Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
GIOVANNI PITRUZZELLA
apresentadas em 21 de janeiro de 2020[1]

**Processo C-746/18**

**H. K.**
**contra**
**Prokuratuur**

[pedido de decisão prejudicial apresentado pelo Riigikohus (Supremo Tribunal, Estónia)]

«Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Confidencialidade das comunicações — Fornecedores de serviços de comunicações eletrónicas — Conservação generalizada e indiferenciada dos dados relativos ao tráfego e dos dados de localização — Investigações penais — Acesso da autoridade encarregada do inquérito aos dados conservados por períodos que vão de um dia a um ano — Autorização dada pelo Ministério Público — Utilização dos dados como provas no âmbito do processo penal — Diretiva 2002/58/CE — Artigo 1.º, n.º 3, artigo 3.º e artigo 15.º, n.º 1 — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.º, 8.º e 11.º bem como artigo 52.º, n.º 1»

## I. Introdução

1. O presente pedido de decisão prejudicial tem por objeto a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)[2], conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009[3], lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia[4].

2. Este pedido foi apresentado no âmbito de um processo penal instaurado contra H. K., pelo facto de esta ter cometido vários furtos, ter utilizado um cartão bancário pertencente a outra pessoa e ter cometido atos de violência contra uma pessoa que participa num processo judicial.

1 Língua original: francês.

2 JO 2002, L 201, p. 37.

3 JO 2009, L 337, p. 11; a seguir «Diretiva 2002/58».

4 A seguir «Carta».

3. As atas nas quais se baseia a constatação dessas infrações foram elaboradas, nomeadamente, com base em dados pessoais gerados no âmbito do fornecimento de serviços de comunicações eletrónicas. O Riigikohus (Supremo Tribunal, Estónia) tem dúvidas quanto à compatibilidade com o direito da União das condições em que os serviços de inquérito tiveram acesso a esses dados.

4. Estas dúvidas dizem respeito, em primeiro lugar, à questão de saber se a duração do período relativamente ao qual os serviços de inquérito tiveram acesso aos dados constitui um critério que permita avaliar a gravidade da ingerência que esse acesso constitui nos direitos fundamentais das pessoas em causa.

5. Em segundo lugar, o órgão jurisdicional de reenvio pretende saber se o Prokuratuur (Ministério Público, Estónia), tendo em conta as diferentes missões que lhe são confiadas pela regulamentação estónia, constitui uma autoridade administrativa «independente», na aceção do Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o.[5].

## II. Quadro jurídico

### *A. Diretiva 2002/58*

6. Por força do artigo 1.º, n.º 3, da Diretiva 2002/58, esta «não é aplicável a atividades fora do âmbito do Tratado que institui a Comunidade Europeia, tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia, e em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em matéria de direito penal».

7. Além disso, o artigo 15.º, n.º 1, desta diretiva dispõe que «[o]s 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 [6]. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito [da União], incluindo os mencionados nos n.ºs 1 e 2 do artigo 6.º do Tratado da União Europeia».

5 C-203/15 e C-698/15, a seguir «Acórdão Tele2 Sverige e Watson e o.», EU:C:2016:970 (n.º 120 e dispositivo, n.º 2).

6 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).

## *B. Direito estónio*

### *1. Lei relativa às Comunicações Eletrónicas*

8. A elektroonilise side seadus (Lei relativa às Comunicações Eletrónicas)[7], de 8 de dezembro de 2004, na versão aplicável ao litígio no processo principal, dispõe, no seu artigo 111[1], intitulado «Obrigação de conservar os dados»:

«[…]

(2) Os fornecedores de serviços de telefonia fixa e de telefonia móvel e da rede de serviços de telefonia fixa e de telefonia móvel têm de conservar os seguintes dados:

1) o número de quem faz a chamada e o nome e a morada do assinante;

2) o número de quem recebe a chamada e o nome e a morada do assinante;

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

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

5) o serviço de telefonia fixa ou móvel utilizado;

6) a identificação internacional de assinante móvel (*International Mobile Subscriber Identity* — IMSI) de quem faz e recebe a chamada;

7) a identificação internacional de equipamento móvel (*International Mobile Equipment Identity* — IMEI) de quem faz e recebe a chamada;

8) o identificador da célula no momento do início da chamada;

9) os dados que identificam a localização geográfica da célula por referência ao identificador do local no período durante o qual os dados são conservados;

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

[…]

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

[…]

[7] RT I 2004, 87, 593.

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

1) nos termos do kriminaalmenetluse seadustik [Código de Processo Penal [8]], para a autoridade encarregada do inquérito, a autoridade habilitada a adotar medidas de vigilância, o Ministério Público, o tribunal;

[…]»

*2. Código de Processo Penal*

9. O artigo 17.º do Código de Processo Penal, na versão aplicável ao litígio no processo principal, intitulado «Partes no processo», dispõe, no seu n.º 1:

«São partes no processo: o Ministério Público […]»

10. Nos termos do artigo 30.º do Código de Processo Penal, intitulado «O Ministério Público no processo penal»:

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

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

11. O artigo 90[1] do Código de Processo Penal, epigrafado «Pedido de dados às empresas de comunicação», prevê, nos seus n.os 2 e 3:

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

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

12. O artigo 211.º do Código de Processo Penal, intitulado «Objetivo da fase de instrução do processo», tem a seguinte redação:

«(1) O objetivo da fase de instrução do processo é a recolha de elementos de prova e a criação das outras condições necessárias a um processo judicial.

(2) Durante a fase de instrução, a autoridade encarregada do inquérito e o Ministério Público verificam os elementos incriminatórios e os elementos desculpantes recolhidos contra o suspeito ou o acusado.»

[8] RT I 2003, 27, 166.

*3. Lei relativa ao Ministério Público*

13. A prokuratuuriseadus (Lei relativa ao Ministério Público)[9], de 22 de abril de 1998, na sua versão aplicável ao litígio no processo principal, dispõe, no seu artigo 1.º, epigrafado «Ministério Público»:

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

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

[…]»

14. O artigo 2.º da Lei relativa ao Ministério Público, epigrafado «Procurador», prevê, no seu n.º 2:

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

## III. Matéria de facto, tramitação do processo principal e questões prejudiciais

15. Por Decisão de 6 de abril de 2017, H. K. foi condenada, pelo Viru Maakohus (Tribunal de Primeira Instância de Viru, Estónia), numa pena de prisão de dois anos por ter cometido, no período compreendido entre 4 de agosto de 2015 e 1 de fevereiro de 2016, oito furtos de produtos alimentares e outros bens materiais de valor compreendido entre 3 e 40 euros bem como de quantias em dinheiro de montantes compreendidos entre 5,20 e 2 100 euros, por ter utilizado o cartão bancário de outra pessoa para levantar dinheiro num distribuidor automático, causando a essa pessoa um prejuízo de 3 941,82 euros e por ter cometido atos de violência contra uma pessoa que participa num processo judicial[10].

16. Para condenar H. K. por estas infrações, o Viru Maakohus (Tribunal de Primeira Instância de Viru) baseou-se, nomeadamente, em várias atas elaboradas a partir de dados relativos a comunicações eletrónicas, previstos no artigo 111[1], n.º 2, da Lei relativa às Comunicações Eletrónicas, que a autoridade encarregada do inquérito tinha recolhido junto de um fornecedor de serviços de telecomunicações durante a fase de instrução, depois de ter obtido, nos termos do artigo 90[1], n.º 2, do Código de Processo Penal, autorizações concedidas por um procurador do Viru Ringkonnaprokuratuur (procuradoria do distrito de Viru, Estónia).

17. Assim, em 2 de novembro de 2015, um procurador da procuradoria do distrito de Viru autorizou a autoridade encarregada do inquérito a exigir à empresa de telecomunicações o fornecimento dos dados referidos no artigo 111[1], n.º 2, da Lei relativa às Comunicações

[9] RT I 1998, 41, 625.

[10] O órgão jurisdicional de reenvio precisa que, após cúmulo desta pena com a pena de prisão de quatro anos e sete meses a que H. K. tinha sido condenada por Decisão de 22 de março de 2016 do Viru Maakohus (Tribunal de Primeira Instância de Viru), H. K. foi condenada numa pena de prisão global de cinco anos e um mês.

Eletrónicas, a fim de determinar, através de dois números de telefone móvel de H. K., a transmissão de comunicações e de mensagens, a duração destas e a maneira como a transmissão foi efetuada, bem como os dados pessoais e a localização de quem fez a chamada/emissor e de quem recebeu/destinatário em 21 de setembro de 2015.

18. Em 4 de novembro de 2015, a autoridade encarregada do inquérito elaborou uma ata relativa aos dados obtidos da empresa de telecomunicações ao abrigo dessa autorização, na qual eram indicados os mastros de transmissão, em cujo raio de ação o número de assinante utilizado por H. K. tinha sido utilizado em 21 de setembro de 2015 depois das 19 horas. O Ministério Público pretendia, através desta ata e de outras provas, demonstrar ao tribunal que H. K. tinha cometido o furto ocorrido em 21 de setembro de 2015.

