Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

6 de outubro de 2020*

«Reenvio prejudicial — Tratamento de dados pessoais no sector das comunicações eletrónicas — Prestadores de serviços de comunicações eletrónicas — Transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização — Salvaguarda da segurança nacional — Diretiva 2002/58/CE — Âmbito de aplicação — Artigo 1.º, n.º 3, e artigo 3.º — Confidencialidade das comunicações eletrónicas — Proteção — Artigo 5.º e artigo 15.º, n.º 1 — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.º, 8.º, 11.º e 52.º, n.º 1 — Artigo 4.º, n.º 2, TUE»

No processo C-623/17,

que tem por objeto um pedido de decisão prejudicial nos termos do artigo 267.º TFUE, apresentado pelo Investigatory Powers Tribunal (Tribunal de Instrução, Reino Unido), por Decisão de 18 de outubro de 2017, que deu entrada no Tribunal de Justiça em 31 de outubro de 2017, no processo

**Privacy International**

contra

**Secretary of State for Foreign and Commonwealth Affairs,**

**Secretary of State for the Home Department,**

**Government Communications Headquarters,**

**Security Service,**

**Secret Intelligence Service,**

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: K. Lenaerts, presidente, R. Silva de Lapuerta, vice-presidente, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P. G. Xuereb e L. S. Rossi, presidentes de secção, J. Malenovský, L. Bay Larsen, T. von Danwitz (relator), C. Toader, K. Jürimäe, C. Lycourgos e N. Piçarra, juízes,

advogado-geral: M. Campos Sánchez-Bordona,

secretário: C. Strömholm, administradora,

vistos os autos e após a audiência de 9 e 10 de setembro de 2019,

* Língua do processo: inglês.

vistas as observações apresentadas:

– em representação da Privacy International, por B. Jaffey e T. de la Mare, QC, por D. Cashman, solicitor, e por H. Roy, avocat,

– em representação do Governo do Reino Unido, por Z. Lavery, D. Guðmundsdóttir e S. Brandon, na qualidade de agentes, assistidos por G. Facenna e D. Beard, QC, e por C. Knight e R. Palmer, barristers,

– em representação do Governo belga, por P. Cottin e J.-C. Halleux, na qualidade de agentes, assistidos por J. Vanpraet, advocaat, e E. de Lophem, avocat,

– em representação do Governo checo, por M. Smolek, J. Vláčil e O. Serdula, na qualidade de agentes,

– em representação do Governo alemão, inicialmente por M. Hellmann, R. Kanitz, D. Klebs e T. Henze e, em seguida, por J. Möller, M. Hellmann, R. Kanitz e D. Klebs, na qualidade de agentes,

– em representação do Governo estónio, por A. Kalbus, na qualidade de agente,

– em representação do Governo irlandês, por M. Browne, G. Hodge e A. Joyce, na qualidade de agentes, assistidos por D. Fennelly, barrister,

– em representação do Governo espanhol, inicialmente por L. Aguilera Ruiz e J. García-Valdecasas Dorrego e, em seguida, por L. Aguilera Ruiz, na qualidade de agentes,

– em representação do Governo francês, inicialmente por E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas e D. Dubois e, em seguida, por E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune e D. Dubois, na qualidade de agentes,

– em representação do Governo cipriota, por E. Symeonidou e E. Neofytou, na qualidade de agentes,

– em representação do Governo letão, inicialmente por V. Soņeca e I. Kucina, em seguida por V. Soņeca, na qualidade de agentes,

– em representação do Governo húngaro, inicialmente por G. Koós, Z. Fehér, G. Tornyai e Z. Wagner e, em seguida, por G. Koós e Z. Fehér, na qualidade de agentes,

– em representação do Governo neerlandês, por C. S. Schillemans e K. Bulterman, na qualidade de agentes,

– em representação do Governo polaco, por B. Majczyna, J. Sawicka e M. Pawlicka, na qualidade de agentes,

– em representação do Governo português, por L. Inez, M. Figueiredo e F. Aragão Homem, na qualidade de agentes,

– em representação do Governo sueco, inicialmente por A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren e A. Alriksson e, em seguida, por H. Shev, C. Meyer-Seitz, L. Zettergren e A. Alriksson, na qualidade de agentes,

– em representação do Governo norueguês, por T. B. Leming, M. Emberland e J. Vangsnes, na qualidade de agentes,

