Diretiva 2016/680, que, nos termos do seu artigo 2.º, n.º 1, se aplica ao tratamento de dados pessoais pelas autoridades competentes para os «efeitos de […] investigação […] de infrações penais».

39. Isto bastaria para concluir pela inadmissibilidade do reenvio prejudicial, tal como tinha sido formulado pelo órgão jurisdicional nacional, uma vez que a legislação do direito da União cuja interpretação solicitava não era aplicável ao processo.

[7] 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; a seguir «Acórdão La Quadrature du Net», n.º 103).

40. Todavia, é verdade que o artigo 267.º TFUE permite que o Tribunal de Justiça reformule as questões que lhe são submetidas ou indique a existência de outras disposições do direito da União eventualmente pertinentes, de modo a dar ao órgão jurisdicional nacional uma resposta útil [8].

41. O Tribunal de Justiça convidou o órgão jurisdicional de reenvio a pronunciar-se sobre a eventual incidência da Diretiva 2016/680. Por conseguinte, deu-lhe a possibilidade de ele próprio completar ou reformular as suas questões. Em vez disso, o órgão jurisdicional de reenvio limitou-se a constatar que, «em todo o caso, no presente processo, há que respeitar as disposições da Diretiva 2016/680», sem no entanto identificar as suas disposições sobre as quais tem dúvidas e sem acrescentar outras considerações quanto ao mérito [9].

42. O Tribunal de Justiça já tem declarado reiteradamente que «é indispensável, como enuncia o artigo 94.º, alínea c), do Regulamento de Processo, que a decisão de reenvio contenha a exposição das razões que conduziram o órgão jurisdicional de reenvio a interrogar-se sobre a interpretação ou a validade de certas disposições do direito da União, bem como o nexo que esse órgão estabelece entre essas disposições e a legislação nacional aplicável ao litígio no processo principal» [10].

43. Ora, a inobservância dos requisitos do artigo 94.º do Regulamento de Processo é clara neste reenvio, em consequência do que precede. Ainda que o Tribunal de Justiça demonstre alguma flexibilidade a este respeito, a cooperação com o órgão jurisdicional de reenvio deve ser recíproca: na falta, injustificada, de colaboração por parte deste último para expor as suas dúvidas quanto à interpretação do direito da União que considere aplicável (no presente processo, a Diretiva 2016/680), parece-me lógico julgar inadmissível o pedido de decisão prejudicial [11].

44. Ao já referido acresce o facto de esse tribunal:

— Não ter especificado a natureza do tratamento tentado pelas autoridades policiais, ou dos dados pessoais concretamente procurados. Num primeiro momento, parece indicar que se limitava a dados de ligação (isto é, de tráfego e de localização), mas, posteriormente, não exclui que o desbloqueio do telefone permitisse o acesso a «todos os dados digitais armazenados» [12] ou mesmo ao conteúdo das comunicações e das mensagens eletrónicas trocadas por seu intermédio [13].

— Referir-se quer à apreensão do telefone e ao acesso, ou tentativa de acesso, aos dados nele contidos, quer à sua subsequente «exploração» (*Auswertung*), ou seja, a sua análise e leitura. Esta última, acrescenta, «implica um acesso total e não controlado a toda a comunicação digital do titular dos dados», o que torna possível «reconstruir uma imagem muito detalhada e aprofundada de quase todas as áreas da vida privada».

8 V., de forma genérica, Acórdão de 28 de abril de 2016, Oniors Bio (C-233/15, EU:C:2016:305, n.º 30).

9 O Tribunal de Justiça foi confrontado com a necessidade de convidar as partes a indicar «quais são, na sua opinião, as disposições pertinentes da Diretiva 2016/680 à luz das quais o Tribunal de Justiça deve, se for caso disso, reformular as três questões prejudiciais submetidas pelo órgão jurisdicional de reenvio» (quarta questão formulada para resposta oral na audiência).

10 Acórdão de 6 de outubro de 2021, Consorzio Italian Management e Catania Multiservizi (C-561/19, EU:C:2021:799, n.º 69).