19. Em 25 de fevereiro de 2016, um procurador da procuradoria do distrito de Viru autorizou a autoridade encarregada do inquérito a exigir à empresa de telecomunicações que fornecesse, com vista ao inquérito relativo a uma infração prevista no artigo 303.º, n.º 1, do Karistusseadustik (Código Penal) [11], dos dados referidos no artigo 111[1], n.º 2, da Lei relativa às Comunicações Eletrónicas relativos aos sete números de assinante utilizados por H. K. durante o período de 1 de março de 2015 a 19 de fevereiro de 2016.

20. Em 15 de março de 2016, a autoridade encarregada do inquérito elaborou uma ata sobre os dados obtidos da empresa de telecomunicações ao abrigo desta autorização, da qual constam as datas em que H. K. telefonou aos seus coacusados e recebeu chamadas destes, bem como as datas em que H. K. enviou mensagens aos seus coacusados e recebeu mensagens destes. O Ministério Público pretendeu, através desta ata e de outras provas, demonstrar ao tribunal que H. K., desde a primavera de 2015, tinha ameaçado repetidamente os coacusados por telefone.

21. Em 20 de abril e 6 de maio de 2016, a autoridade encarregada do inquérito elaborou ainda mais atas relativas aos dados obtidos da empresa de telecomunicações ao abrigo da mesma autorização. Estas atas indicam as estações base em cujo raio de ação foram feitas e recebidas as chamadas de 4, 27 e 31 de agosto de 2015 bem como de 1 a 3 de setembro de 2015, através dos seis números de assinante utilizados por H. K. Através dessas atas e de todas as outras provas, o Ministério Público pretendeu demonstrar ao tribunal que os seis furtos ocorridos nos dias indicados tinham sido cometidos por H. K.

22. Em 20 de abril de 2016, a autoridade encarregada do inquérito elaborou uma ata que continha os dados relativos a dois números de assinante utilizados por H. K. Mais precisamente, esta ata indica as estações base em cujo raio de ação foram feitas e recebidas chamadas de 16 a 19 de janeiro de 2015 através desses números de assinante. Com essa ata e outras provas, o Ministério Público pretendeu demonstrar que era H. K. quem, de 17 a 19 de janeiro de 2015, tinha levantado dinheiro do caixa automático utilizando o cartão bancário da vítima.

23. Os dados na origem da referida ata foram obtidos da empresa de telecomunicações ao abrigo das autorizações que um procurador da procuradoria do distrito de Viru tinha emitido noutro processo penal em 28 de janeiro e em 2 de fevereiro de 2015. Este processo tinha por objeto infrações previstas no artigo 200.º, n.º 2, pontos 7, 8 e 9, do Código Penal, a saber, dois roubos, cometidos em 23 e 27 de janeiro de 2015 por um grupo com utilização de uma arma e por arrombamento. Ao abrigo dessas autorizações, a autoridade encarregada do inquérito podia

[11] Trata-se da infração que consiste em exercer influência sobre a justiça. Saliento que os factos imputados a H. K. foram, quanto a este aspeto, requalificados pelo Viru Maakohus (Tribunal de Primeira Instância de Viru), em conformidade com o artigo 323.º, n.º 1, do Código Penal, como violência contra uma pessoa que participa num processo judicial.

exigir à empresa de telecomunicações o fornecimento, para o período de 1 de janeiro a 2 de fevereiro de 2015, dos dados referidos no artigo 111[1], n.º 2, da Lei relativa às Comunicações Eletrónicas quanto aos dois números de assinante e às diferentes identificações internacionais de equipamento móvel de H. K.

24. Resulta desta descrição dos factos do processo principal que o Ministério Público, em conformidade com o artigo 90[1], n.º 2, do Código de Processo Penal, autorizou a autoridade encarregada do inquérito a enviar pedidos de fornecimento de dados à empresa de telecomunicações no decurso da fase de instrução. As autorizações relativas aos dados dos números de assinante da pessoa arguida foram emitidas com vista a um inquérito relativo a diferentes infrações penais quanto a um período de, respetivamente, um dia, cerca de um mês e cerca de um ano.

25. H. K. interpôs recurso da decisão do Viru Maakohus (Tribunal de Primeira Instância de Viru) para o Tartu Ringkonnakohus (Tribunal de Recurso de Tartu, Estónia), que negou provimento ao mesmo por Decisão de 17 de novembro de 2017. H. K. interpôs então recurso de cassação no Riigikohus (Supremo Tribunal), pedindo a anulação das decisões de primeira e de segunda instância, a extinção do processo penal e a sua absolvição.

26. H. K. alega que as atas que contêm dados obtidos junto da empresa de telecomunicações não são provas admissíveis e que a sua condenação a partir dessas atas é infundada. Em conformidade com o Acórdão Tele2 Sverige e Watson e o., as regras do artigo 111[1] da Lei relativa às Comunicações Eletrónicas que preveem a obrigação destes fornecedores de serviços de conservarem dados relativos às comunicações bem como a utilização desses dados para efeitos da sua condenação são contrárias ao artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta.

27. Segundo o órgão jurisdicional de reenvio, coloca-se, assim, a questão de saber se as atas em causa, que a autoridade encarregada do inquérito elaborou a partir de dados, previstos no artigo 111[1], n.º 2, da Lei relativa às Comunicações Eletrónicas, exigidos à empresa de telecomunicações com a autorização do Ministério Público, podem ser consideradas provas admissíveis.

28. Os dados que os fornecedores de serviços de comunicações eletrónicas deviam conservar durante um ano incluem, nomeadamente, o número de quem faz e quem recebe a chamada, o nome e a morada do assinante, a data e a hora do início e do fim da chamada, o serviço de telefonia fixa ou móvel utilizado, a identificação internacional de assinante móvel e a identificação internacional de equipamento móvel de quem faz e de quem recebe a chamada, bem como o identificador da célula no momento do início da chamada e os dados que identificam a localização geográfica da célula. O órgão jurisdicional de reenvio salienta que se trata de dados que estão associados à existência de uma transferência de comunicações e de mensagens através de um telefone fixo ou móvel, bem como à localização da utilização do aparelho de comunicação móvel, mas que esses dados não fornecem informações sobre o conteúdo das comunicações.

29. Como resulta dos Acórdãos Tele2 Sverige e Watson e o. e de 2 de outubro de 2018, Ministerio Fiscal [12], uma regulamentação nacional que rege a conservação dos dados de tráfego e dos dados de localização, bem como o acesso a esses dados no âmbito de um processo penal, como o artigo 111[1], n.os 2 e 4, da Lei relativa às Comunicações Eletrónicas e o artigo 90[1], n.º 2, do Código de Processo Penal, está abrangida pelo âmbito de aplicação da Diretiva 2002/58.

30. A admissibilidade das provas depende da observância das regras processuais que regem a recolha destas. Assim, ao apreciar a admissibilidade, enquanto provas, das atas em questão no processo principal, importa igualmente examinar a questão de saber em que medida a recolha dos dados junto da empresa de telecomunicações, em que essas atas se baseiam, estava em conformidade com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta.

31. Tendo em conta os Acórdãos Tele2 Sverige e Watson e o. [13] bem como Ministerio Fiscal [14], o órgão jurisdicional de reenvio interroga-se sobre a questão de saber se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que o acesso das autoridades nacionais a dados que permitem encontrar e identificar a origem e o destino de uma comunicação telefónica a partir do telefone fixo ou móvel do suspeito, determinar a respetiva data, hora, duração e natureza, identificar o material de comunicação utilizado, bem como localizar o material de comunicação móvel utilizado, constitui uma ingerência de tal modo grave nos direitos fundamentais garantidos por estes artigos da Carta que esse acesso deve ser limitado à luta contra a criminalidade grave, independentemente do período em relação ao qual as autoridades nacionais têm acesso aos dados conservados.

32. A este respeito, o órgão jurisdicional de reenvio considera que o período durante o qual os dados em causa são exigidos constitui um elemento essencial para a apreciação da gravidade da ingerência nos direitos fundamentais que constitui o acesso aos dados em causa. É possível, portanto, que essa ingerência não deva ser considerada grave, quando os dados exigidos apenas digam respeito a um período muito curto, como um dia. Neste caso, não é possível, em geral, retirar, a partir destes dados, conclusões precisas sobre a vida privada da pessoa em causa, pelo que o acesso das autoridades nacionais aos referidos dados poderia ser justificado pelo objetivo de investigação e de repressão das infrações penais em geral.

33. Além disso, o órgão jurisdicional de reenvio interroga-se sobre a questão de saber se o acesso a dados como os que estão em causa no processo principal, tendo em conta os ensinamentos decorrentes do Acórdão Ministerio Fiscal [15], pode ser justificado por esse mesmo objetivo, quando a quantidade de dados a que as autoridades têm acesso é reduzida e a ingerência nos direitos fundamentais em causa não é, portanto, grave. No que respeita à quantidade de dados, é essencial ter em conta o tipo de dados (como os relativos ao destino de uma comunicação ou à localização do material) e a duração do período em causa (por exemplo, um mês ou um ano). Segundo este órgão jurisdicional, quanto mais grave for a infração, mais grave pode ser a ingerência autorizada nos direitos fundamentais no âmbito do processo, o que significa que a quantidade de dados a que as autoridades nacionais podem ter acesso é igualmente maior.