– em representação da Comissão Europeia, inicialmente por H. Kranenborg, M. Wasmeier, D. Nardi e P. Costa de Oliveira e, em seguida, por H. Kranenborg, M. Wasmeier e D. Nardi, na qualidade de agentes,

– em representação da Autoridade Europeia para a Proteção de Dados, por T. Zerdick e A. Buchta, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 15 de janeiro de 2020,

profere o presente

## Acórdão

1 O pedido de decisão prejudicial tem por objeto a interpretação do artigo 1.º, n.º 3, e 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 sector 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»), lidos à luz do artigo 4.º, n.º 2, TUE, bem como dos artigos 7.º e 8.º e do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

2 Este pedido foi apresentado no âmbito de um litígio que opõe a Privacy International ao Secretary of State for Foreign and Commonwealth Affairs (Ministro dos Negócios Estrangeiros e da Commonwealth, Reino Unido), ao Secretary of State for the Home Departement (Ministro da Administração Interna, Reino Unido), ao Government Communications Headquarters (Sede de Comunicações do Governo, Reino Unido) (a seguir «GCHQ»), ao Security Service (Serviço de Segurança, Reino Unido, a seguir «MI5») e ao Secret Intelligence Service (Serviços Secretos de Informações, Reino Unido, a seguir «MI6»), relativo à legalidade de uma legislação que autoriza a aquisição e a utilização, pelos serviços de segurança e de informações, de dados de comunicações em massa (*bulk communications data*).

## Quadro jurídico

### *Direito da União*

*Diretiva 95/46*

3 A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31), foi revogada, com efeitos a contar de 25 de maio de 2018, pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (JO 2016, L 119, p. 1). O artigo 3.º da referida diretiva, sob a epígrafe «Âmbito de aplicação», tinha a seguinte redação:

«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 [TUE], 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*

4 Os considerandos 2, 6, 7, 11, 22, 26 e 30 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 da [mesma].

[…]

(6) A Internet está a derrubar as tradicionais estruturas do mercado, proporcionando uma infraestrutura mundial para o fornecimento de uma vasta gama de serviços de comunicações eletrónicas. Os serviços de comunicações eletrónicas publicamente disponíveis através da Internet abrem novas possibilidades aos utilizadores, mas suscitam igualmente novos riscos quanto aos seus dados pessoais e à sua privacidade.

(7) No caso das redes de comunicações públicas, é necessário estabelecer disposições legislativas, regulamentares e técnicas específicas para a proteção dos direitos e liberdades fundamentais das pessoas singulares e dos interesses legítimos das pessoas coletivas, em especial no que respeita à capacidade crescente em termos de armazenamento e de processamento informático de dados relativos a assinantes e utilizadores.

[…]

(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 [da União]. Portanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.º 1 do artigo 15.º da presente diretiva, necessários para a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal. Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, [assinada em Roma em 4 de novembro de 1950,] segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais.

[…]

(22) A proibição de armazenamento das comunicações e dos dados de tráfego a elas relativos por terceiros que não os utilizadores ou sem o seu consentimento não tem por objetivo proibir qualquer armazenamento automático, intermédio e transitório de informações, desde que esse armazenamento se efetue com o propósito exclusivo de realizar a transmissão através da rede de comunicação eletrónica e desde que as informações não sejam armazenadas por um período de tempo superior ao necessário para a transmissão e para fins de gestão de tráfego e que durante o período de armazenamento se encontre garantida a confidencialidade das informações. Sempre que tal se torne necessário para tornar mais eficiente o reenvio de informações acessíveis publicamente a outros destinatários do serviço, a seu pedido, a presente diretiva não deve impedir que as informações em causa possam continuar armazenadas, desde que as mesmas sejam, de qualquer modo, acessíveis ao público sem restrições e na condição de serem eliminados os dados relativos aos assinantes ou utilizadores que o solicitem.

[…]

(26) Os dados relativos aos assinantes tratados em redes de comunicações eletrónicas para estabelecer ligações e para transmitir informações contêm informações sobre a vida privada das pessoas singulares e incidem no direito ao sigilo da sua correspondência ou incidem nos legítimos interesses das pessoas coletivas. Esses dados apenas podem ser armazenados na medida do necessário para a prestação do serviço, para efeitos de faturação e de pagamentos de interligação, e por um período limitado. Qualquer outro tratamento desses dados […] só é permitido se o assinante tiver dado o seu acordo, com base nas informações exatas e completas que o prestador de serviços de comunicações eletrónicas publicamente disponíveis lhe tiver comunicado relativamente aos tipos de tratamento posterior que pretenda efetuar e sobre o direito do assinante de não dar ou retirar o seu consentimento a esse tratamento. Os dados de tráfego utilizados para comercialização de serviços de comunicações […]

[…]

(30) Os sistemas de fornecimento de redes e serviços de comunicações eletrónicas devem ser concebidos de modo a limitar ao mínimo o volume necessário de dados pessoais. […]»

5 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 sector das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na [União Europeia].