11 Concordo com esta posição do Governo francês (n.ºs 36 a 41 das suas observações escritas).

12 Nomeadamente na segunda questão prejudicial.

13 O órgão jurisdicional de reenvio afirma que «no que se refere aos dados de ligação, o conteúdo de quase todos os contactos, de acordo com a frequência, o tempo e a duração da comunicação, no que se refere à comunicação efetuada através de SMS e outros serviços de mensagens, também pode ser reconstruído; através da análise de fotografias armazenadas e histórico de navegação, é fornecida igualmente uma visão muito íntima da vida privada da pessoa em questão».

45. Nestas condições, mais do que uma *reformulação* das questões do tribunal de origem, o Tribunal de Justiça procederia a uma verdadeira *reconstrução* do reenvio prejudicial que, além disso, se basearia parcialmente em considerações hipotéticas, e não em factos provados. Tudo isto, insisto, depois de ter dado ao órgão jurisdicional a possibilidade de ele próprio completar ou reformular as suas questões.

46. Por conseguinte, proponho que o reenvio prejudicial seja declarado inadmissível, como pediram vários dos Estados intervenientes.

47. O facto, salientado na audiência, de, no órgão jurisdicional de reenvio, já não existir um verdadeiro litígio que exija a interpretação de normas do direito da União também deveria conduzir a essa declaração de inadmissibilidade.

48. Com efeito, o Governo austríaco (de que dependem as autoridades policiais envolvidas na investigação) reconhece que a atuação dessas autoridades foi ilícita e violou os direitos da pessoa em causa. Uma vez que, segundo o despacho de reenvio, o pedido do recorrente no Tribunal Administrativo se dirigia precisamente contra as medidas de polícia consideradas ilícitas pela Administração recorrida, o diferendo submetido à apreciação do órgão jurisdicional de reenvio desapareceu.

49. De qualquer forma, caso o Tribunal de Justiça não concorde com a minha opinião, abordarei a seguir, a título subsidiário, os problemas de fundo que estão na base das questões prejudiciais.

50. Todavia, parece-me necessário começar por afastar a existência de outro fundamento de inadmissibilidade invocado por alguns intervenientes no processo [14]. Na sua opinião, como a Diretiva 2016/680 visa proteger as pessoas singulares no que diz respeito ao *tratamento* dos seus dados, não regularia situações como esta, em que não teria havido tratamento, mas sim uma simples *tentativa de acesso* a dados que acabaram por não poder ser obtidos.

51. Pelo contrário, para a Comissão, o efeito útil da Diretiva 2016/680 deverá privilegiar uma interpretação do seu objeto que não esteja limitada ao tratamento de dados em sentido estrito, abrangendo também questões que lhe estejam diretamente relacionadas. Uma destas seria a tentativa de aceder aos dados cujo tratamento se pretende [15].

52. Na minha opinião, sem que seja necessário forçar os limites do âmbito de aplicação da Diretiva 2016/680 [16], a sua aplicação a esta situação não se justifica pela apreensão do telefone móvel [17], mas sim pela atuação subsequente das autoridades policiais para obterem do mesmo determinados dados pessoais do titular dos dados, razão pela qual tentaram desbloqueá-lo e disponibilizar o acesso ao seu conteúdo.

[14] Refiro-me, em especial, aos Governos austríaco, francês, neerlandês e norueguês.

[15] Para a Comissão, «é indiferente que as tentativas tenham ou não sido bem-sucedidas. O surgimento de dificuldades técnicas que impedem o sucesso das tentativas de acesso constitui uma circunstância que não pode ser conhecida antecipadamente e que não afeta os riscos para a proteção dos dados pessoais».

[16] Em especial, parece-me desnecessário o recurso aos artigos 27.º e 28.º da Diretiva 2016/680, sugerido pela Comissão nas suas observações escritas. A «avaliação de impacto sobre a proteção de dados» prevista pelo artigo 27.º diz respeito, genericamente, a «um tipo de tratamento» e não a tratamentos individuais ou específicos. É o que resulta do considerando 58 da Diretiva 2016/680: «[a]s avaliações de impacto deverão ter como objeto os sistemas e processos pertinentes das operações de tratamento, mas *não casos individuais*» (o sublinhado é meu). Na audiência, a Comissão matizou a sua invocação destas duas disposições, que apenas teria referido para sublinhar o facto de a Diretiva 2016/680 prever igualmente situações anteriores ao tratamento dos dados propriamente dito.