12 C-207/16, a seguir «Acórdão Ministerio Fiscal», EU:C:2018:788.

13 Dispositivo, n.º 2), desse acórdão.

14 N.os 53 e 57 desse acórdão.

15 N.os 55 a 57 desse acórdão.

34. Por fim, o órgão jurisdicional de reenvio interroga-se sobre a questão de saber se o Ministério Público pode ser considerado uma autoridade administrativa «independente», na aceção do Acórdão Tele2 Sverige e Watson e o.[16]. Salienta que, na Estónia, é o Ministério Público que dirige a fase de instrução cujo objetivo é, nomeadamente, a recolha de provas. Sublinha igualmente que a autoridade encarregada do inquérito e o Ministério Público verificam os elementos incriminadores e os elementos desculpantes relativos ao suspeito. Observa, por último, que as competências do Ministério Público são exercidas em seu nome por um procurador que desempenha as suas funções de modo independente, o que resulta do artigo 30.º, n.ºs 1 e 2, do Código de Processo Penal e do artigo 1.º, n.ºs 1 e 1[1], bem como do artigo 2.º, n.º 2, da Lei relativa ao Ministério Público.

35. Neste contexto, o órgão jurisdicional de reenvio sublinha que as suas dúvidas quanto à independência exigida pelo direito da União são principalmente devidas ao facto de, após a fase de instrução, caso o Ministério Público esteja convencido de que todas as provas necessárias foram recolhidas e se houver motivos para o fazer, o Ministério Público apresenta a acusação contra a pessoa em causa. O órgão jurisdicional de reenvio salienta que, neste caso, é o Ministério Público que representa a ação penal no processo e que é também, portanto, parte no processo. O órgão jurisdicional de reenvio salienta igualmente que Tribunal Europeu dos Direitos do Homem já admitiu que, em certas condições, podem ser autorizados atos de vigilância sem fiscalização jurisdicional prévia, desde que exista uma fiscalização jurisdicional *a posteriori*[17].

36. Nestas condições, o Riigikohus (Supremo Tribunal) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Deve o artigo 15.º, n.º 1, da Diretiva [2002/58], lido em conjugação com os artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da [Carta], ser interpretado no sentido de que o acesso das autoridades nacionais, no âmbito de um processo penal, a dados que permitem encontrar e identificar a origem e o destino de uma comunicação telefónica a partir do telefone fixo ou móvel do suspeito, determinar a data, a hora, a duração e a natureza, identificar o material de comunicação utilizado e localizar o material de comunicação móvel utilizado constitui uma ingerência de tal modo grave nos direitos fundamentais garantidos pelos artigos já referidos da Carta que, relativamente à prevenção, à investigação, à deteção e à repressão de infrações penais, este acesso deve ser limitado à luta contra a criminalidade grave, independentemente do período em relação ao qual as autoridades nacionais têm acesso aos dados conservados?

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

[16] N.º 120 e dispositivo, n.º 2), desse acórdão.

[17] O órgão jurisdicional de reenvio refere, a este respeito, os Acórdãos do TEDH de 2 de setembro de 2010, Uzun c. Alemanha (CE:ECHR:2010:0902JUD003562305, §§ 71 a 74), e de 12 de janeiro de 2016, Szabó e Vissy c. Hungria (CE:ECHR:2016:0112JUD003713814, § 77).

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

## IV. Análise

37. Com a primeira e a segunda questões prejudiciais, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que, entre os critérios que permitem apreciar a gravidade da ingerência nos direitos fundamentais que constitui o acesso pelas autoridades nacionais competentes a dados pessoais que os fornecedores de serviços de comunicações eletrónicas são obrigados a conservar por força de uma regulamentação nacional, se encontram as categorias de dados em causa bem como a duração do período relativamente ao qual o acesso é pedido.

38. Antes de responder a esta questão, formularei duas séries de observações preliminares que me permitirão responder, por um lado, aos argumentos invocados por alguns Estados-Membros no que respeita ao âmbito de aplicação da Diretiva 2002/58 e, por outro, à sugestão da Comissão Europeia de examinar, no âmbito do presente reenvio prejudicial, a compatibilidade com o direito da União da regulamentação estónia, na medida em que impõe aos fornecedores de serviços de comunicações eletrónicas que conservem várias categorias de dados pessoais gerados no âmbito desses serviços.

### *A. Observações preliminares*

#### *1. Quanto ao âmbito de aplicação da Diretiva 2002/58*

39. Os Governos irlandês, húngaro e polaco suscitam questões quanto ao âmbito de aplicação da Diretiva 2002/58.

40. O Governo irlandês parece considerar que uma regulamentação nacional relativa ao acesso das autoridades competentes em matéria penal a dados conservados é, por força do artigo 1.º, n.º 3, da Diretiva 2002/58, excluída do âmbito de aplicação desta diretiva.

41. Este argumento deve ser afastado, aplicando a jurisprudência do Tribunal de Justiça decorrente dos Acórdãos Tele2 Sverige e Watson e o. bem como Ministerio Fiscal.

42. A este respeito, há que indicar que o Tribunal de Justiça declarou que as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 «estão abrangidas pelo âmbito de aplicação desta diretiva, mesmo que digam respeito a atividades próprias do Estado ou das autoridades estatais, estranhas aos domínios de atividade dos particulares e mesmo que as finalidades a que tais

medidas devem dar resposta coincidam substancialmente com as finalidades prosseguidas pelas atividades referidas no artigo 1.º, n.º 3, da Diretiva 2002/58» [18]. Com efeito, segundo o Tribunal de Justiça, «o artigo 15.º, n.º 1, desta diretiva pressupõe necessariamente que as medidas nacionais aí referidas estão abrangidas pelo âmbito de aplicação da referida diretiva, uma vez que esta última só autoriza expressamente os Estados-Membros a adotá-las respeitando as condições nela previstas. Além disso, as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 regulam, para os efeitos mencionados nesta disposição, a atividade dos fornecedores de serviços de comunicações eletrónicas» [19].

43. O Tribunal de Justiça retirou daí a conclusão de que «o referido artigo 15.º, n.º 1, lido em conjugação com o artigo 3.º da Diretiva 2002/58, deve ser interpretado no sentido de que está abrangida pelo âmbito de aplicação desta diretiva, não só uma medida legislativa que impõe aos fornecedores de serviços de comunicações eletrónicas a conservação dos dados de tráfego e dos dados de localização, mas também uma medida legislativa que tem por objeto o acesso das autoridades nacionais aos dados conservados por esses fornecedores» [20].

44. Com efeito, segundo o Tribunal de Justiça, «a proteção da confidencialidade das comunicações eletrónicas e dos respetivos dados de tráfego, 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. Como confirma o considerando 21 desta diretiva, esta tem como objetivo impedir "o acesso" não autorizado às comunicações, incluindo a "quaisquer dados com ela relacionados", para proteger a confidencialidade das comunicações eletrónicas» [21].

45. A estes argumentos, o Tribunal de Justiça acrescentou que «medidas legislativas que impõem aos fornecedores de serviços de comunicações eletrónicas a conservação dos dados pessoais ou de conceder às autoridades nacionais competentes o acesso a esses dados, implicam necessariamente, da parte destes, o tratamento dos referidos dados […]. Por conseguinte, essas medidas, dado que regulam as atividades dos referidos fornecedores, não podem ser equiparadas às atividades próprias dos Estados, referidas no artigo 1.º, n.º 3, da Diretiva 2002/58» [22].

46. À semelhança do que o Tribunal de Justiça declarou no seu Acórdão Ministerio Fiscal [23], há que deduzir de todos estes argumentos que um pedido de acesso a dados pessoais conservados por fornecedores de serviços de comunicações eletrónicas, formulado no âmbito de uma fase de instrução penal, é abrangido pelo âmbito de aplicação da Diretiva 2002/58.

47. Por outro lado, os Governos húngaro e polaco invocam o argumento segundo o qual o direito da União não regula a questão da admissibilidade das provas nos processos penais.

48. Embora seja verdade que o direito da União, no estado atual da sua evolução, não regula as regras relativas à admissibilidade das provas num processo penal, o órgão jurisdicional de reenvio sublinhou claramente, todavia, de que modo a interpretação do direito da União que solicita é necessária para que possa pronunciar-se sobre a admissibilidade das provas. Com efeito, essa admissibilidade depende da observância dos requisitos e das regras processuais que regem a

18 Acórdão Ministerio Fiscal (n.º 34 e jurisprudência referida).

19 *Idem.*

20 Acórdão Ministerio Fiscal (n.º 35 e jurisprudência referida).

21 Acórdão Ministerio Fiscal (n.º 36 e jurisprudência referida).

22 Acórdão Ministerio Fiscal (n.º 37 e jurisprudência referida).

23 V. Acórdão Ministerio Fiscal (n.ºs 38 e 39).

recolha dessas provas. Assim, ao apreciar a admissibilidade como provas das atas em causa no processo principal, o órgão jurisdicional de reenvio deve examinar a questão prévia de saber em que medida a recolha de dados junto da empresa de telecomunicações, em que essas atas se basearam, era conforme com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta. Ora, esta questão prévia tem por objeto um aspeto que, como salientei atrás, é regido pelo direito da União. Quanto a este aspeto, as regras nacionais aplicáveis em matéria de produção da prova devem, portanto, respeitar as exigências decorrentes dos direitos fundamentais garantidos pelo direito da União [24]. Nestas condições, o argumento invocado pelos Governos húngaro e polaco não é, na minha opinião, pertinente.