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 [TFUE], 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.»

6 Segundo o artigo 2.º desta diretiva, que tem por epígrafe «Definições»:

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

São também aplicáveis as seguintes definições:

a) "Utilizador": é qualquer pessoa singular que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

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

c) "Dados de localização": são quaisquer dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público;

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

[…]»

7 O artigo 3.º da referida diretiva, 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 [União], nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação.»

8 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 O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.

[…]

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

transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.»

9 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.

3. Para efeitos de comercialização dos serviços de comunicações eletrónicas ou para a prestação de serviços de valor acrescentado, o prestador de um serviço de comunicações eletrónicas acessível ao público pode tratar os dados referidos no n.º 1 na medida do necessário e pelo tempo necessário para a prestação desses serviços ou essa comercialização, se o assinante ou utilizador a quem os dados dizem respeito tiver dado o seu consentimento prévio. Deve ser dada a possibilidade aos utilizadores ou assinantes de retirarem a qualquer momento o seu consentimento para o tratamento dos dados de tráfego.

[…]

5. O tratamento de dados de tráfego, em conformidade com o disposto nos n.os 1 a 4, será limitado ao pessoal que trabalha para os fornecedores de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis encarregado da faturação ou da gestão do tráfego, das informações a clientes, da deteção de fraudes, da comercialização dos serviços de comunicações eletrónicas publicamente disponíveis, ou da prestação de um serviço de valor acrescentado, devendo ser limitado ao necessário para efeitos das referidas atividades.»

10 O artigo 9.º desta diretiva, sob a epígrafe «Dados de localização para além dos dados de tráfego», prevê, no seu n.º 1:

«Nos casos em que são processados dados de localização, para além dos dados de tráfego, relativos a utilizadores ou assinantes de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis, esses dados só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado. O prestador de serviços deve informar os utilizadores ou assinantes, antes de obter o seu consentimento, do tipo de dados de localização, para além dos dados de tráfego, que serão tratados, dos fins e duração do tratamento e da eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado. […]»

11 O artigo 15.º da referida diretiva, sob a epígrafe «Aplicação de determinadas disposições da Diretiva [95/46]», enuncia, 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 [da União], incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do Tratado da União Europeia.»

*Regulamento 2016/679*

12 O artigo 2.º do Regulamento 2016/679 dispõe:

«1. O presente regulamento 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 em ficheiros ou a eles destinados.

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

a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;

b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE;

[…]

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

[…]»

13 O artigo 4.º deste regulamento prevê:

«Para efeitos do presente regulamento, entende-se por:

[…]

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

[…]»

14 Nos termos do artigo 23.º, n.º 1, do mesmo regulamento:

«O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais

disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:

a) A segurança do Estado;

b) A defesa;

c) A segurança pública;

d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;

e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social;

f) A defesa da independência judiciária e dos processos judiciais;

g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas;

h) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas a) a e) e g);

i) A defesa do titular dos dados ou dos direitos e liberdades de outrem;

j) A execução de ações cíveis.»

15 Segundo o artigo 94.º, n.º 2, do Regulamento 2016/679:

«As remissões para a diretiva revogada são consideradas remissões para presente regulamento. As referências ao Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, criado pelo artigo 29.º da Diretiva [95/46], são consideradas referências ao Comité Europeu para a Proteção de Dados criado pelo presente regulamento.»

### *Direito do Reino Unido*

16 A section 94 do Telecommunications Act 1984, na sua versão aplicável aos factos em causa no processo principal (a seguir «Lei de 1984»), sob a epígrafe «Instruções no interesse da segurança nacional etc.», dispõe:

«(1) O ministro pode, após consultar uma pessoa a quem se aplique a presente section, dirigir a essa pessoa instruções de caráter geral, na medida em que considere que as mesmas são necessárias no interesse da segurança nacional ou das relações mantidas com o governo de um país ou território situado fora do Reino Unido.