[17] A Diretiva 2016/680 não regula a apreensão do telefone como meio de prova no âmbito de uma investigação criminal.

53. Entre as operações definidas como «tratamento» pelo artigo 3.º, ponto 2, da Diretiva 2016/680 encontra-se «qualquer outra forma de disponibilização» dos dados pessoais, efetuada no âmbito de uma investigação criminal. Considero que, quando a autoridade policial apreende um telefone onde esses dados são conservados e o manipula para dele os extrair, dá início a uma «operação» de tratamento, mesmo que não seja bem-sucedida por razões técnicas relativas à segurança criptográfica.

54. Uma tentativa malsucedida de acesso aos dados pessoais conservados num telemóvel, no âmbito de uma investigação criminal, é regulada pela Diretiva 2016/680 por motivos análogos aos que levaram o Tribunal de Justiça a declarar aplicável a Diretiva 2002/58 à *tentativa* (igualmente sem sucesso) de obter autorização judicial para aceder a determinados dados da pessoa objeto da investigação, detidos por um operador de comunicações eletrónicas [18].

55. Nesse contexto, se o órgão jurisdicional de reenvio tivesse de se pronunciar sobre a ilicitude da atuação policial (reconhecida pelo Governo austríaco, como já referi), a sua apreciação poderia depender da legalidade do fim visado por essa atuação, quer a medida tenha sido bem-sucedida, quer a sua execução tenha apenas sido iniciada, sem sucesso.

B. Quanto ao mérito

1. Primeira questão prejudicial

56. O órgão jurisdicional de reenvio pretende saber se, em conformidade com o artigo 15.º, n.º 1 (eventualmente em conjugação com o artigo 5.º), da Diretiva 2002/58, lido à luz dos artigos 7.º e 8.º da Carta, «o acesso das autoridades públicas a dados armazenados em telemóveis constitui uma ingerência nos direitos fundamentais consagrados nestes artigos da Carta de tal modo grave que, no domínio da prevenção, investigação, deteção e repressão de infrações penais, esse acesso deve ser limitado à luta contra a criminalidade grave».

57. Se o reenvio fosse admissível, a inaplicabilidade da Diretiva 2002/58 exigiria a reformulação da primeira questão, de modo que a resposta do Tribunal de Justiça interpretasse a Diretiva 2016/680.

58. Essa resposta deveria clarificar sucessivamente se se pode falar de ingerência em situações como a do presente processo e, havendo ingerência, se a Diretiva 2016/680 exige que o acesso aos dados seja limitado aos casos de luta contra a criminalidade grave.

59. Por definição, as operações de tratamento de dados são suscetíveis de comprometer o direito ao respeito pela vida privada (artigo 7.º da Carta) e o direito à proteção dos dados de caráter pessoal (artigo 8.º da Carta). Por conseguinte, as autoridades públicas devem respeitar as condições previstas no artigo 52.º, n.º 1, da Carta para justificar a sua intrusão no exercício desses direitos fundamentais.

[18] Acórdão de 2 de outubro de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

60. A intrusão nos direitos protegidos pelos artigos 7.º e 8.º da Carta será tanto maior quanto, com a mesma: a) se pretende o acesso a dados de natureza sensível habitualmente registados nos telemóveis e cujo conhecimento possa revelar aspetos da vida dos seus titulares que devem ficar ao abrigo do conhecimento de terceiros; e b) se possibilite o acesso ao conteúdo das comunicações.

61. Ora, de um ponto de vista geral e tendo em conta o seu conteúdo, a Diretiva 2016/680 não deve ser interpretada no sentido de que os tratamentos de dados a que se refere se limitam apenas aos casos de luta contra a criminalidade grave.

62. A Diretiva 2016/680 visa qualquer operação de tratamento [19] de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de *todos os tipos* de infrações penais.

63. Não resulta dos princípios que a Diretiva 2016/680 consagra relativamente ao tratamento de dados pessoais para esses efeitos (artigo 4.º), ou das condições de licitude para a sua realização (artigo 8.º), que, por via de regra, o tratamento de dados seja apenas possível em casos de criminalidade grave.