*2. Quanto à conservação dos dados de tráfego e dos dados de localização*

49. Embora as questões submetidas pelo órgão jurisdicional de reenvio incidam sobre as condições de acesso aos dados, a Comissão convida o Tribunal de Justiça a pronunciar-se igualmente, no âmbito do presente reenvio prejudicial, sobre a problemática relativa à conservação dos dados. A este respeito, observa, em substância, que um acesso legal aos dados conservados exige que a regulamentação nacional que impõe aos fornecedores de serviços de comunicações eletrónicas a conservação dos dados gerados no âmbito desses serviços satisfaça as exigências impostas pelo artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz da Carta, ou que os dados em causa tenham sido conservados por esses fornecedores por sua própria iniciativa, nomeadamente para fins comerciais, em conformidade com esta mesma diretiva.

50. No que respeita ao processo principal, a Comissão observa que os dados a que a autoridade encarregada do inquérito teve acesso não foram conservados pelos fornecedores de serviços de comunicações eletrónicas por sua iniciativa própria para fins comerciais, mas por força da obrigação de conservação que lhes é imposta pelo artigo 111[1] da Lei relativa às Comunicações Eletrónicas. Salienta igualmente que H. K. contesta a legalidade das regras nacionais relativas tanto ao acesso aos dados como à sua conservação [25].

51. No entanto, saliento que, à semelhança do que se verificava no âmbito do reenvio prejudicial que deu origem ao Acórdão Ministerio Fiscal [26], as questões formuladas pelo órgão jurisdicional de reenvio no âmbito do presente processo não visam determinar se os dados pessoais em causa no processo principal foram conservados pelos fornecedores de serviços de comunicações eletrónicas respeitando os requisitos previstos no artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta. Estas questões dizem unicamente respeito à compatibilidade com estas disposições das condições em que o acesso pelas autoridades nacionais de inquérito a esses dados é autorizado nos termos da regulamentação estónia. Foi por esta razão que o debate que se gerou perante o Tribunal de Justiça incidiu quase exclusivamente sobre estas condições de acesso.

52. Em qualquer caso, o órgão jurisdicional de reenvio pode basear-se na jurisprudência decorrente do Acórdão Tele2 Sverige e Watson e o. se considerar necessário, para resolver o litígio no processo principal, pronunciar-se sobre a compatibilidade com o direito da União do artigo 111[1] da Lei relativa às Comunicações Eletrónicas.

[24] V., nomeadamente, por analogia, Acórdão de 10 de abril de 2003, Steffensen (C-276/01, EU:C:2003:228, n.º 71). Neste acórdão, o Tribunal de Justiça aborda igualmente esta problemática na perspetiva do princípio da efetividade, como limite à autonomia processual dos Estados-Membros (n.os 66 a 68 do referido acórdão).

[25] A Comissão sublinha, neste contexto, que o presente processo se distingue do que deu origem ao Acórdão Ministerio Fiscal.

[26] V. Acórdão Ministerio Fiscal (n.os 49 e 50).

53. A este respeito, gostaria apenas de recordar que, segundo o Tribunal de Justiça, «o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica» [27].

54. Incumbe ao órgão jurisdicional de reenvio verificar, sendo caso disso, se a regulamentação estónia impõe aos fornecedores de serviços de comunicações eletrónicas uma obrigação de conservação dos dados que apresente tal caráter generalizado e indiferenciado e daí retirar as consequências para a resolução do litígio no processo principal. Se o regime de conservação de dados instituído pela República da Estónia fosse considerado não conforme com o direito da União, por ser desproporcionado relativamente ao objetivo prosseguido, o acesso aos dados assim conservados também não poderia ser justificado por esse mesmo objetivo.

55. É só no caso de esta obrigação de conservação ser acompanhada de limitações adequadas, nomeadamente no que respeita às categorias de dados em causa e ao período de conservação, de acordo com um regime diferenciado em função do objetivo prosseguido e estritamente necessário para atingir esse objetivo, que o critério da proporcionalidade poderá ser satisfeito.

56. Também não desenvolverei no âmbito das presentes conclusões o conceito de «conservação limitada dos dados», examinado em pormenor pelo advogado-geral M. Campos Sánchez-Bordona nas Conclusões que apresentou em 15 de janeiro de 2020 no âmbito do processo C-520/18, Ordre des barreaux francophones et germanophone e o. [28].

### *B. Quanto ao acesso das autoridades nacionais competentes aos dados conservados*

#### *1. Ensinamentos retirados do Acórdão Tele2 Sverige e Watson e o.*

57. O Tribunal de Justiça aborda a problemática relativa ao acesso das autoridades nacionais competentes aos dados conservados «independentemente do âmbito da obrigação de conservação de dados imposta aos prestadores de serviços de comunicações eletrónicas» e, em particular, independentemente do caráter generalizado ou circunscrito de uma conservação de dados [29]. Esta conclusão está relacionada com o facto de o Tribunal de Justiça considerar que a conservação dos dados e o acesso aos mesmos são duas ingerências distintas nos direitos fundamentais protegidos pela Carta.

58. O acesso aos dados conservados «deve responder efetiva e estritamente a um [dos] objetivos» que figuram no artigo 15.º, n.º 1, da Diretiva 2002/58. Deve igualmente existir uma concordância entre a gravidade da ingerência e o objetivo prosseguido. Se a ingerência for qualificada de «grave», só pode ser justificada pela luta contra a criminalidade grave [30].

27 Acórdão Tele2 Sverige e Watson e o. (n.º 112).

28 C-520/18, EU:C:2020:7. V., em particular, n.ºs 72 a 107 dessas conclusões.

29 V. Acórdão Tele2 Sverige e Watson e o. (n.º 113).

30 V. Acórdão Tele2 Sverige e Watson e o. (n.º 115).

59. À semelhança do que é válida para a conservação dos dados, o acesso a estes pelas autoridades competentes só pode ser autorizado dentro dos limites do estritamente necessário [31]. Além disso, as medidas legislativas devem «prever normas claras e precisas que indiquem em que circunstâncias e em que condições os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes acesso aos dados. Do mesmo modo, uma medida desta natureza deve também ser vinculativa em direito interno» [32]. Mais precisamente, as regulamentações nacionais devem «prever as condições materiais e processuais que regulam o acesso das autoridades nacionais competentes aos dados conservados» [33].

60. Pode deduzir-se do que precede que «um acesso generalizado a todos os dados conservados, independentemente de uma qualquer relação, no mínimo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário» [34].

61. Segundo o Tribunal de Justiça, «a regulamentação nacional em causa deve basear-se em critérios objetivos para definir as circunstâncias e as condições nas quais deve ser concedido às autoridades nacionais competentes o acesso aos dados dos assinantes ou dos utilizadores registados. A este respeito, só poderá, em princípio, ser concedido acesso, em relação com o objetivo da luta contra a criminalidade, aos dados de pessoas suspeitas de terem planeado, de estarem a cometer ou de terem cometido uma infração grave ou ainda de estarem envolvidas de uma maneira ou de outra numa infração deste tipo» [35].

62. Por outras palavras, a regulamentação nacional que atribui às autoridades nacionais competentes o acesso aos dados conservados deve ter um alcance suficientemente delimitado para impedir que esse acesso seja suscetível de incidir sobre um número significativo de pessoas, ou mesmo sobre todas as pessoas e todos os meios de comunicação eletrónica bem como sobre a totalidade dos dados conservados. Por conseguinte, o Tribunal de Justiça destacou o critério do nexo entre as pessoas em causa e o objetivo prosseguido.

63. Por outro lado, o Tribunal de Justiça estabeleceu as condições a que deve obedecer qualquer acesso das autoridades nacionais competentes aos dados conservados.

64. Antes de mais, esse acesso deve «em princípio, salvo em casos de urgência devidamente justificados, [ser] sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente» [36]. A decisão desse órgão jurisdicional ou dessa entidade deve ocorrer «na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal» [37].

65. Em seguida, importa, segundo o Tribunal de Justiça, que «as autoridades nacionais competentes às quais foi concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível comprometer as investigações levadas a cabo por essas autoridades» [38].

31 V. Acórdão Tele2 Sverige e Watson e o. (n.º 116).

32 Acórdão Tele2 Sverige e Watson e o. (n.º 117).

33 Acórdão Tele2 Sverige e Watson e o. (n.º 118).

34 Acórdão Tele2 Sverige e Watson e o. (n.º 119).

35 *Idem.*

36 Acórdão Tele2 Sverige e Watson e o. (n.º 120).

37 *Idem.*

38 Acórdão Tele2 Sverige e Watson e o. (n.º 121).

66. Por último, os Estados-Membros devem adotar regras destinadas à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas, a fim de evitar abusos bem como qualquer acesso ilícito aos dados [39].

*2. Ensinamentos retirados do Acórdão Ministerio Fiscal*

67. Neste processo, tinha sido submetida ao Tribunal de Justiça a questão da compatibilidade com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º e 8.º da Carta, de uma regulamentação nacional que previa o acesso das autoridades nacionais competentes, como a Polícia Judiciária, a dados relativos à identidade civil dos titulares de determinados cartões SIM.