(2) Sempre que o ministro considere necessário proceder de tal modo no interesse da segurança nacional ou das relações mantidas com o governo de um país ou território situado fora do Reino Unido, pode, após consultar uma pessoa a quem se aplique a presente section, dirigir instruções a essa pessoa, exigindo-lhe que (consoante as circunstâncias do caso concreto) execute, ou não, uma determinada ação especificada nas instruções.

(2A) O ministro apenas pode dirigir instruções ao abrigo do (1) ou do (2) se considerar que o comportamento exigido pelas instruções é proporcional ao objetivo a atingir através desse comportamento.

(3) A pessoa a quem se aplique o presente artigo deve dar cumprimento a todas as instruções que lhe sejam dirigidas pelo ministro ao abrigo do presente artigo, não obstante qualquer outra obrigação que lhe incumba por força da parte 1 ou da parte 2, capítulo 1, do Communications Act 2003 [Lei de 2003 das Comunicações] e, no caso de instruções dirigidas ao prestador de uma rede pública de comunicações eletrónicas, mesmo que as referidas instruções lhe sejam dirigidas a título de uma qualidade diferente da de prestador de acesso a tal rede.

(4) O ministro apresenta a cada uma das câmaras do Parlamento uma cópia de todas as instruções dirigidas nos termos do presente artigo, salvo se considerar que a divulgação das referidas instruções é contrária aos interesses da segurança nacional ou das relações mantidas com o governo de um país ou território situado fora do Reino Unido ou aos interesses comerciais de uma pessoa.

(5) Ninguém deve divulgar nem pode ser obrigado a divulgar, por força de lei ou de qualquer outra regulamentação, quaisquer informações relativas a medidas adotadas em conformidade com a presente section caso o ministro o tenha notificado de que considerava que a divulgação destas informações era contrária aos interesses da segurança nacional ou das relações mantidas com o governo de um país ou território situado fora do Reino Unido ou aos interesses comerciais de outra pessoa.

[…]

(8) A presente section é aplicável ao [Instituto das Comunicações (OFCOM)] e aos prestadores de redes públicas de comunicações eletrónicas.»

17 A section 21(4) e (6), do Regulation of Investigatory Powers Act 2000 (Lei de 2000 relativa à regulamentação dos poderes de investigação, a seguir «RIPA»), dispõe:

«(4) [E]ntende-se por "dados relativos a comunicações" qualquer um dos conceitos seguintes:

(a) quaisquer dados relativos ao tráfego contidos numa comunicação ou a ela anexados (pelo remetente ou por outra entidade) para efeitos de um serviço postal ou de um sistema de telecomunicações através do qual seja ou possa ser transmitida;

(b) quaisquer informações que não incluam o conteúdo de uma comunicação [exceto informações abrangidas pela (a)] e que digam respeito à utilização por qualquer pessoa:
(i) de um serviço postal ou de um serviço de telecomunicações; ou
(ii) de uma parte de um sistema de telecomunicações, no âmbito do fornecimento ou da utilização de um serviço de telecomunicações;

(c) de quaisquer informações não abrangidas pelas alíneas (a) ou (b), que se encontrem na posse de uma pessoa que forneça um serviço postal ou um serviço de telecomunicações, ou que sejam obtidas por essa pessoa, relativas aos destinatários desse serviço.

[…]

(6) [O] conceito de "dado de tráfego", relacionado com qualquer comunicação, visa:

(a) qualquer dado que identifique ou seja suscetível de identificar qualquer pessoa, qualquer aparelho ou localização para os quais ou a partir dos quais uma comunicação seja ou possa ser transmitida,

b) qualquer dado que identifique ou selecione ou seja suscetível de identificar ou selecionar o aparelho através do qual a comunicação seja ou possa ser transmitida,

(c) qualquer dado que contenha sinais para a ativação do aparelho utilizado nos objetivos de um sistema de comunicação para efeitos da transmissão de qualquer comunicação, e

(d) qualquer dado que identifique os dados incluídos numa determinada comunicação ou outros dados enquanto dados incluídos ou juntos a uma determinada comunicação.

[…]»

18 As sections 65 a 69 da RIPA estabelecem as regras relativas ao funcionamento e às competências do Investigatory Powers Tribunal (Tribunal de Instrução, Reino Unido). Em conformidade com a section 65 dessa lei, podem ser apresentadas queixas nesse tribunal se existirem razões para supor que os dados foram obtidos de forma inadequada.