64. Uma limitação aos casos de luta contra a criminalidade grave também não se poderia basear na simples extrapolação da jurisprudência do Tribunal de Justiça relativa à Diretiva 2002/58 [20] para situações como a do presente processo.

65. Na minha opinião, não se pode fazê-lo porque, sob reserva do que exporei posteriormente, essa jurisprudência diz respeito à conservação generalizada e indiferenciada dos dados pessoais de um grupo genérico e indeterminado, efetuada de forma sistemática pelos prestadores de serviços de comunicações eletrónicas. A amplitude da ingerência que este tipo de conservação implica para a sociedade no seu conjunto explica que o Tribunal de Justiça se tenha manifestado de modo particularmente rigoroso ao proibi-la e ao prever as exceções a essa proibição.

66. Não é esse o caso quando o acesso pretendido não diz respeito ao conjunto ou a grandes grupos da população (isto é, aos dados pessoais de um grupo genérico e indeterminado), mas sim às informações armazenadas num determinado telemóvel, no âmbito de um processo de investigação criminal também determinado, regulado especificamente pela Diretiva 2016/680.

67. O objeto da Diretiva 2016/680 não é outro senão o tratamento de dados pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais. De todos os tipos de infrações penais, e não apenas das de natureza grave.

[19] A tipologia das «operações» a que se refere o artigo 3.º, ponto 2, da Diretiva 2016/680 é muito abrangente. V. a sua transcrição no n.º 9 das presentes conclusões.

[20] Acórdãos La Quadrature du Net e de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970; a seguir «Acórdão Tele2 Sverige e Watson»); de 2 de outubro de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); de 6 de outubro de 2020, Privacy International (C-623/17, EU:C:2020:790); e 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»).

68. De resto, como salientaram alguns intervenientes no reenvio prejudicial, na falta de uma indicação sobre a gravidade das infrações penais na Diretiva 2016/680, esta poderia não ser aplicada de modo uniforme nos Estados-Membros, uma vez que as apreciações de cada direito nacional relativas à maior ou menor gravidade de um comportamento punível divergem significativamente [21].

69. Em suma, a Diretiva 2016/680 não impõe, como condição de licitude, que o tratamento de dados pessoais aí previsto seja apenas possível para efeitos da luta contra a criminalidade grave.

70. Isto não prejudica o facto de que, em aplicação do princípio da proporcionalidade e caso a caso, o tratamento de dados que as autoridades competentes pretendam efetuar ao abrigo da Diretiva 2016/680 deva ser ajustado em função: a) da natureza das infrações penais objeto de repressão; e b) da qualidade dos dados pessoais visados por esse tratamento.

71. Nesse sentido, concordo com algumas das afirmações do Governo alemão relativas à limitação do acesso aos dados dos telefones apreendidos, quando permitam estabelecer um perfil completo da personalidade dos seus titulares, tendo em conta o seu conteúdo digital. Para o Governo alemão, esse acesso deveria limitar-se aos dados que sejam necessários como meio de prova numa situação concreta e poderia não ser adequado em presença de fatores como «o caráter menor da infração objeto da investigação ou o reduzido valor probatório dos dados que se pretendem obter» [22].

72. Por conseguinte, em *abstrato*, a Diretiva 2016/680 não implica que, por sistema, seja ilícito o acesso aos dados pessoais armazenados num telemóvel com o objetivo de facilitar a investigação sobre comportamentos suscetíveis de serem abrangidos pela criminalidade geral ou comum. O facto de esse acesso ser possível *em concreto* terá de ser apreciado em cada caso pela autoridade correspondente, à luz da sua necessidade e do critério de proporcionalidade a que acabo de fazer referência.

73. Em meu entender, é isso que resulta das disposições da Diretiva 2016/680 que fixam as condições de validade do tratamento de dados pessoais no âmbito da luta contra a criminalidade:

— O artigo 4.º, n.º 1, alínea a), nos termos do qual os dados devem ser «[o]bjeto de um tratamento lícito e leal».

— O artigo 8.º, n.º 1, em que se dispõe que o tratamento deve ser *necessário* e ter por base o direito da União ou de um Estado-Membro.