68. No seu acórdão, o Tribunal de Justiça salientou que, no que diz respeito ao objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais, a redação do artigo 15.º, n.º 1, primeira frase, da Diretiva 2002/58 não limita este objetivo à luta contra as infrações graves, mas visa as «infrações penais» em geral [40].

69. O raciocínio desenvolvido pelo Tribunal de Justiça esclarece que, no que respeita ao acesso aos dados pelas autoridades nacionais competentes, deve existir uma correspondência entre a gravidade da ingerência e a gravidade das infrações em causa.

70. Assim, o Tribunal de Justiça recorda, referindo-se ao n.º 99 do seu Acórdão Tele2 Sverige e Watson e o., que é certo que declarou que, «em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, apenas a luta contra a criminalidade grave é suscetível de justificar um acesso das autoridades públicas a dados pessoais conservados pelos fornecedores de serviços de comunicações que, considerados no seu conjunto, permitem tirar conclusões precisas sobre a vida privada das pessoas cujos dados estão em causa» [41].

71. No entanto, o Tribunal de Justiça precisa que «fundamentou esta interpretação com o facto de que o objetivo prosseguido por esta regulamentação deve estar relacionado com a gravidade da ingerência nos direitos fundamentais que esse acesso gera» [42].

72. Com efeito, «em conformidade com o princípio da proporcionalidade, uma ingerência grave só pode ser justificada, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, por um objetivo de luta contra a criminalidade, devendo também esta ser qualificada de "grave"» [43].

73. Em contrapartida, «quando a ingerência que esse acesso implica não for grave, o referido acesso é suscetível de ser justificado por um objetivo de prevenção, de investigação, de deteção e de repressão de "infrações penais" em geral» [44].

39 V. Acórdão Tele2 Sverige e Watson e o. (n.º 122).

40 V. Acórdão Ministerio Fiscal (n.º 53).

41 Acórdão Ministerio Fiscal (n.º 54).

42 Acórdão Ministerio Fiscal (n.º 55).

43 Acórdão Ministerio Fiscal (n.º 56).

44 Acórdão Ministerio Fiscal (n.º 57).

74. Estas considerações exigiam, portanto, uma apreciação da questão de saber se, à luz das circunstâncias do caso concreto, a ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que um acesso da Polícia Judiciária aos dados em causa no processo principal teria implicado devia ou não ser considerada «grave».

75. Ora, ao contrário do que se passava no seu Acórdão Tele2 Sverige e Watson e o., a ingerência nos direitos protegidos pelos artigos 7.º e 8.º da Carta que constituía o acesso aos dados em causa, não foi qualificada de «grave» pelo Tribunal de Justiça [45]. Com efeito, o pedido de acesso tinha «por único objetivo identificar os titulares dos cartões SIM ativados durante um período de 12 dias, com o código [de identidade internacional de equipamento móvel] do telemóvel roubado» [46]. Tratava-se apenas do acesso «aos números de telefone correspondentes a esses cartões SIM e aos dados relativos à identidade civil dos titulares dos referidos cartões, tais como o apelido, o nome próprio e, sendo caso disso, o endereço. No entanto, esses dados não [tinham] por objeto […] as comunicações efetuadas com o telemóvel roubado nem a sua localização» [47].

76. O Tribunal de Justiça deduziu daí que «os dados visados pelo pedido de acesso em causa no processo principal permitem apenas associar, durante um determinado período, o cartão ou os cartões SIM ativados no telemóvel roubado à identidade civil dos titulares desses cartões SIM. Sem um cruzamento com os dados relativos às comunicações efetuadas com os referidos cartões SIM e os dados de localização, esses dados não permitem conhecer a data, a hora, a duração e os destinatários das comunicações efetuadas com o ou os cartões SIM em causa, nem os locais onde essas comunicações tiveram lugar ou a frequência destas com determinadas pessoas durante um dado período. Os referidos dados não permitem, assim, tirar conclusões precisas a respeito da vida privada das pessoas cujos dados estão em causa» [48].

77. Uma vez afastada a qualificação de «ingerência grave», o Tribunal de Justiça pôde considerar que o objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral, ainda que não graves, podia ser invocado para justificar a ingerência em causa [49].

78. É à luz desta jurisprudência que o órgão jurisdicional de reenvio submete a sua primeira e segunda questões prejudiciais, com o objetivo de apreciar a gravidade da ingerência que constitui o acesso aos dados no âmbito do processo penal em causa no processo principal. Mais precisamente, pretende saber se as categorias de dados em causa e a duração do período relativamente ao qual o acesso a esses dados é solicitado constituem, nesta perspetiva, critérios pertinentes.

### *3. Quanto aos critérios que permitem avaliar a gravidade da ingerência*

79. Como resulta da jurisprudência do Tribunal de Justiça, quanto mais numerosas forem as categorias de dados aos quais é pedido acesso, maior é a probabilidade de a ingerência ser qualificada de «grave».

[45] Acórdão Ministerio Fiscal (n.º 61).

[46] Acórdão Ministerio Fiscal (n.º 59).

[47] *Idem.*

[48] Acórdão Ministerio Fiscal (n.º 60).

[49] Acórdão Ministerio Fiscal (n.º 62).

80. No entanto, a primeira e segunda questões submetidas pelo órgão jurisdicional de reenvio levarão o Tribunal de Justiça a precisar se, para além das categorias de dados em causa, a extensão do período abrangido por este acesso desempenha também um papel na determinação da gravidade da ingerência.

81. Na minha opinião, a resposta deve ser afirmativa. Observo, de resto, que, no seu Acórdão Ministerio Fiscal, o Tribunal de Justiça teve igualmente em conta a duração do período abrangido pelo acesso no âmbito da sua apreciação, a saber, nesse caso, de doze dias [50].

82. É a conjugação entre a natureza dos dados em causa e a duração do período abrangido pelo acesso que permite apreciar a gravidade da ingerência. Com efeito, estes dois aspetos permitem verificar se o critério determinante da gravidade da ingerência está preenchido, ou seja, se o acesso aos dados em causa é suscetível de permitir às autoridades nacionais competentes tirar conclusões precisas sobre a vida privada das pessoas cujos dados são afetados por esse acesso. Ora, para poder traçar o retrato preciso de uma pessoa, é necessário não só que o acesso se refira a várias categorias de dados, como os dados de identificação, de tráfego e de localização, mas também que esse acesso incida sobre um período suficientemente longo para poder revelar com suficiente precisão os traços principais da vida de uma pessoa.

83. À semelhança do número de categorias em causa, a duração do período relativamente ao qual são exigidos dados em conformidade com uma autorização de acesso constitui, portanto, um elemento essencial para apreciar a gravidade da ingerência nos direitos fundamentais das pessoas em causa. Como a Comissão indica, o cúmulo de vários pedidos de acesso relativos a uma única e mesma pessoa deve igualmente ser tomado em consideração, ainda que incidam sobre períodos curtos.

84. Como resulta do pedido de decisão prejudicial, os dados a que a autoridade encarregada do inquérito teve acesso são os referidos no artigo 111[1], n.º 2, da Lei relativa às Comunicações Eletrónicas. Estes dados permitem encontrar e identificar a origem e o destino de uma comunicação telefónica a partir do telefone fixo ou móvel de uma pessoa, determinar a respetiva data, hora, duração e natureza, identificar o material de comunicação utilizado bem como localizar o material de comunicação móvel utilizado. Estes dados foram transmitidos à autoridade encarregada do inquérito relativamente a períodos de um dia, de um mês e de quase um ano.

85. A apreciação do grau de ingerência nos direitos fundamentais que implica o acesso das autoridades nacionais competentes aos dados pessoais conservados resulta de um exame concreto das circunstâncias próprias de cada caso. Em cada situação, incumbe ao órgão jurisdicional de reenvio apreciar se os dados aos quais foi autorizado o acesso eram suscetíveis de permitir, em função da sua natureza e da duração do período abrangido por esse acesso, tirar conclusões precisas sobre a vida privada das pessoas em causa.

86. Se assim for, a ingerência deve ser qualificada de «grave», na aceção da jurisprudência do Tribunal de Justiça e só pode, portanto, ser justificada, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, por um objetivo de luta contra a criminalidade, que deve igualmente ser qualificada de «grave» [51].

[50] V. Acórdão Ministerio Fiscal (n.º 59). V., no mesmo sentido, Conclusões do advogado-geral H. Saugmandsgaard Øe no processo Ministerio Fiscal (C-207/16, EU:C:2018:300), que observa que o pedido das autoridades policiais dizia respeito «a um período claramente definido e limitado no tempo, ou seja, doze dias» (n.º 33 bem como n.º 84).

[51] Acórdão Ministerio Fiscal (n.º 56).

*4. Quanto à concordância entre a gravidade da ingerência e o objetivo prosseguido*

87. Resulta da jurisprudência do Tribunal de Justiça que uma ingerência nos direitos fundamentais que seja qualificada de «grave» implica uma exigência de justificação reforçada.

88. No que diz respeito à gravidade das infrações penais presumidas a respeito das quais foi concedido o acesso aos dados, a Comissão observa que a regulamentação nacional em causa no processo principal autoriza, nomeadamente, o acesso para lutar contra as infrações penais em geral [52].

