



## Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

2 de outubro de 2018\*

«Reenvio prejudicial — Comunicações eletrónicas — Tratamento dos dados pessoais — Diretiva 2002/58/CE — Artigos 1.º e 3.º — Âmbito de aplicação — Confidencialidade das comunicações eletrónicas — Proteção — Artigos 5.º e 15.º, n.º 1 — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.º e 8.º — Dados tratados no âmbito do fornecimento de serviços de comunicações eletrónicas — Acesso das autoridades nacionais aos dados para fins de investigação — Limiar de gravidade da infração suscetível de justificar o acesso aos dados»

No processo C-207/16,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pela Audiencia Provincial de Tarragona (Audiência Provincial de Tarragona, Espanha), por decisão de 6 de abril de 2016, que deu entrada no Tribunal de Justiça em 14 de abril de 2016, no processo intentado por

**Ministerio Fiscal,**

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: K. Lenaerts, presidente, A. Tizzano, vice-presidente, R. Silva de Lapuerta, T. von Danwitz (relator), J. L. da Cruz Vilaça, C. G. Fernlund e C. Vajda, presidentes de secção, E. Juhász, A. Borg Barthet, C. Toader, M. Safjan, D. Šváby, M. Berger, E. Jarašiūnas e E. Regan, juízes,

advogado-geral: H. Saugmandsgaard Øe,

secretário: L. Carrasco Marco, administradora,

vistos os autos e após a audiência de 29 de janeiro de 2018,

vistas as observações apresentadas:

- em representação do Ministerio Fiscal, por E. Tejada de la Fuente,
- em representação do Governo espanhol, por M. Sampol Pucurull, na qualidade de agente,
- em representação do Governo checo, por M. Smolek, J. Vláčil e A. Brabcová, na qualidade de agentes,
- em representação do Governo dinamarquês, por J. Nymann-Lindegren e M. Wolff, na qualidade de agentes,
- em representação do Governo estónio, por N. Grünberg, na qualidade de agente,

\* Língua do processo: espanhol.

- em representação da Irlanda, por M. Browne, L. Williams, E. Creedon e A. Joyce, na qualidade de agentes, assistidos por E. Gibson, BL,
- em representação do Governo francês, por D. Colas, E. de Moustier e E. Armoet, na qualidade de agentes,
- em representação do Governo letão, por I. Kucina e J. Davidoviča, na qualidade de agentes,
- em representação do Governo húngaro, por M. Fehér e G. Koós, na qualidade de agentes,
- em representação do Governo austríaco, por C. Pesendorfer, na qualidade de agente,
- em representação do Governo polaco, por B. Majczyna, D. Lutostańska e J. Sawicka, na qualidade de agentes,
- em representação do Governo do Reino Unido, por S. Brandon e C. Brodie, na qualidade de agentes, assistidos por C. Knight, barrister, e G. Facenna, QC,
- em representação da Comissão Europeia, por I. Martínez del Peral, P. Costa de Oliveira, R. Troosters e D. Nardi, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 3 de maio de 2018,

profere o presente

### **Acórdão**

- 1 O pedido de decisão prejudicial tem por objeto, em substância, a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 201, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO 2009, L 337, p. 11) (a seguir «Diretiva 2002/58»), lido à luz dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).
- 2 Este pedido foi apresentado no âmbito de um recurso interposto pelo Ministerio Fiscal (Ministério Público, Espanha) da decisão do Juzgado de Instrucción n.º 3 de Tarragona (Tribunal de Instrução n.º 3 de Tarragona, a seguir «juiz de instrução») sobre a recusa em autorizar o acesso da Polícia Judiciária a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas.

### **Quadro jurídico**

#### ***Direito da União***

##### *Diretiva 95/46*

- 3 Nos termos do artigo 2.º, alínea b), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31), há que, para efeitos desta última, considerar «tratamento de dados pessoais», «qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo,

organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição».

4 O artigo 3.º desta diretiva, sob a epígrafe «Âmbito de aplicação», prevê:

«1. A presente diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.

2. A presente diretiva não se aplica ao tratamento de dados pessoais:

- efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal,
- efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.»