## Litígio no processo principal e questões prejudiciais

19 No início de 2015, a existência de práticas de recolha e de utilização de dados de comunicações em massa por diferentes serviços de segurança e de informações do Reino Unido, a saber, o GCHQ, o MI5 e o MI6, foi tornada pública, nomeadamente num relatório do Intelligence and Security Committee of Parliament (Comissão de Informação e Segurança do Parlamento, Reino Unido). Em 5 de junho de 2015, a Privacy International, organização não-governamental, propôs uma ação no Investigatory Powers Tribunal (Tribunal de Instrução, Reino Unido) contra o Ministro dos Negócios Estrangeiros e da Commonwealth, o Ministro da Administração Interna e os referidos serviços de segurança e de informações, na qual contestava a legalidade dessas práticas.

20 O órgão jurisdicional de reenvio apreciou a legalidade das referidas práticas à luz, em primeiro lugar, do direito interno e das disposições da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, assinada em Roma em 4 de novembro de 1950 (a seguir «CEDH»), e, posteriormente, do direito da União. Numa Decisão de 17 de outubro de 2016, esse órgão jurisdicional concluiu que os demandados no processo principal tinham reconhecido que os referidos serviços de segurança e de informação recolhiam e utilizavam, no âmbito das suas atividades, conjuntos de dados relativos a particulares e pertencentes a diferentes categorias (*bulk personal data*), tais como dados biográficos ou relativos a viagens, informações de natureza financeira ou comercial, dados relacionados com comunicações e suscetíveis de incluir dados sensíveis, abrangidos pelo segredo profissional, ou ainda material jornalístico. Estes dados, obtidos por diversas vias, eventualmente secretos, seriam analisados através de cruzamento e de tratamentos automatizados, poderiam ser divulgados a outras pessoas e autoridades e partilhados com parceiros estrangeiros. Neste âmbito, os serviços de segurança e de informação utilizariam igualmente dados relativos a comunicações em massa, recolhidos junto dos prestadores de redes públicas de comunicações eletrónicas ao abrigo, nomeadamente, de instruções ministeriais adotadas com base na section 94 da Lei de 1984. O GCHQ e o MI5 atuariam deste modo, respetivamente, desde os anos de 2001 e 2005.

21 O referido órgão jurisdicional considerou que essas medidas de recolha e de utilização de dados estavam em conformidade com o direito interno e, desde 2015, sem prejuízo das questões ainda não apreciadas relativas à proporcionalidade das referidas medidas e às transferências de dados para terceiros, ao artigo 8.º da CEDH. A esse respeito, precisou que lhe tinham sido apresentadas provas relativas às garantias aplicáveis, nomeadamente quanto aos procedimentos de acesso e de divulgação fora dos serviços de segurança e de informação, às modalidades de conservação dos dados e à existência de controlos independentes.

22 No que se refere à legalidade das medidas de recolha e de utilização em causa no processo principal à luz do direito da União, o órgão jurisdicional de reenvio examinou, em Decisão de 8 de setembro de 2017, se essas medidas se integravam no âmbito de aplicação desse direito e, em caso afirmativo, se eram compatíveis com o mesmo. O referido órgão jurisdicional concluiu, quanto aos dados relativos às comunicações em massa, que os prestadores de redes de comunicações eletrónicas estavam obrigados, por força da section 94 da Lei de 1984, em caso de instruções nesse sentido emanadas por um ministro, a fornecer os dados recolhidos no âmbito da sua atividade económica abrangida pelo direito da União aos serviços de segurança e de informações. Em contrapartida, isso não sucedia quanto à recolha de outros dados, obtidos por tais serviços sem recurso a esses poderes vinculativos. Com base nesta constatação, o referido órgão jurisdicional considerou necessário colocar ao Tribunal de Justiça a questão de saber se um regime como o que resulta dessa section 94 está abrangido pelo direito da União e, em caso afirmativo, se, e de que maneira, são aplicáveis a esse regime os requisitos impostos pela jurisprudência decorrente do Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, a seguir «Acórdão Tele2», EU:C:2016:970).