89. Incumbe ao órgão jurisdicional de reenvio verificar, em função das circunstâncias do caso em apreço, se o acesso a dados como os que estão em causa no processo principal responde efetiva e estritamente a um dos objetivos previstos no artigo 15.º, n.º 1, da Diretiva 2002/58. Importa recordar, a este respeito, que esta disposição não limita o objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais apenas à luta contra as infrações graves, mas visa as «infrações penais» em geral [53].

90. Se o órgão jurisdicional de reenvio chegar à conclusão de que a ingerência deve ser qualificada de «grave», cabe-lhe apreciar se a infração em causa pode igualmente ser qualificada de «grave», segundo o direito penal nacional.

91. A este respeito, considero que a definição do que pode ser qualificado de «infração grave» deve ser deixada à apreciação dos Estados-Membros.

92. Com efeito, consoante os sistemas jurídicos nacionais, a mesma infração pode ser punida com maior ou menor severidade. A definição das circunstâncias agravantes pode igualmente variar consoante os Estados-Membros.

93. Como o Governo estónio salienta com razão, a pena aplicável não é o único critério para determinar a gravidade das infrações. É igualmente necessário tomar em conta a natureza das infrações, os danos que causam à sociedade, a violação dos interesses jurídicos e os efeitos globais que têm sobre a ordem jurídica nacional bem como sobre os valores de uma sociedade democrática. O contexto histórico, económico e social específico de cada Estado-Membro desempenha também um papel a este respeito. Por outro lado, no que respeita às circunstâncias agravantes, há que procurar saber se as infrações penais foram cometidas, por exemplo, de forma repetida, ou contra um grupo de pessoas vulneráveis.

94. A fim de avaliar a proporcionalidade do acesso, há que ter igualmente em conta que, em conformidade com o artigo 90[1], n.º 3, do Código de Processo Penal, «[o]s pedidos de fornecimento de dados […] só podem ser feitos se forem absolutamente necessários para se atingir o objetivo do processo penal». Como o Governo estónio indica, o critério da absoluta necessidade [54] obriga tanto os investigadores como as pessoas incumbidas de emitir a autorização a considerar e a apreciar quais os dados necessários para levar a bom termo o processo penal e sem os quais não seria possível, no âmbito de um dado processo, trabalhar para apurar a verdade ou deter um presumido delinquente ou criminoso.

[52] Artigo 111[1], n.º 11, da Lei relativa às Comunicações Eletrónicas e artigo 90[1] do Código de Processo Penal.

[53] V. Acórdão Ministerio Fiscal (n.º 53).

[54] Igualmente designado «princípio da *ultima ratio*».

95. Acrescento que, como o Governo francês sublinhou, com razão, o grau de gravidade de uma infração, ou mesmo a sua exata qualificação jurídica, nem sempre podem ser determinados de forma precisa quando a autorização de acesso a dados conservados ocorre numa fase precoce do inquérito, pelo que poderia afigurar-se prematuro, nessa fase, inserir tal infração na categoria das infrações penais graves ou na das infrações penais em geral. Esta incerteza, que é inerente aos inquéritos penais que têm precisamente como objeto contribuir para o apuramento da verdade, deve ser tomada em conta pelo órgão jurisdicional de reenvio na sua apreciação do caráter proporcionado do acesso.

96. Todavia, a incerteza que pode, assim, existir no início do inquérito penal sobre esses aspetos não pode eliminar a exigência de que cada pedido de acesso seja fundamentado pela necessidade de procurar provas relativas a um comportamento delituoso ou criminoso específico, com base numa suspeita sustentada por elementos objetivos. Assim, um pedido de acesso não pode ter como objetivo examinar, relativamente a um determinado período, todos os factos e atos de uma pessoa, com vista a detetar eventuais infrações. Por outro lado, se forem revelados novos factos durante o inquérito, o acesso aos dados para prova destes últimos deverá ser objeto de uma nova autorização de acesso.

97. Atendendo às considerações precedentes, sugiro ao Tribunal de Justiça que declare que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que, entre os critérios que permitem avaliar a gravidade da ingerência nos direitos fundamentais que constitui o acesso pelas autoridades nacionais competentes a dados pessoais que os fornecedores de serviços de comunicações eletrónicas são obrigados a conservar por força de uma regulamentação nacional, se encontram as categorias de dados em causa bem como a duração do período relativamente ao qual esse acesso é pedido. Incumbe ao órgão jurisdicional de reenvio apreciar, em função da gravidade da ingerência, se o referido acesso era estritamente necessário para atingir o objetivo que visa assegurar a prevenção, a investigação, a deteção e a repressão de infrações penais.

### *C. Controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente*

98. A fim de garantir que o acesso das autoridades nacionais competentes aos dados conservados seja limitado ao estritamente necessário para atingir o objetivo prosseguido, o Tribunal de Justiça considerou essencial que esse acesso «seja, em princípio, salvo em casos de urgência devidamente justificados, sujeito a um controlo prévio efetuado *por um órgão jurisdicional ou por uma entidade administrativa independente*, e que a decisão desse órgão jurisdicional ou dessa entidade ocorra na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal» [55].

99. Com a sua terceira questão prejudicial, o órgão jurisdicional de reenvio convida o Tribunal de Justiça a precisar os critérios que uma autoridade administrativa deve satisfazer para poder ser considerada «independente», na aceção do Acórdão Tele2 Sverige e Watson e o. Mais precisamente, o órgão jurisdicional de reenvio interroga-se sobre a questão de saber se o Ministério Público pode ser considerado uma autoridade administrativa independente, tendo em conta o facto de que dirige a fase de instrução e que representa a ação penal durante o processo.

[55] Acórdão Tele2 Sverige e Watson e o. (n.º 120 e jurisprudência referida), o sublinhado é meu. V., no mesmo sentido, Parecer 1/15 (Acordo PNR UE-Canadá) de 26 de julho de 2017 (EU:C:2017:592, n.ºs 202 e 208).

100. Para responder a esta questão, parece-me útil ter em conta duas vertentes da jurisprudência do Tribunal de Justiça, a saber, por um lado, a jurisprudência relativa à independência das autoridades nacionais de controlo da proteção de dados pessoais e, por outro, a jurisprudência relativa à independência da autoridade judiciária de emissão no âmbito do mandado de detenção europeu.

101. Segundo o Tribunal de Justiça, a independência constitui uma característica essencial, afirmada, designadamente, no artigo 8.º, n.º 3, da Carta, das autoridades encarregadas de fiscalizar o respeito das regras da União relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, com o objetivo de assegurar a eficácia e a fiabilidade desse controlo e de reforçar a proteção das pessoas abrangidas pelas decisões dessas autoridades [56].

102. O Tribunal de Justiça já declarou, a respeito do artigo 28.º, n.º 1, segundo parágrafo, da Diretiva 95/46, que «as autoridades de fiscalização competentes para a supervisão do tratamento de dados pessoais devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. Esta independência exclui, designadamente, qualquer instrução e qualquer outra influência externa, sob qualquer forma, seja direta ou indireta, suscetíveis de orientar as suas decisões e que podem assim pôr em causa o cumprimento, pelas referidas autoridades, da sua função de estabelecer um justo equilíbrio entre a proteção do direito à vida privada e a livre circulação dos dados de natureza pessoal» [57].

103. O Tribunal de Justiça destacou igualmente a exigência segundo a qual estas autoridades de fiscalização, tendo em conta o seu papel de guardiãs do direito à reserva da vida privada, devem estar «acima de qualquer suspeita de parcialidade» [58].

104. Na medida em que a terceira questão submetida pelo órgão jurisdicional de reenvio diz respeito ao Ministério Público, é igualmente pertinente ter em conta os critérios formulados pelo Tribunal de Justiça na sua jurisprudência relativa à independência da autoridade judiciária de emissão no âmbito do mandado de detenção europeu. Assim, segundo o Tribunal de Justiça, o controlo efetuado aquando da adoção de um mandado de detenção «deve ser exercido com objetividade, tendo em conta todos os elementos incriminatórios e ilibatórios, e independência, o que pressupõe a existência de regras estatutárias e organizativas adequadas a excluir qualquer risco de a adoção de uma decisão de emitir tal mandado de detenção estar sujeita a instruções externas, nomeadamente por parte do poder executivo» [59]. Importa, no entanto, ter presente que a apreciação concreta, pelo Tribunal de Justiça, em cada caso, da questão de saber se o Ministério Público preenche ou não todos os critérios [60].

105. As duas vertentes da jurisprudência do Tribunal de Justiça coincidem, portanto, ao sublinhar, em cada um dos domínios em causa, que a autoridade nacional competente para verificar o respeito das regras do direito da União deve revestir caráter independente, o que

[56] V., nomeadamente, Acórdão de 6 de outubro de 2015, Schrems (C-362/14, EU:C:2015:650, n.ºs 40 e 41 e jurisprudência referida). V., igualmente, Parecer 1/15 (Acordo PNR UE-Canadá) de 26 de julho de 2017 (EU:C:2017:592, n.º 229).

[57] Acórdão de 8 de abril de 2014, Comissão/Hungria (C-288/12, EU:C:2014:237, n.º 51 e jurisprudência referida).