2. Segunda questão prejudicial

74. Com a sua segunda questão prejudicial, o órgão jurisdicional de reenvio pretende saber 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 «se opõe a uma regulamentação nacional como o § 18, em conjugação com o § 99, n.º 1, do [StPO], que permite às autoridades de segurança obterem por si próprias, durante um inquérito penal e sem autorização de um tribunal ou de uma autoridade administrativa independente, um acesso total e não controlado a todos os dados digitais armazenados num telemóvel».

[21] O Governo francês dá como exemplo as infrações em matéria de detenção e tráfico de droga, sobre cuja gravidade as normas penais da Áustria e da França divergem. O Governo sueco pronuncia-se no mesmo sentido.

[22] Observações escritas do Governo alemão, n.º 20.

75. A formulação da questão apresenta uma certa ambiguidade. O órgão jurisdicional de reenvio:

— Reconhece que o § 110.º, n.º 2, do StPO prevê que, em princípio, as apreensões de bens necessitam de autorização do Ministério Público. A autoridade policial só pode proceder a essas apreensões sem essa autorização nas situações excecionais previstas no n.º 3 desse mesmo artigo (que não parecem ocorrer no presente processo).

— Todavia, acrescenta que a análise das informações armazenadas nos telemóveis «não está regulamentado [no StPO] de forma unívoca» e que poderia ser assegurado pelas autoridades de segurança por sua própria iniciativa, sem autorização prévia.

76. O Governo austríaco disponibiliza uma versão da regulamentação nacional que não está em conformidade com a exposta no despacho de reenvio. Em especial, afirma que, nos termos do direito nacional, tanto a apreensão do telefone (exceto nos casos de urgência) como a análise dos dados aí armazenados é apenas possível após autorização do Ministério Público [23]. Na falta de uma ordem do Ministério Público, a exploração policial dos dados conservados nesse telefone é ilícita.

77. Compete ao órgão jurisdicional de reenvio verificar os termos da regulamentação interna. No âmbito do processo previsto no artigo 267.º TFUE, o Tribunal de Justiça não é competente para interpretar o direito nacional, e é ao juiz de reenvio, exclusivamente, que cabe determinar o exato alcance das disposições legislativas, regulamentares ou administrativas nacionais [24].

78. Sem pretender intervir na controvérsia sobre a interpretação do direito austríaco, parece-me difícil inferir das únicas disposições que o órgão jurisdicional de reenvio identifica (§ 18, em conjugação com o § 99, n.º 1, do StPO) a consequência que o próprio tribunal retira. Mas, repito, isso é algo que só esse órgão jurisdicional pode decidir.

79. Seja como for, o órgão jurisdicional de reenvio considera que a jurisprudência do Acórdão Prokuratuur [25], relativo à fiscalização prévia, por um órgão jurisdicional ou por uma autoridade independente, do acesso aos dados conservados, seria transponível para uma situação como a do presente processo.

80. Em contrapartida, para o Governo neerlandês, essa jurisprudência deve ser entendida no contexto de uma legislação nacional que permitia o acesso *geral* das autoridades competentes a *todos* os dados de tráfego e de localização conservados. Assim se explicaria a exigência de uma autorização judicial prévia que, todavia, poderia não se justificar no caso do acesso aos dados de um único telemóvel.

81. Na mesma ordem de ideias, o Governo norueguês argumenta que, entre as diversas garantias previstas pela Diretiva 2016/680 [26] não consta expressamente a relativa à necessidade de uma autorização prévia de uma autoridade judicial ou de uma autoridade administrativa independente.

[23] N.º 19 das observações do Governo austríaco. Refere a Decisão do Oberster Gerichtshof (Supremo Tribunal de Justiça, Áustria) de 13 de outubro de 2020 (Processo 11 Os 56/20z) que qualifica de ilegal, como violação dos direitos subjetivos da pessoa em causa, a análise da Polícia Judiciária dos dados de um telemóvel sem autorização do Ministério Público.

[24] V., de forma genérica, Acórdão de 28 de abril de 2022, SeGEC e o. (C-277/21, EU:C:2022:318, n.º 21).