23 A esse respeito, no seu pedido de decisão prejudicial, o órgão jurisdicional de reenvio indica que, segundo a referida section 94, um ministro pode dirigir aos prestadores de serviços de comunicações eletrónicas as instruções gerais ou específicas que considere necessárias no interesse da segurança nacional ou das relações com um governo estrangeiro. Remetendo para as definições que figuram na section 21(4) e (6) da RIPA, esse órgão jurisdicional precisa que os dados em causa incluem dados de tráfego, assim como informações sobre os serviços utilizados, na aceção desta última disposição, estando apenas excluído o conteúdo das comunicações. Esses dados e essas informações permitem, nomeadamente, conhecer «quem, onde, quando e como» efetua uma comunicação. Os referidos dados são transmitidos aos serviços de segurança e de informações e conservados por estes para efeitos das suas atividades.

24 Segundo o referido órgão jurisdicional, o regime em causa no processo principal distingue-se do que resulta do Data Retention and Investigatory Powers Act 2014 (Lei de 2014 sobre a Conservação de Dados e os Poderes de Investigação), em causa no processo que deu origem ao Acórdão de 21 de dezembro de 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970), uma vez que este último regime previa a conservação dos dados pelos prestadores de serviços de comunicações eletrónicas e a sua disponibilização não apenas aos serviços de segurança e de informações, no interesse da segurança nacional, mas igualmente a outras autoridades públicas, em função das suas necessidades. Além disso, esse acórdão dizia respeito a uma investigação criminal e não à segurança nacional.

25 O órgão jurisdicional de reenvio acrescenta que as bases de dados constituídas pelos serviços de segurança e de informações são objeto de tratamento em massa e automatizado, não específico, que visa revelar a existência de eventuais ameaças desconhecidas. Para o efeito, esse órgão jurisdicional refere que os conjuntos de metadados assim constituídos devem ser tão completos quanto possível, de modo que exista um «palheiro» no qual se possa encontrar «a agulha» nele escondida. Quanto à utilidade da recolha de dados em massa pelos referidos serviços e das técnicas de consulta desses dados, o referido órgão jurisdicional menciona, em particular, as conclusões do relatório apresentado em 19 de agosto de 2016 por David Anderson, QC, enquanto United Kingdom Independent Reviewer of Terrorism Legislation (auditor independente do Reino Unido no que respeita à legislação relativa ao terrorismo), e que se baseou, para elaborar esse relatório, num exame efetuado por uma equipa de especialistas da informação e no testemunho de agentes dos serviços de segurança e de informação.

26 O órgão jurisdicional de reenvio precisa igualmente que, segundo a Privacy International, o regime em causa no processo principal é ilegal à luz do direito da União, ao passo que os demandados no processo principal consideram que a obrigação de transmissão dos dados prevista por esse regime, o acesso a esses dados e a sua utilização não estão abrangidos pelas competências da União, em conformidade, nomeadamente, com o artigo 4.º, n.º 2, TUE, segundo o qual a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro.

27 A esse respeito, o órgão jurisdicional de reenvio considera, com base no Acórdão de 30 de maio de 2006, Parlamento/Conselho e Comissão (C-317/04 e C-318/04, EU:C:2006:346, n.os 56 a 59), relativo à transferência de dados PNR (*Passenger Name Record*) para efeitos de proteção da segurança pública, que as atividades das sociedades comerciais enquadradas no tratamento e na transferência de dados para proteger a segurança nacional não se afiguram abrangidas pelo âmbito de aplicação do direito da União. Não é necessário apreciar se a atividade em causa constitui um tratamento de dados, mas apenas se, na sua substância e nos seus efeitos, o objeto de tal atividade é apoiar uma função essencial do Estado, na aceção do artigo 4.º, n.º 2, TUE, através de um quadro estabelecido pelas autoridades públicas relativo à segurança pública.

28 No caso de as medidas em causa no processo principal estarem, ainda assim, abrangidas pelo direito da União, o órgão jurisdicional de reenvio considera que os requisitos que figuram nos n.os 119 a 125 do Acórdão de 21 de dezembro de 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970), parecem inadequados no âmbito da segurança nacional e são suscetíveis de prejudicar a capacidade dos serviços de segurança e de informação para controlarem determinadas ameaças à segurança nacional.