[58] Acórdão de 8 de abril de 2014, Comissão/Hungria (C-288/12, EU:C:2014:237, n.º 53 e jurisprudência referida).

[59] V. Acórdão de 9 de outubro de 2019, NJ (Procuradoria de Viena) (C-489/19 PPU, EU:C:2019:849, n.º 38 e jurisprudência referida).

[60] V., por último, Acórdão de 12 de dezembro de 2019, JR e YC (Procuradores de Lyon e Tours e Procuradores de Lyon e de Tours) (C-566/19 PPU e C-626/19 PPU, EU:C:2019:1077), no qual, o Tribunal de Justiça considerou, designadamente, que os elementos que lhe foram apresentados eram suficientes para demonstrar que, em França, «os magistrados da Procuradoria dispõem do poder de apreciar de maneira independente, designadamente em relação ao poder executivo, a necessidade e o caráter proporcionado da emissão de um mandado de detenção europeu e que exercem esse poder de modo objetivo, tendo em conta todos os elementos inculpatórios e exculpatórios.

comporta duas exigências [61]. Por um lado, essa autoridade não deve estar sujeita a instruções ou pressões externas suscetíveis de influenciar as suas decisões. Por outro lado, a referida autoridade deve, por força do seu estatuto e das missões que lhe são conferidas, satisfazer uma exigência de objetividade ao proceder ao seu controlo, ou seja, deve oferecer garantias de imparcialidade. Mais especificamente, a apreciação por uma autoridade administrativa do caráter proporcionado do acesso aos dados conservados exige que esta possa alcançar um justo equilíbrio entre os interesses associados à eficácia do inquérito no âmbito da luta contra a criminalidade e os que respeitam à proteção dos dados pessoais das pessoas afetadas pelo acesso. Quanto a este último aspeto, a exigência de imparcialidade é, portanto, inerente ao conceito de «autoridade administrativa independente» destacado pelo Tribunal de Justiça no seu Acórdão Tele2 Sverige e Watson e o.

106. Há que verificar se o Ministério Público, tendo em conta as diferentes missões que lhe são confiadas pela regulamentação estónia, satisfaz este critério de independência, em ambas as suas dimensões, quando é chamado a controlar o caráter estritamente necessário do acesso aos dados. Assim, o conceito de «independência» que deve caracterizar a autoridade administrativa encarregada desse controlo reveste uma dimensão funcional, no sentido de que é tendo em conta o objeto específico deste controlo que se deve apreciar se essa autoridade pode assegurar o referido controlo sem intervenções nem pressões externas suscetíveis de influenciar as suas decisões, respeitando a objetividade e a estrita aplicação da regra de direito. Em suma, o conceito de «autoridade administrativa independente», na aceção do Acórdão Tele2 Sverige e Watson e o., destina-se a garantir a objetividade, a fiabilidade e a eficácia desse controlo.

107. Tal implica que se examine se a regulamentação estónia que precisa o estatuto e as missões do Ministério Público é suscetível de criar dúvidas legítimas, no espírito das pessoas em causa, quanto à impermeabilidade dos procuradores em relação a elementos externos e à sua neutralidade relativamente aos interesses em confronto, quando são chamados a assegurar o controlo prévio do caráter proporcionado do acesso aos dados.

108. O Ministério Público desempenha um papel essencial na tramitação do processo penal, uma vez que dirige a fase de instrução e que tem, nomeadamente, competência para instaurar uma ação penal contra uma pessoa suspeita de ter cometido uma infração penal, para que seja demandada num órgão jurisdicional. Nesta medida, deve ser considerado uma autoridade que participa na administração da justiça penal [62].

109. Como o Tribunal de Justiça referiu a propósito da Procura della Repubblica (Procurador da República, Itália) e segundo uma fórmula que me parece poder ser transposta para o âmbito do presente processo, «a função [do procurador] não é resolver com total independência um litígio, mas submetê-lo, se for caso disso, ao órgão jurisdicional competente, enquanto parte no processo em que se exerce a ação penal» [63].

110. Embora o Ministério Público apresente assim, no seu estatuto, na sua organização e nas suas missões, traços particulares que o distinguem de um órgão jurisdicional e que justificam que seja qualificado como «autoridade que participa na administração da justiça penal nos

[61] Quanto aos dois aspetos da exigência de independência, v., por analogia, a propósito dos órgãos jurisdicionais nacionais que são chamados a pronunciar-se sobre questões relacionadas com a interpretação e a aplicação do direito da União, Acórdão de 5 de novembro de 2019, Comissão/Polónia (Independência dos órgãos jurisdicionais de direito comum) (C-192/18, EU:C:2019:924, n.os 108 a 110 e jurisprudência referida).

[62] V., nomeadamente, Acórdão de 27 de maio de 2019, PF (Procurador-Geral da Lituânia) (C-509/18, EU:C:2019:457, n.os 39 e 40).

[63] Acórdão de 12 de dezembro de 1996, X (C-74/95 e C-129/95, EU:C:1996:491, n.º 19).

Estados-Membros», não deixa de ser verdade que, do ponto de vista funcional, quando o direito nacional prevê que a autoridade que exerce o controlo prévio da proporcionalidade do acesso que é exigido pelo Acórdão Tele2 Sverige e Watson e o. é o Ministério Público, este último deve, quanto a este aspeto, manifestar um grau de independência análogo ao de um órgão jurisdicional. Com efeito, o exercício desta função por uma autoridade administrativa, e não por um órgão jurisdicional, não deve afetar a objetividade, a fiabilidade e a eficácia desse controlo.

111. A este respeito, há que recordar que, em conformidade com o artigo 90[1], n.º 2, do Código de Processo Penal, a autoridade encarregada do inquérito pode, mediante autorização do Ministério Público durante a fase de instrução ou mediante autorização do tribunal no decurso do processo que lhe foi submetido, pedir a uma empresa de comunicações eletrónicas que forneça os dados enumerados no artigo 111[1], n.os 2 e 3, da Lei relativa às Comunicações Eletrónicas.

112. Por outro lado, resulta da regulamentação estónia que o Ministério Público, no âmbito de um processo penal, dirige a fase de instrução, cujo objetivo é a recolha de elementos de prova e a criação das outras condições necessárias a um processo judicial. Além disso, a autoridade encarregada do inquérito e o Ministério Público verificam, durante a fase de instrução, os elementos incriminadores e os elementos desculpantes recolhidos contra o suspeito ou o acusado. Se o Ministério Público estiver convencido de que foram recolhidas todas as provas necessárias e se houver motivos para o fazer, o Ministério Público apresenta a acusação contra a pessoa em causa e, nesse caso, é ele que representa a ação penal no processo.

113. O órgão jurisdicional de reenvio observa igualmente que, embora, no âmbito do processo penal, o Ministério Público deva, quanto às medidas que constituem as mais graves ingerências nos direitos fundamentais, pedir uma autorização a um magistrado instrutor (por exemplo, para a maioria das medidas de vigilância e para a detenção), o Ministério Público tem igualmente competência para decidir da adoção de atos processuais que constituem uma ingerência significativa em vários direitos fundamentais [64].

114. As dúvidas manifestadas pelo órgão jurisdicional de reenvio quanto à qualificação do Ministério Público como «autoridade administrativa independente», na aceção do Acórdão Tele2 Sverige e Watson e o., são principalmente devidas ao facto de que, após a fase de instrução, se o Ministério Público estiver convencido de que, no processo penal, foram recolhidas todas as provas necessárias e se houver motivos para o fazer, é ao Ministério Público que compete apresentar a acusação contra a pessoa em causa. Nesse caso, é o Ministério Público que representa a ação penal no processo e é, portanto, igualmente parte no processo. Assim, é principalmente devido à sua qualidade de parte responsável pela acusação que a qualificação do Ministério Público como «autoridade administrativa independente», na aceção do Acórdão Tele2 Sverige e Watson e o., é questionada pelo órgão jurisdicional de reenvio.

115. Expressas deste modo, as dúvidas manifestadas pelo órgão jurisdicional de reenvio respeitam, portanto, mais especificamente à imparcialidade do Ministério Público no controlo da proporcionalidade do acesso aos dados pelos serviços de inquérito a que deve proceder antes de autorizar esse acesso.

[64] Por exemplo, o Ministério Público emite uma autorização com vista à vigilância discreta de uma pessoa, de uma coisa ou de um local, bem como, em muitos casos, para efeitos de uma busca.

116. Antes de abordar este aspeto relativo à imparcialidade, saliento que o artigo 1.º, n.º 1[1], da Lei relativa ao Ministério Público dispõe que este último «cumpre de forma independente as missões que lhe incumbem por força da lei». Além disso, por força do artigo 2.º, n.º 2, desta mesma lei, «[o] procurador cumpre as suas missões de forma independente e age unicamente nos termos da lei e segundo a sua convicção» [65].

117. A este respeito, o Governo estónio indica que, embora o Ministério Público seja uma autoridade que faz parte do Ministério da Justiça, a regulamentação estónia recusa, todavia, a este último qualquer possibilidade de formular uma apreciação sobre um processo específico ou de intervir num processo penal em curso. Este governo precisa que a violação da independência do Ministério Público constituiria uma infração punível.