*Diretiva 2002/58*

5 Os considerandos 2, 11, 15 e 21 da Diretiva 2002/58 enunciam:

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

[...]

(11) Tal como a Diretiva [95/46], a presente diretiva não trata questões relativas à proteção dos direitos e liberdades fundamentais relacionadas com atividades não reguladas pelo direito comunitário. Portanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.º 1 do artigo 15.º da presente diretiva, necessários para a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal. Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se for caso disso, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais.

[...]

(15) Uma comunicação pode incluir qualquer informação relativa a nomes, números ou endereços fornecida pelo remetente de uma comunicação ou pelo utilizador de uma ligação para efetuar a comunicação. Os dados de tráfego podem incluir qualquer tradução desta informação pela rede através da qual a comunicação é transmitida, para efeitos de execução da transmissão. [...]

[...]

(21) Devem ser tomadas medidas para impedir o acesso não autorizado às comunicações efetuadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis, a fim de proteger a confidencialidade do seu conteúdo e de quaisquer dados com elas relacionados. A legislação nacional de alguns Estados-Membros apenas proíbe o acesso intencional não autorizado às comunicações.»

6 O artigo 1.º da Diretiva 2002/58, sob a epígrafe «Âmbito e objetivos», dispõe:

«1. A presente diretiva prevê a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na Comunidade.

2. Para os efeitos do n.º 1, as disposições da presente diretiva especificam e complementam a Diretiva [95/46]. Além disso, estas disposições asseguram a proteção dos legítimos interesses dos assinantes que são pessoas coletivas.

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

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

São também aplicáveis as seguintes definições:

[...]

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

c) “Dados de localização” são quaisquer dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas publicamente disponível;

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

[...]»

- 8 O artigo 3.º da Diretiva 2002/58, sob a epígrafe «Serviços abrangidos», prevê:

«A presente diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na Comunidade, nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação;»

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

«1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.º 1 do artigo 15.º [...]

[...]

3. Os Estados-Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Diretiva [95/46], nomeadamente sobre os objetivos do processamento. [...]

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

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

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

[...]»

- 11 O artigo 15.º da referida diretiva, sob a epígrafe «Aplicação de determinadas disposições da Diretiva [95/46]», prevê, no seu n.º 1:

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

## *Direito espanhol*

### *Lei 25/2007*

- 12 O artigo 1.º da Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (Lei n.º 25/2007 relativa à conservação de dados relativos a comunicações eletrónicas e a redes públicas de comunicações), de 18 de outubro de 2007 (BOE n.º 251, de 19 de outubro de 2007, p. 42517), dispõe:

«1. A presente lei tem por objeto regular a obrigação dos operadores de conservarem os dados gerados ou tratados no contexto da prestação de serviços de comunicações eletrónicas ou de redes públicas de comunicações, bem como a obrigação de comunicar esses dados às autoridades, sempre que lhes seja solicitado através da necessária autorização judicial, para efeitos de deteção, de inquérito e de julgamento de crimes graves previstos no Código Penal ou nas leis penais especiais.

2. A presente lei é aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares quer a pessoas coletivas, bem como aos dados conexos necessários para identificar o assinante ou o utilizador registado.

[...]»

### *Código Penal*

- 13 O artigo 13.º, n.º 1, da Ley Orgánica 10/1995 del Código Penal (Código Penal), de 23 de novembro de 1995 (BOE n.º 281, de 24 de novembro de 1995, p. 33987), tem a seguinte redação:

«Constituem crimes graves as infrações que a lei pune com pena grave.»

- 14 O artigo 33.º do referido código prevê:

«1. Em função da sua natureza e da sua duração, as penas são classificadas como graves, menos graves e leves.

2. São penas graves:

- a) A pena de prisão perpétua, passível de revisão.
- b) A pena de prisão por um período superior a cinco anos.

[...]»