29 Neste contexto, o Investigatory Powers Tribunal (Tribunal de Instrução) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«Em circunstâncias em que:

a) a capacidade [de os serviços de segurança e de informações] utilizarem [os dados de comunicações em massa] que lhes são fornecidos é essencial para a proteção da segurança nacional do Reino Unido, nomeadamente nos domínios do combate ao terrorismo, à espionagem e à proliferação nuclear;

b) um elemento fundamental da utilização de [dados de comunicações em massa] pelos [serviços de segurança e de informações] é a deteção de ameaças à segurança nacional até aí desconhecidas, através de técnicas em massa sem alvo específico, cuja utilização depende da reunião dos [dados de comunicações em massa] num único local. A sua principal utilidade está relacionada com a identificação rápida dos alvos e o seu seguimento, bem como com o fornecimento de uma base de ação em caso de ameaça iminente;

c) o prestador de uma rede de comunicações eletrónicas não tem, por conseguinte, de guardar os [dados de comunicações em massa] (para além dos prazos habitualmente aplicáveis à sua atividade), que são conservados apenas pelo Estado ([serviços de segurança e de informações]);

d) órgão jurisdicional nacional concluiu (sob reserva de algumas questões) que as salvaguardas relativas à utilização dos [dados de comunicações em massa] pelos [serviços de segurança e de informações] são conformes com os requisitos da CEDH; e

e) órgão jurisdicional nacional concluiu que a imposição dos requisitos descritos nos n.os 119-125 do Acórdão [de 21 de dezembro de 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970)], quando aplicáveis, comprometeria as medidas de proteção da segurança nacional adotadas pelos [serviços de segurança e de informações] e, consequentemente, poria em risco a segurança nacional do Reino Unido;

1) Tendo em conta o artigo 4.º TUE e o artigo 1.º, n.º 3, da Diretiva [2002/58], uma imposição constante de uma instrução de um [ministro] ao prestador de uma rede de comunicações eletrónicas, de fornecimento de dados de comunicações em massa aos serviços de segurança e de informações de um Estado-Membro enquadra-se no âmbito de aplicação do direito da União e da Diretiva [2002/58]?

2) Em caso de resposta afirmativa à [primeira questão], os requisitos [aplicáveis aos dados relativos às comunicações conservadas, especificadas nos n.os 119 a 125 do Acórdão de 21 de dezembro de 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970)] ou quaisquer outros requisitos que vão além dos previstos pela CEDH, são aplicáveis à referida instrução do [ministro]? E, se assim for, quais as modalidades e o alcance da aplicação desses requisitos, tendo em conta a necessidade essencial dos [serviços de segurança e de informações] de recorrerem à aquisição em massa e a técnicas de tratamento automatizado com vista à proteção da segurança nacional e a medida em que o exercício dessa faculdade, se no demais respeitar a CEDH, pode ser gravemente dificultado pela imposição de tais requisitos?»

## Quanto às questões prejudiciais

### *Quanto à primeira questão*

30 Com a sua primeira questão, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 1.º, n.º 3, da Diretiva 2002/58, lido à luz do artigo 4.º, n.º 2, TUE, deve ser interpretado no sentido de que o âmbito de aplicação desta diretiva abrange uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas a transmissão de dados de tráfego e de dados de localização aos serviços de segurança e de informações para efeitos da salvaguarda da segurança nacional.

31 A este respeito, a Privacy International alega, em substância, que, tendo em consideração os ensinamentos decorrentes da jurisprudência do Tribunal de Justiça quanto ao âmbito de aplicação da Diretiva 2002/58, tanto a recolha de dados pelos serviços de segurança e de informações junto desses prestadores, ao abrigo da section 94 da Lei de 1984, como a sua utilização pelos referidos serviços se integram no âmbito de aplicação dessa diretiva, quer esses dados sejam recolhidos através de uma transmissão efetuada em tempo diferido quer em tempo real. Em particular, o facto de o objetivo de proteção da segurança nacional ser expressamente enumerado no artigo 15.º, n.º 1, da referida diretiva não tem como consequência a inaplicabilidade desta a tais situações, e o artigo 4.º, n.º 2, TUE não afeta esta apreciação.

32 Em contrapartida, os Governos do Reino Unido, checo e estónio, a Irlanda, bem como os Governos francês, cipriota, húngaro, polaco e sueco, alegam, em substância, que a Diretiva 2002/58 não é aplicável à regulamentação em causa no processo principal, na medida em que esta tem por finalidade a salvaguarda da segurança nacional. As atividades dos serviços de segurança e de informações fazem parte das funções essenciais dos Estados-Membros relativas à manutenção da ordem pública assim como à salvaguarda da segurança interna e da integridade territorial e, por conseguinte, são da exclusiva competência destes últimos, como demonstra, nomeadamente, o artigo 4.º, n.º 2, terceiro período, TUE.