[25] Acórdão Prokuratuur, n.º 51: «é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja, em princípio, sujeito a uma fiscalização prévia efetuada por um órgão jurisdicional ou por uma entidade administrativa independente e que a decisão desse órgão jurisdicional ou dessa entidade seja tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de perseguição penal».

[26] Além das dos artigos 4.º e 8.º, as previstas nos capítulos III («Direitos do titular dos dados»), IV («Responsável pelo tratamento e subcontratante»), VI («Autoridades de controlo independentes») e VIII («Vias de recurso, responsabilidade e sanções»).

82. A Comissão, partindo do facto de as disposições da Diretiva 2016/680 deverem ser interpretadas à luz da Carta, argumenta que a obrigação imposta aos Estados-Membros pelo artigo 8.º, n.º 1, dessa diretiva (condições de licitude do tratamento) implica a necessidade de respeitar os direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta.

83. Partilho da opinião da Comissão de que, no respeito dessas disposições da Carta, os legisladores nacionais são obrigados a definir as regras necessárias para assegurar que o acesso aos dados seja justificado caso a caso e que seja limitado ao estritamente necessário e proporcionado.

84. Todavia, essas regras nacionais não têm necessariamente de ser específicas para o acesso aos dados pessoais contidos, como no presente processo, num telefone móvel, podendo ser as previstas no direito interno, a título geral, em matéria de obtenção de provas.

85. A este respeito, já reproduzi o n.º 103 do Acórdão La Quadrature du Net no que respeita às medidas dos Estados-Membros que afetam a confidencialidade das comunicações eletrónicas, sem imporem obrigações de tratamento aos prestadores de serviços de tais comunicações [27].

86. Por conseguinte, sem que seja necessário deduzir da Diretiva 2016/680 regras *específicas* de natureza processual que garantam a licitude do acesso às informações armazenadas num telemóvel [28], aplicam-se as normas nacionais que regulam o exercício dos poderes de busca e de apreensão no âmbito das investigações criminais [29].

87. A remissão para as disposições do direito interno para garantir a legalidade do acesso nos termos da Diretiva 2016/680 é, aliás, conforme com a jurisprudência do TEDH. Foi precisamente numa situação respeitante à República da Áustria relativa ao artigo 8.º CEDH (direito ao respeito da vida privada e familiar, do domicílio e da correspondência) que o TEDH declarou que a legislação austríaca sobre a apreensão de objetos, nomeadamente documentos, é aplicável à busca e à apreensão de dados conservados em suportes informáticos [30].

88. Se, como defende o Governo austríaco ao referir-se à jurisprudência do Oberster Gerichtshof (Supremo Tribunal de Justiça, Áustria), as autoridades policiais não têm o direito de aceder aos dados conservados num determinado telemóvel sem autorização do Ministério Público, a segunda questão prejudicial perde grande parte do seu sentido.

89. Em todo o caso, a resposta a esta questão não pode excluir que o acesso aos dados pessoais do telefone apreendido conduza a «reconstruir uma imagem muito detalhada e aprofundada de quase todas as áreas da vida privada» do titular dos dados [31]. Se assim fosse, as autoridades policiais não poderiam prescindir da autorização prévia a que se refere o Acórdão Prokuratuur.

27 V. n.º 36 das presentes conclusões.

28 Empreendimento cuja dificuldade é demonstrada pelos esforços da Comissão nos n.ºs 34 a 39 das suas observações para contribuir para a definição de regras claras e precisas para a configuração dos limites e das garantias adequadas no que respeita ao acesso aos dados de um telemóvel.

29 Normas que, como recordam, por exemplo, os Governos dinamarquês e irlandês, não estão abrangidas pelo âmbito de aplicação do direito da União, mas que podem servir para satisfazer uma exigência resultante desse direito.

30 Acórdão do TEDH, 16 de outubro de 2007, Wieser e Bicos Beteiligungen c. Áustria (CE:ECHR:2007:1016JUD007433601, § 54): «the Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data».

31 V. afirmações do órgão jurisdicional de reenvio reproduzidas no n.º 44 das presentes conclusões.

90. À primeira vista, esta afirmação pareceria ser compaginável com a não aplicação a esta situação da Diretiva 2002/58 (interpretada pelo Acórdão Prokuratuur), como já defendi anteriormente. Todavia, considero que a *ratio* desse acórdão milita em favor da mesma solução.