### *Código de Processo Penal*

- 15 Depois da data dos factos do processo principal, a Ley de Enjuiciamiento Criminal (Código de Processo Penal) foi alterada pela Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (Lei Orgânica n.º 13/2015, que altera o Código de Processo Penal com vista ao reforço das garantias processuais e à regulamentação das medidas de investigação tecnológica), de 5 de outubro de 2015 (BOE n.º 239, de 6 de outubro de 2015, p. 90192, a seguir «Código de Processo Penal, na sua versão resultante da Lei Orgânica n.º 13/2015»)

16 Esta lei entrou em vigor em 6 de dezembro de 2015. A referida lei incorpora no Código de Processo Penal o domínio do acesso aos dados relativos às comunicações telefónicas e telemáticas que foram conservados pelos fornecedores de serviços de comunicações eletrónicas.

17 O artigo 579.º, n.º 1, do Código de Processo Penal, na sua versão resultante da Lei Orgânica n.º 13/2015, dispõe:

«1. O juiz pode autorizar a interceção da correspondência privada, postal e telegráfica, incluindo *fax*, *buofax* e de vales postais internacionais, que o suspeito envie ou receba, bem como a sua abertura e análise, se existirem indícios de que, através destes meios, será descoberto ou comprovado um facto ou uma circunstância pertinente para o processo, quando o inquérito tenha por objeto uma das seguintes infrações:

- 1) Crimes dolosos puníveis com uma pena máxima de prisão não inferior a três anos.
- 2) Crimes cometidos no âmbito de um grupo ou organização criminosa.
- 3) Crimes terroristas.

[...]»

18 O artigo 588.º-B, alínea j), do referido código prevê:

«1. Os dados eletrónicos conservados pelos prestadores de serviços ou pelas pessoas que fornecem a comunicação em aplicação da legislação sobre a conservação de dados relativos às comunicações eletrónicas, ou por sua própria iniciativa por motivos comerciais ou outros, e que estejam ligadas a processos de comunicação, só poderão ser comunicados, a fim de poderem ser tomados em consideração no âmbito do processo, mediante autorização judicial.

2. Sempre que o conhecimento desses dados se revelar indispensável para o inquérito, deverá pedir se ao juiz competente autorização para aceder às informações que se encontram nos arquivos automatizados dos prestadores de serviços, em especial para uma investigação cruzada ou inteligente de dados, devendo ser especificada a natureza dos dados de que é necessário tomar conhecimento e as razões que justificam a sua apresentação.»

### **Tramitação no processo principal e questões prejudiciais**

19 Hernandez Sierra apresentou na Polícia queixa por roubo, cometido em 16 de fevereiro de 2015, no decurso do qual foi ferido e lhe roubaram a carteira e o telemóvel.

20 Em 27 de fevereiro de 2015, a Polícia Judiciária apresentou ao juiz de instrução um pedido solicitando que fosse ordenado a diferentes fornecedores de serviços de comunicações eletrónicas que transmitissem os números de telefone ativados, entre 16 de fevereiro e 27 de fevereiro de 2015, com o código relativo à Identidade Internacional de Equipamento Móvel (a seguir «código IMEI») do telemóvel roubado, bem como os dados pessoais relativos à identidade civil dos titulares ou dos utilizadores dos números de telefone correspondentes aos cartões SIM ativados com esse código, tais como o seu apelido, nome próprio e, sendo caso disso, o endereço.

21 Por despacho de 5 de maio de 2015, o juiz de instrução indeferiu esse pedido. Por um lado, declarou que a medida exigida não era útil para efeitos da identificação dos autores da infração. Por outro lado, recusou acolher o pedido com o fundamento de que a Lei n.º 25/2007 limitava a transmissão dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas às infrações graves. Em

conformidade com o Código Penal, as infrações graves são punidas com penas privativas de liberdade superiores a 5 anos, enquanto os factos em causa no processo principal não parecem ser constitutivos dessa infração.