118. Embora não haja, portanto, motivos para duvidar da independência do Ministério Público no âmbito das missões que lhe incumbem por força da regulamentação estónia, parece-me, contudo, que esta é suscetível de gerar dúvidas legítimas quanto à aptidão do Ministério Público para exercer um controlo prévio neutro e objetivo sobre o caráter proporcionado do acesso aos dados quando pode ser chamado, no âmbito de um dado processo, a exercer simultaneamente as missões que consistem em dirigir o inquérito penal, a decidir do exercício da ação penal e a representar a ação pública durante o processo.

119. É certo que vários elementos que constam da regulamentação estónia constituem garantias de que o Ministério Público, no âmbito das missões que assume, age respeitando a exigência de imparcialidade.

120. Assim, nos termos do artigo 211.º, n.º 2, do Código de Processo Penal, o Ministério Público deve verificar os elementos inculpatórios e os elementos exculpatórios recolhidos contra o suspeito ou o acusado.

121. Por outro lado, como resulta do artigo 1.º, n.º 1, da Lei relativa ao Ministério Público, este é obrigado a garantir a legalidade da fase de instrução penal que lhe incumbe dirigir. Além disso, nos termos do artigo 1.º, n.º 1[1], e do artigo 2.º, n.º 2, desta mesma lei, o Ministério Público deve exercer as suas funções respeitando as leis. Isto pressupõe que o Ministério Público, quando dirige a fase de instrução penal, deve ter como objetivo não só assegurar a eficácia desta última, como também garantir que essa fase de instrução não seja conduzida de modo a causar um prejuízo desproporcionado ao direito à vida privada das pessoas em causa. Com efeito, pode considerar-se que a autorização de acesso aos dados conservados faz parte integrante da missão mais geral do Ministério Público, que consiste em fiscalizar a legalidade dos meios utilizados pelos serviços de inquérito, em especial a proporcionalidade dos atos de investigação à luz da natureza e da gravidade dos factos.

122. Poderia, portanto, invocar-se o argumento de que é justamente por dirigir a fase de instrução que o Ministério Público está em condições de avaliar se, à luz das especificidades de cada processo, é estritamente necessário um acesso a dados conservados pelos operadores de telecomunicações, na falta de elementos de prova alternativos, a fim de dar seguimento ao inquérito sobre uma infração presumida.

[65] V., igualmente, no mesmo sentido, artigo 30.º, n.º 2, do Código de Processo Penal.

123. Todavia, do ponto de vista das pessoas afetadas pelo pedido de acesso aos dados, a circunstância de a autoridade administrativa que deve verificar se esse acesso é estritamente necessário no âmbito do inquérito ser simultaneamente a que é suscetível de exercer a ação penal e, em seguida, de representar a ação pública num eventual processo subsequente pode, na minha opinião, ser suscetível de enfraquecer as garantias de imparcialidade previstas pela regulamentação estónia. Deste ponto de vista, pode existir um conflito potencial entre, por um lado, estas missões do Ministério Público e, por outro, a exigência de neutralidade e de objetividade do controlo prévio do caráter proporcionado do acesso aos dados.

124. Com efeito, no âmbito das suas missões, o Ministério Público é obrigado a recolher as provas, a apreciar a sua pertinência e a retirar conclusões quanto à culpabilidade da pessoa em causa. Incumbe a esta autoridade do Estado apresentar e fundamentar a acusação no âmbito da ação pública que está encarregada de representar no processo, sendo, portanto, uma parte no processo. Devido a estas missões, o Ministério Público está sujeito a uma exigência probatória que, aos olhos das pessoas suspeitas de terem cometido uma infração, pode afigurar-se incompatível com a capacidade dessa mesma autoridade para efetuar, de forma neutra e objetiva, um controlo prévio do caráter proporcionado do acesso aos dados.

125. Como salienta a Comissão, poderia haver o risco de, em razão do cúmulo das missões que lhe incumbem, o Ministério Público poder ser visto pelas pessoas em causa como tendo interesse em permitir amplo acesso aos seus dados, sejam eles incriminadores ou desculpantes. Além disso, as pessoas suspeitas de terem cometido uma infração podem ter dúvidas legítimas sobre a imparcialidade do Ministério Público quando este autoriza o acesso aos seus dados, uma vez que pode agir contra elas em processos subsequentes, na qualidade de parte responsável pela acusação. Ora, considero que a exigência de imparcialidade da autoridade administrativa que é encarregada de proceder ao controlo prévio exigido pelo Acórdão Tele2 Sverige e Watson e o. pressupõe uma certa distância e uma neutralidade relativamente aos interesses que são suscetíveis de se confrontar no âmbito da fase de instrução, a saber, por um lado, a eficácia desta última e, por outro, a proteção dos dados pessoais das pessoas em causa. Segundo a Comissão, a situação poderia ser diferente se a organização administrativa interna do Ministério Público fosse tal que o procurador que deve pronunciar-se sobre o pedido de acesso não desempenhasse qualquer papel na fase de instrução e nas etapas subsequentes do processo, incluindo a ação penal pública.

126. Na medida em que, como foi confirmado na audiência, a procuradoria está organizada de forma hierárquica na República da Estónia, não estou certo que esta sugestão da Comissão possa sanar os inconvenientes decorrentes do cúmulo das missões de que a regulamentação estónia encarrega o Ministério Público. Em qualquer caso, tal não prejudica a pertinência da ideia subjacente a esta sugestão, a saber, a de que o controlo prévio do caráter proporcionado do acesso aos dados deve ser efetuado por uma autoridade administrativa que, por um lado, não esteja diretamente implicada na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal. Essa autoridade, separada dos interesses ligados ao inquérito e à ação penal no processo em questão, não poderia ser acusada de privilegiar os interesses do inquérito em detrimento dos relativos à proteção dos dados das pessoas em causa. A referida autoridade poderia então adotar, com toda a imparcialidade, uma decisão que limitasse o acesso aos dados conservados ao estritamente necessário para alcançar o objetivo prosseguido, em conformidade com o que é exigido pelo artigo 15.º, n.º 1, da Diretiva 2002/58, conforme interpretado pelo Tribunal de Justiça nos Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o.[66] e Tele2 Sverige e Watson e o. Simultaneamente, tenho perfeita

[66] C-293/12 e C-594/12, EU:C:2014:238.

consciência de que a instituição de uma apreciação externa aos interesses associados ao processo em causa não ser feita à custa de uma redução da eficácia da investigação e da repressão das infrações penais.

127. A fim de respeitar a autonomia processual dos Estados-Membros, o Tribunal de Justiça não deve interferir mais na organização geral da administração da justiça nos Estados-Membros, nem na organização interna das procuradorias. Incumbe aos Estados-Membros criar os instrumentos adequados para garantir que o controlo prévio do acesso aos dados conservados assegura um justo equilíbrio entre os interesses relacionados com a eficácia do inquérito penal e o direito à proteção dos dados das pessoas afetadas por esse acesso.

128. Por fim, esclareço que, na minha opinião, a falta de um controlo prévio efetuado por uma autoridade administrativa «independente», na aceção do Acórdão Tele2 Sverige e Watson e o., não pode ser compensada pela existência de um controlo jurisdicional que possa ser efetuado depois de o acesso ter sido autorizado [67]. Caso contrário, a exigência do caráter prévio do controlo perderia a sua razão de ser, que consiste em impedir que seja autorizado um acesso aos dados conservados que seria desproporcionado relativamente ao objetivo de investigar, punir e reprimir as infrações penais.

129. À luz das considerações precedentes, sugiro ao Tribunal de Justiça que responda à terceira questão prejudicial que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º e do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que a exigência segundo a qual o acesso das autoridades nacionais competentes aos dados conservados deve ser submetido a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente não é respeitada quando uma regulamentação nacional prevê que esse controlo seja efetuado pelo Ministério Público, que tem por missão dirigir a fase de instrução e é, simultaneamente, suscetível de representar a ação penal no processo.

## V. Conclusão

130. À luz do que precede, proponho ao Tribunal de Justiça que responda às questões submetidas pelo Riigikohus (Supremo Tribunal, Estónia) do seguinte modo:

1) O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que, entre os critérios que permitem avaliar a gravidade da ingerência nos direitos fundamentais que constitui o acesso pelas autoridades nacionais competentes a dados pessoais que os fornecedores de serviços de comunicações eletrónicas são obrigados a conservar por força de uma regulamentação nacional, se encontram as categorias de dados em causa bem como a duração do período relativamente ao qual esse

[67] Segundo os elementos que foram apresentados ao Tribunal de Justiça na audiência, no direito estónio, este controlo jurisdicional pode ser efetuado no final da fase de instrução, quando um suspeito, tendo acesso aos autos, decida impugnar um ato da fase de instrução, ou durante o processo.

acesso é pedido. Incumbe ao órgão jurisdicional de reenvio apreciar, em função da gravidade da ingerência, se o referido acesso era estritamente necessário para atingir o objetivo que visa assegurar a prevenção, a investigação, a deteção e a repressão de infrações penais.

2) O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que a exigência segundo a qual o acesso das autoridades nacionais competentes aos dados conservados deve ser submetido a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente não é respeitada quando uma regulamentação nacional prevê que esse controlo seja efetuado pelo Ministério Público, que tem por missão dirigir a fase de instrução e é, simultaneamente, suscetível de representar a ação penal no processo.