91. No processo que deu origem ao Acórdão Prokuratuur, embora o acesso tenha sido realizado mediante a obtenção dos dados (metadados) dos prestadores de serviços de comunicações eletrónicas, tratava-se, como no presente processo, de um inquérito penal individual, dirigido contra uma pessoa determinada. Estava em causa a recolha de «dados de vários números de telefone […] e diferentes identidades internacionais de equipamento móvel desta» [32].

92. Na minha opinião, no Acórdão Prokuratuur podem distinguir-se dois planos: a) o que põe em causa a regulamentação geral de um Estado-Membro relativa à conservação generalizada e indiferenciada e ao acesso posterior aos dados detidos pelos prestadores de serviços; e b) o da fiscalização prévia, num caso particular, do acesso a esses metadados, quando permitem definir um perfil preciso da vida privada de uma pessoa.

93. O facto de, no presente processo, os dados reveladores da vida privada não serem detidos pelos prestadores de serviços e de serem obtidos (ou de se tentarem obter) a partir de um único telefone apreendido parece-me ter uma importância secundária relativamente à *ratio* da exigência de fiscalização prévia a que se recorre no Acórdão Prokuratuur.

94. Esta fiscalização prévia tem o seu fundamento último na proteção garantida pelos artigos 7.º e 8.º da Carta. A autoridade que a realize deve «[poder] assegurar um justo equilíbrio entre, por um lado, os interesses ligados às necessidades do inquérito no âmbito da luta contra a criminalidade e, por outro, os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas às quais o acesso diz respeito» [33].

3. Terceira questão prejudicial

95. Com a terceira questão prejudicial, o órgão jurisdicional de reenvio pretende saber se o artigo 47.º (em conjugação com o artigo 41.º e com o artigo 52.º) da Carta se opõe a uma legislação como a austríaca [34] que «permite que um telemóvel seja analisado digitalmente, sem que o interessado seja informado previamente ou, pelo menos, depois de a medida ter sido tomada».

96. Considero que a questão assim redigida poderia não ser necessária para resolver o litígio, pois o titular dos dados pôde exercer o direito consagrado no artigo 47.º da Carta, pedindo ao tribunal de reenvio a declaração da nulidade da atuação policial relativa ao telefone apreendido, que incluía a posterior (e malsucedida) exploração dos dados nele conservados.

97. No que respeita a esses dois momentos da atuação policial, importaria distinguir:

— Quanto à apreensão do próprio telefone, resulta das informações constantes dos autos que o titular dos dados dela teve conhecimento e que se recusou a fornecer às autoridades policiais o código de acesso para o desbloquear quando o apreenderam.

[32] Acórdão Prokuratuur, n.º 17.

[33] Acórdão Prokuratuur, n.º 52.

[34] Refere-se novamente ao § 18, em conjugação com o § 99, do StPO.

— Quanto à tentativa de análise dos dados, tudo parece indicar que o responsável pelo tratamento não informou o titular dos dados relativamente a essa operação, embora o Governo austríaco afirme que este último teve conhecimento de um relatório em que constatava a atuação da Polícia Judiciária respeitante ao telefone [35].

98. Por conseguinte, subsistem em torno da exploração dos dados e do seu conhecimento pelo titular dos mesmos determinadas ambiguidades que, como já referi, deveriam ter sido clarificadas pelo órgão jurisdicional de reenvio no despacho de reenvio e que não permitem dar uma resposta útil à terceira questão prejudicial.

99. De qualquer forma, para o caso de o Tribunal de Justiça não considerar inadmissível esta questão, pronunciar-me-ei sobre a mesma. Nessa situação, e tendo em conta a inaplicabilidade da Diretiva 2002/58, será necessário reformulá-la à luz da Diretiva 2016/680, cujos artigos 13.º, 15.º e 54.º contêm as pistas para a sua resposta.

100. Nos termos da Diretiva 2016/680, as informações sobre o tratamento dos dados a fornecer ao seu titular são as que são necessárias, nomeadamente, para: a) apresentar reclamação à autoridade de controlo [artigo 13.º, n.º 1, alínea d)]; e b) intentar ação judicial em caso de violação dos direitos garantidos pela Diretiva 2016/680, sem prejuízo de qualquer via de recurso administrativo ou extrajudicial disponível (artigo 54.º).