- 22 O Ministério Público interpôs recurso deste despacho para o órgão jurisdicional de reenvio, por considerar que a comunicação dos dados em causa devia ter sido concedida em razão da natureza dos factos e por força de um Acórdão do Tribunal Supremo (Supremo Tribunal, Espanha), de 26 de julho de 2010, sobre um caso semelhante.
- 23 O órgão jurisdicional de reenvio considera que, posteriormente ao referido despacho, o legislador espanhol alterou o Código de Processo Penal através da adoção da Lei Orgânica n.º 13/2015. Esta lei, que é pertinente para a resolução do recurso no processo principal, introduziu dois novos critérios alternativos para determinar o grau de gravidade de uma infração. Trata-se, por um lado, de um critério material identificado por comportamentos que correspondem a qualificações penais cuja natureza criminal é específica e grave, e que são particularmente ofensivos dos interesses jurídicos individuais e coletivos. Por outro lado, o legislador nacional recorreu a um critério normativo formal, baseado na pena prevista para a infração em causa. O limiar de três anos de prisão aí previsto abrange, contudo, a grande maioria das infrações. Além disso, o órgão jurisdicional de reenvio considera que o interesse do Estado em reprimir os comportamentos infratores não pode justificar ingerências desproporcionadas nos direitos fundamentais consagrados na Carta.
- 24 A este respeito, o referido órgão jurisdicional considera que, no processo principal, as Diretivas 95/46 e 2002/58 estabelecem onexo de conexão com a Carta. A regulamentação nacional em causa no processo principal está abrangida, por conseguinte, em conformidade com o artigo 51.º, n.º 1, da Carta, pelo seu âmbito de aplicação, apesar de a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO 2006, L 105, p. 54), ter sido declarada inválida pelo Acórdão de 8 de abril de 2014, *Digital Rights Ireland e o.* (C-293/12 e C-594/12, EU:C:2014:238).
- 25 Neste acórdão, o Tribunal de Justiça reconheceu que a conservação e a comunicação de dados relativos ao tráfego constituem ingerências particularmente graves nos direitos garantidos pelos artigos 7.º e 8.º da Carta e identificou os critérios de apreciação do respeito pelo princípio da proporcionalidade, cuja gravidade das infrações justifica a conservação e o acesso a esses dados para efeitos de investigação.
- 26 Foi nestas circunstâncias que a Audiencia Provincial de Tarragona (Audiência Provincial de Tarragona) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:
- «1) Pode a suficiente gravidade dos crimes, enquanto critério que justifica a ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, ser determinada tendo em consideração unicamente a pena suscetível de ser aplicada ao crime investigado ou, além disso, é necessário identificar na conduta infratora especiais níveis de lesão de bens jurídicos individuais e/ou coletivos?
- 2) No caso de ser conforme aos princípios constitucionais da União, aplicados pelo TJUE no seu Acórdão de 8 de abril de 2014 [processos apensos C-293/12, *Digital Rights Ireland e C-594/12, Seitlinger e o.*, EU:C:2014:238] como critérios de fiscalização estrita da Diretiva 2002/58, a determinação da gravidade do crime atendendo apenas à pena suscetível de ser aplicada, qual deve ser o limiar mínimo desta? Seria compatível com uma norma geral que estabeleça como limite os três anos de prisão?»

## Tramitação do processo no Tribunal de Justiça

- 27 Por decisão do Presidente do Tribunal de Justiça, de 23 de maio de 2016, foi suspenso o processo no Tribunal de Justiça até à prolação do Acórdão nos processos apensos Tele2 Sverige e Watson e o., C-203/15 e C-698/15 (Acórdão de 21 de dezembro de 2016, EU:C:2016:970, a seguir «Acórdão Tele2 Sverige e Watson e o.»). Na sequência da prolação deste acórdão, o órgão jurisdicional de reenvio foi interrogado quanto à questão de saber se desejava manter ou retirar o seu pedido de decisão prejudicial. Em resposta, o órgão jurisdicional de reenvio, por carta de 30 de janeiro de 2017, que deu entrada no Tribunal de Justiça em 14 de fevereiro de 2017, fez saber que considerava que este acórdão não lhe permitia apreciar, com suficiente certeza, a regulamentação nacional em causa no processo principal à luz do direito da União. Por conseguinte, o processo no Tribunal de Justiça foi reatado em 16 de fevereiro de 2017.

## Quanto às questões prejudiciais

- 28 O Governo espanhol alega, por um lado, a incompetência do Tribunal de Justiça para responder ao pedido de decisão prejudicial e, por outro, a inadmissibilidade deste pedido.