101. Todavia, importa não esquecer, que tanto o artigo 13.º, n.º 3, como o artigo 15.º, n.º 1, da Diretiva 2016/680 permitem que os Estados-Membros adotem medidas legislativas:

— Que prevejam o adiamento, a limitação ou a não prestação aos titulares dos dados das informações a que se refere o n.º 2 do artigo 13.º

— Para limitar, total ou parcialmente, o direito de acesso do titular dos dados aos dados tratados, se e enquanto essa limitação constituir uma medida necessária e proporcionada para, *inter alia*, evitar prejudicar as investigações ou os procedimentos oficiais ou judiciais ou evitar prejudicar a investigação de infrações penais [36].

102. Em todo o caso, a licitude do tratamento de dados não depende do respeito pelas autoridades competentes dos deveres (posteriores) que lhes são impostos pelo artigo 13.º da Diretiva 2016/680, mas sim da legalidade da finalidade que o tenha justificado; ou seja, do facto de essas autoridades administrativas terem o direito de proceder ao tratamento de dados pessoais.

103. Sob este ponto de vista, o facto de o titular dos dados ter sido informado das tentativas de acesso aos dados armazenados no telefone que lhe foi apreendido é de certa forma alheio, por si só, à legalidade por motivos materiais da atuação policial. O comportamento do responsável pelo tratamento eventualmente contrário aos deveres que o artigo 13.º da Diretiva 2016/680 lhe impõe poderá ter outras consequências, mas, repito, não afeta em si a licitude ou a ilicitude desse mesmo tratamento.

104. Cabe ao órgão jurisdicional de reenvio determinar se a regulamentação nacional permite o exercício eficaz desses direitos pela pessoa em causa.

[35] N.º 37 das suas observações escritas.

[36] Neste sentido, v. Acórdão Tele2 Sverige e Watson, n.º 121. A sua jurisprudência relativa à Diretiva 2002/58 é transponível para a Diretiva 2016/680 no contexto da garantia da proteção jurisdicional dos direitos dos titulares de dados objeto de tratamento.

V. Conclusão

105. Atendendo ao exposto, proponho que o Tribunal de Justiça declare inadmissível o pedido de decisão prejudicial apresentado pelo Landesverwaltungsgericht Tirol (Tribunal Administrativo Regional do Tirol, Áustria).

A título subsidiário, proponho que responda a esse pedido nos seguintes termos:

«1) Os artigos 4.º, n.º 1, alínea a), e 8.º, n.º 1, da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, em conjugação com os artigos 7.º, 8.º, e 52.º da Carta dos Direitos Fundamentais da União Europeia,

devem ser interpretados no sentido de que

num inquérito penal, o acesso pelas autoridades públicas aos dados pessoais armazenados num telemóvel, com vista ao seu tratamento, não está limitado aos casos de luta contra a criminalidade grave.

Esse acesso deve ser justificado caso a caso e limitar-se ao estritamente necessário e proporcionado, em função da natureza das infrações penais objeto de repressão e dos dados pessoais cujo acesso é pretendido.

As autoridades policiais não podem obter, por si próprias e sem autorização prévia de um órgão judicial, num inquérito penal, acesso total e não controlado a todos os dados armazenados num telemóvel, quando estes permitam obter uma imagem precisa da vida privada de uma pessoa.

2) Os artigos 13.º, 15.º e 54.º da Diretiva 2016/680, em conjugação com os artigos 47.º e 52.º da Carta,

devem ser interpretados no sentido de que

sem prejuízo das limitações permitidas pelo artigo 15.º, n.º 1, da Diretiva 2016/680, ou de outras vias de recurso administrativo ou extrajudicial disponíveis, o detentor de um telemóvel deve ser informado do tratamento dos dados pessoais nele armazenados que tenha sido realizado pelas autoridades correspondentes, no momento e nos termos que sejam necessários para garantir o exercício efetivo do seu direito de intentar ação judicial em caso de violação dos direitos reconhecidos pela Diretiva 2016/680.»