## Quanto à competência do Tribunal de Justiça

- 29 Nas suas observações escritas apresentadas ao Tribunal de Justiça, o Governo espanhol manifestou a opinião, à qual aderiu o Governo do Reino Unido na audiência, de que o Tribunal de Justiça não é competente para responder ao pedido de decisão prejudicial com o fundamento de que o processo principal está, em conformidade com o artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46 e o artigo 1.º, n.º 3, da Diretiva 2002/58, excluído do âmbito de aplicação destas duas diretivas. Por conseguinte, este processo não está abrangido pelo âmbito de aplicação do direito da União, pelo que a Carta, em conformidade com o seu artigo 51.º, n.º 1, não é aplicável.
- 30 Segundo o Governo espanhol, é verdade que o Tribunal de Justiça declarou, no Acórdão Tele2 Sverige e Watson e o., que uma medida legislativa que regula o acesso das autoridades nacionais aos dados conservados pelos fornecedores de serviços de comunicações eletrónicas está abrangida pelo âmbito de aplicação da Diretiva 2002/58. No entanto, no caso em apreço, trata-se de um pedido de acesso de uma autoridade pública, ao abrigo de uma decisão judicial no âmbito de um processo de instrução penal, a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas. O Governo espanhol conclui que este pedido de acesso se inscreve no exercício, pelas autoridades nacionais, do *ius puniendi*, de forma que constitui uma atividade do Estado relativa a domínios do direito penal abrangidos pela exceção prevista no artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46 e no artigo 1.º, n.º 3, da Diretiva 2002/58.
- 31 Para apreciar esta exceção de incompetência, importa salientar que o artigo 1.º da Diretiva 2002/58 dispõe, no seu n.º 1, que esta diretiva prevê a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas. Em conformidade com o seu artigo 1.º, n.º 2, a referida diretiva específica e complementa a Diretiva 95/46 para os efeitos enunciados no seu n.º 1.
- 32 O artigo 1.º, n.º 3, da Diretiva 2002/58 exclui do seu âmbito de aplicação as «atividades do Estado» nos domínios aí referidos, entre as quais figuram as atividades do Estado no domínio penal e as 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 (Acórdão Tele2 Sverige e Watson e o., n.º 69 e jurisprudência referida). As atividades aí referidas a título de exemplo serão, em qualquer caso, atividades próprias dos Estados ou das autoridades

estatais, alheias aos domínios de atividade dos particulares (v., por analogia, no que respeita ao artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, Acórdão de 10 de julho de 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, n.º 38 e jurisprudência referida).

- 33 Quanto ao artigo 3.º da Diretiva 2002/58, este enuncia que esta diretiva é aplicável ao tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na União, incluindo as redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação (a seguir «serviços de comunicações eletrónicas»). Por conseguinte, deve considerar-se que a referida diretiva regula as atividades dos fornecedores de tais serviços (Acórdão Tele2 Sverige e Watson e o., n.º 70).
- 34 No que diz respeito ao artigo 15.º, n.º 1, da Diretiva 2002/58, o Tribunal de Justiça já declarou que as medidas legislativas referidas nesta disposição 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. Com efeito, 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 (v., neste sentido, Acórdão Tele2 Sverige e Watson e o., n.ºs 72 a 74).
- 35 O Tribunal de Justiça conclui 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 (v., neste sentido, Acórdão Tele2 Sverige e Watson e o., n.ºs 75 e 76).
- 36 Com efeito, 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 (Acórdão Tele2 Sverige e Watson e o., n.º 77).
- 37 Há que acrescentar 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 (v., neste sentido, Acórdão Tele2 Sverige e Watson e o., n.ºs 75 e 78). 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.
- 38 No presente caso, como resulta da decisão de reenvio, o pedido em causa no processo principal, através do qual a Polícia Judiciária solicita uma autorização judicial para aceder a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas, baseia-se na Lei n.º 25/2007, lida em conjugação com o Código de Processo Penal, na sua versão aplicável aos factos no processo principal, que regula o acesso das autoridades públicas a esses dados. A referida regulamentação é suscetível de permitir à Polícia Judiciária, em caso de concessão da autorização judicial solicitada com fundamento nesta, exigir aos fornecedores de serviços de comunicações eletrónicas que coloquem à sua disposição dados pessoais e que, deste modo, tendo em conta a definição que figura no artigo 2.º,

alínea b), da Diretiva 95/46, aplicável no contexto da Diretiva 2002/58 por força do artigo 2.º, primeiro travessão, desta última, procedam a um «tratamento» desses dados, na aceção das duas diretivas. A referida regulamentação regula, assim, as atividades dos fornecedores de serviços de comunicações eletrónicas e está abrangida, por conseguinte, pelo âmbito de aplicação da Diretiva 2002/58.

- 39 Nestas condições, a circunstância invocada pelo Governo espanhol, segundo a qual este pedido de acesso é apresentado no âmbito de um processo de instrução penal, não pode tornar a Diretiva 2002/58 inaplicável ao processo principal, por força do seu artigo 1.º, n.º 3.
- 40 A este respeito, é igualmente irrelevante que o pedido de acesso em causa no processo principal vise, como decorre da resposta escrita do Governo espanhol a uma pergunta feita pelo Tribunal de Justiça, e como confirmaram tanto esse Governo como o Ministério Público na audiência, permitir o acesso unicamente aos números de telefone correspondentes aos cartões SIM ativados com o código IMEI do telemóvel roubado e aos dados relativos à identidade civil dos titulares desses cartões, tais como o seu apelido, o nome próprio e, sendo caso disso, o endereço, excluindo os dados relativos às comunicações efetuadas com os referidos cartões SIM e os dados de localização relativos ao telemóvel roubado.
- 41 Com efeito, como salientou o advogado-geral no n.º 54 das suas conclusões, a Diretiva 2002/58 regula, por força do seu artigo 1.º, n.º 1, e do seu artigo 3.º, qualquer tratamento de dados pessoais no âmbito do fornecimento de serviços de comunicações eletrónicas. Além disso, em conformidade com o artigo 2.º, segundo parágrafo, alínea b), desta diretiva, o conceito de «Dados de tráfego» abrange «quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma».
- 42 Quanto a este último aspeto, no que diz respeito mais especificamente a dados relativos à identidade civil dos titulares dos cartões SIM, resulta do considerando 15 da Diretiva 2002/58 que os dados de tráfego podem, nomeadamente, incluir o nome e o endereço do remetente de uma comunicação ou pelo utilizador de uma ligação para efetuar uma comunicação. Os dados relativos à identidade civil dos titulares de cartões SIM podem, além disso, ser necessários para a faturação dos serviços de comunicações eletrónicas fornecidos e fazem, por conseguinte, parte dos dados de tráfego, conforme definidos no artigo 2.º, segundo parágrafo, alínea b), desta diretiva. Consequentemente, esses dados estão abrangidos pelo âmbito de aplicação da Diretiva 2002/58.
- 43 O Tribunal de Justiça é, por isso, competente para responder à questão submetida pelo órgão jurisdicional de reenvio.

### *Quanto à admissibilidade*

- 44 O Governo espanhol afirma que o pedido de decisão prejudicial é inadmissível uma vez que não identifica claramente as disposições do direito da União sobre as quais o Tribunal de Justiça foi chamado a pronunciar-se. Além do mais, o pedido da Polícia Judiciária em causa no processo principal tem por objeto, não a interceção das comunicações efetuadas através dos cartões SIM ativados com o código IMEI do telemóvel roubado, mas uma relação entre esses cartões e os seus titulares, pelo que a confidencialidade das comunicações não é afetada. O artigo 7.º da Carta, referido pelas questões prejudiciais, é, desta forma, irrelevante no contexto do presente processo.
- 45 Em conformidade com jurisprudência constante do Tribunal de Justiça, compete exclusivamente ao juiz nacional, a quem foi submetido o litígio e que deve assumir a responsabilidade pela decisão jurisdicional a tomar, apreciar, tendo em conta as especificidades do processo, tanto a necessidade de uma decisão prejudicial para poder proferir a sua decisão como a pertinência das questões que submete ao Tribunal de Justiça. Consequentemente, desde que as questões submetidas sejam relativas à interpretação do direito da União, o Tribunal de Justiça é, em princípio, obrigado a pronunciar-se. O

Tribunal de Justiça só pode recusar pronunciar-se sobre uma questão prejudicial submetida por um órgão jurisdicional nacional quando for manifesto que a interpretação do direito da União solicitada não tem nenhuma relação com a realidade ou com o objeto do litígio no processo principal, quando o problema for hipotético ou ainda quando o Tribunal não dispuser dos elementos de facto e de direito necessários para dar uma resposta útil às questões que lhe são submetidas (Acórdão de 10 de julho de 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, n.º 31 e jurisprudência referida).

- 46 No caso em apreço, a decisão de reenvio contém elementos de facto e de direito suficientes tanto para a identificação das disposições do direito da União referidas pelas questões prejudiciais como para a compreensão do alcance dessas questões. Em particular, resulta da decisão de reenvio que as questões prejudiciais visam permitir ao órgão jurisdicional de reenvio apreciar a questão de saber se e em que medida a regulamentação nacional, na qual é baseado o pedido da Polícia Judiciária em causa no processo principal, prossegue um objetivo que é suscetível de justificar uma violação dos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta. Ora, segundo as indicações desse órgão jurisdicional de reenvio, esta regulamentação nacional está abrangida pelo âmbito de aplicação da Diretiva 2002/58, pelo que a Carta é aplicável ao processo principal. As questões prejudiciais apresentam assim uma relação direta com o objeto do processo principal e não podem, por conseguinte, ser consideradas hipotéticas.
- 47 Nestas circunstâncias, as questões prejudiciais são admissíveis.

#### *Quanto ao mérito*

- 48 Com as suas duas questões, que importa examinar em conjunto, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º e 8.º da Carta, deve ser interpretado no sentido de que o acesso das autoridades públicas aos dados com vista à identificação dos titulares dos cartões SIM ativados num telemóvel roubado, tais como o apelido, o nome próprio e, sendo caso disso, o endereço desses titulares, constitui uma ingerência nos direitos fundamentais destes últimos, consagrados nesses artigos da Carta, que apresenta uma gravidade tal que esse acesso deva ser limitado, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, à luta contra a criminalidade grave e, em caso afirmativo, com base em que critérios se deve apreciar a gravidade da infração em causa.
- 49 A este respeito, resulta da decisão de reenvio que, como salientou, em substância, o advogado-geral no n.º 38 das suas conclusões, o pedido de decisão prejudicial não visa determinar se os dados pessoais em causa no processo principal foram conservados pelos fornecedores de serviços de comunicações eletrónicas no respeito pelas condições referidas no artigo 15.º, n.º 1, da Diretiva 2002/58, lido em conjugação com os artigos 7.º e 8.º da Carta. Este pedido tem por objeto, como resulta do n.º 46 do presente acórdão, apenas a questão de saber se e em que medida o objetivo prosseguido pela regulamentação em causa no processo principal é suscetível de justificar o acesso das autoridades públicas, como a Polícia Judiciária, a esses dados, sem que as restantes condições de acesso resultantes deste artigo 15.º, n.º 1, sejam objeto desse pedido.
- 50 Em particular, este órgão jurisdicional interroga-se sobre os elementos a ter em conta para apreciar se as infrações em relação às quais as autoridades policiais podem ser autorizadas, para efeitos da investigação, a aceder a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas, são de gravidade suficiente para justificar a ingerência que esse acesso implica nos direitos fundamentais garantidos nos artigos 7.º e 8.º da Carta, conforme interpretados pelo Tribunal de Justiça nos seus Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238), e Tele2 Sverige e Watson e o.

- 51 Quanto à existência de uma ingerência nesses direitos fundamentais, há que recordar que, como salientou o advogado-geral nos n.ºs 76 e 77 das suas conclusões, o acesso das autoridades públicas a esses dados é constitutivo de uma ingerência no direito fundamental ao respeito da vida privada, consagrado no artigo 7.º da Carta, mesmo na falta de circunstâncias que permitam qualificar esta ingerência como «grave» e sem que seja relevante se as informações relativas à vida privada em questão sejam ou não sensíveis, ou se os interessados tenham ou não sofrido eventuais inconvenientes em razão dessa ingerência. Esse acesso constitui igualmente uma ingerência no direito fundamental à proteção dos dados pessoais, garantido pelo artigo 8.º da Carta, uma vez que constitui um tratamento de dados pessoais [v., neste sentido, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.ºs 124 e 126 e jurisprudência referida].
- 52 No que se refere aos objetivos suscetíveis de justificar uma regulamentação nacional como a que está em causa no processo principal, que regula o acesso das autoridades públicas aos dados conservados pelos fornecedores de serviços de comunicações eletrónicas e que derroga, assim, o princípio da confidencialidade das comunicações eletrónicas, há que recordar que a enumeração dos objetivos que figuram no artigo 15.º, n.º 1, primeira frase, da Diretiva 2002/58 reveste um caráter exaustivo, pelo que este acesso deve responder efetiva e estritamente a um desses objetivos (v., neste sentido, Acórdão Tele2 Sverige e Watson e o., n.ºs 90 e 115).
- 53 Ora, no que diz respeito ao objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais, há que observar que 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.
- 54 A este respeito, é certo que o Tribunal de Justiça 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 (v., neste sentido, Acórdão Tele2 Sverige e Watson e o., n.º 99).
- 55 No entanto, o Tribunal de Justiça 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 (v., neste sentido, Acórdão Tele2 Sverige e Watson e o., n.º 115).
- 56 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».
- 57 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.
- 58 Por conseguinte, antes de mais, há que determinar se, no presente processo, em função 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 implica deve ser considerada como sendo «grave».
- 59 A este respeito, o pedido em causa no processo principal, pelo qual a Polícia Judiciária solicita, para efeitos de uma investigação penal, a autorização judicial para aceder a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas, tem por único objetivo identificar os titulares dos cartões SIM ativados durante um período de 12 dias, com o código IMEI do telemóvel roubado. Como foi salientado no n.º 40 do presente acórdão, este pedido visa apenas o 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 têm por objeto, como confirmaram o Governo espanhol e o Ministério Público na audiência, as comunicações efetuadas com o telemóvel roubado nem a sua localização.

- 60 Desta forma, é evidente 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.
- 61 Nestas condições, o acesso apenas aos dados visados pelo pedido em causa no processo principal não pode ser qualificado de ingerência «grave» nos direitos fundamentais das pessoas cujos dados estão em causa.
- 62 Como resulta dos n.ºs 53 a 57 do presente acórdão, a ingerência que implica um acesso a esses dados é, por conseguinte, suscetível de ser justificada pelo objetivo de prevenção, de investigação, de deteção e de repressão de «infrações penais» em geral, ao qual se refere o artigo 15.º, n.º 1, primeira frase, da Diretiva 2002/58, sem que seja necessário que essas infrações sejam qualificadas de «graves».
- 63 Tendo em conta as considerações precedentes, há que responder às questões submetidas que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º e 8.º da Carta, deve ser interpretado no sentido de que o acesso das autoridades públicas aos dados com vista à identificação dos titulares dos cartões SIM ativados num telemóvel roubado, tais como o apelido, o nome próprio e, sendo caso disso, o endereço desses titulares, constitui uma ingerência nos direitos fundamentais destes últimos, consagrados nesses artigos da Carta, que não apresenta uma gravidade tal que esse acesso deva ser limitado, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, à luta contra a criminalidade grave.

### Quanto às despesas

- 64 Revestindo o processo, quanto às partes na causa principal, a natureza de incidente suscitado perante o órgão jurisdicional de reenvio, compete a este decidir quanto às despesas. As despesas efetuadas pelas outras partes para a apresentação de observações ao Tribunal de Justiça não são reembolsáveis.

Pelos fundamentos expostos, o Tribunal de Justiça (Grande Secção) declara:

**O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que o acesso das autoridades públicas aos dados com vista à identificação dos titulares dos cartões SIM ativados num telemóvel roubado, tais como o apelido, o nome próprio e, sendo caso disso, o endereço desses titulares, constitui uma ingerência nos direitos fundamentais destes últimos, consagrados nesses artigos da Carta, que não apresenta uma gravidade tal que esse acesso deva ser limitado, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, à luta contra a criminalidade grave.**

## Assinaturas