33 Segundo esses Governos, a Diretiva 2002/58 não pode, assim, ser interpretada no sentido de que as medidas nacionais que visam a salvaguarda da segurança nacional se integram no seu âmbito de aplicação. O artigo 1.º, n.º 3, dessa diretiva limita esse âmbito de aplicação e exclui do mesmo, à semelhança do que já previa o artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, as atividades relativas à segurança pública, à defesa e à segurança do Estado. Estas disposições refletem a repartição de competências previstas no artigo 4.º, n.º 2, TUE e ficariam privadas de efeito útil se medidas pertencentes ao domínio da segurança nacional tivessem de respeitar os requisitos da Diretiva 2002/58. Por outro lado, a jurisprudência do Tribunal de Justiça decorrente do Acórdão de 30 de maio de 2006, Parlamento/Conselho e Comissão (C-317/04 e C-318/04, EU:C:2006:346), relativa ao artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, é transponível para o artigo 1.º, n.º 3, da Diretiva 2002/58.

34 A este respeito, importa referir que, nos termos do seu artigo 1.º, n.º 1, a Diretiva 2002/58 prevê, nomeadamente, 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 sector das comunicações eletrónicas.

35 O artigo 1.º, n.º 3, dessa diretiva 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. As atividades assim referidas a título de exemplo serão, em qualquer caso, atividades próprias dos Estados ou das autoridades estatais, alheias aos domínios de atividade dos particulares (Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 32 e jurisprudência aí referida).

36 Além disso, o artigo 3.º da Diretiva 2002/58 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 de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 33 e jurisprudência aí referida).

37 Neste âmbito, o artigo 15.º, n.º 1, da Diretiva 2002/58 autoriza os Estados-Membros a adotarem, desde que respeitadas as condições nele previstas, «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 [dessa] diretiva» (Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 71).

38 Ora, o artigo 15.º, n.º 1, da Diretiva 2002/58 pressupõe necessariamente que as medidas legislativas 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 (Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 34 e jurisprudência aí referida).

39 Foi nomeadamente à luz destas considerações que o Tribunal de Justiça declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido em conjugação com o artigo 3.º da mesma, 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 os obriga a conceder às autoridades nacionais o acesso aos dados conservados. Com efeito, tais medidas legislativas implicam necessariamente, da parte destes prestadores, o tratamento dos referidos dados, e não podem, visto que regulam as atividades destes mesmos prestadores, ser equiparadas às atividades próprias dos Estados, referidas no artigo 1.º, n.º 3, da referida diretiva (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.ºs 35 e 37 e jurisprudência aí referida).

40 No que diz respeito a uma medida legislativa como a section 94 da Lei de 1984, com base na qual a autoridade competente pode dirigir aos prestadores de serviços de comunicações eletrónicas a instrução de comunicarem por transmissão dados em massa aos serviços de segurança e de informações, importa assinalar que, em virtude da definição que figura no artigo 4.º, ponto 2, do Regulamento 2016/679, que é aplicável, em conformidade com o artigo 2.º da Diretiva 2002/58, lido em conjugação com o artigo 94.º, n.º 2, do referido regulamento, o conceito de «tratamento de dados pessoais» designa «uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou

sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, […], a conservação, […], a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização […]».

41 Daqui decorre que uma comunicação de dados pessoais por transmissão, tal como uma conservação de dados ou qualquer outra forma de disponibilização, constitui um tratamento, na aceção do artigo 3.º da Diretiva 2002/58, e, por conseguinte, integra-se na aplicação dessa diretiva (v., neste sentido, Acórdão de 29 de janeiro de 2008, Promusicae, C-275/06, EU:C:2008:54, n.º 45).

42 Além disso, à luz das considerações que figuram no n.º 38 do presente acórdão e da sistemática geral da Diretiva 2002/58, uma interpretação desta diretiva segundo a qual as medidas legislativas previstas no seu artigo 15.º, n.º 1, são excluídas do âmbito de aplicação da referida diretiva devido ao facto de as finalidades a que tais medidas devem responder coincidirem substancialmente com as finalidades prosseguidas pelas atividades referidas no artigo 1.º, n.º 3, da mesma diretiva, priva este artigo 15.º, n.º 1, de efeito útil (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.ºs 72 e 73).

43 O conceito de «atividades» que figura no artigo 1.º, n.º 3, da Diretiva 2002/58 não pode, como salientou, em substância, o advogado-geral no n.º 75 das Conclusões que apresentou nos processos apensos La Quadrature du Net e o. (C-511/18 e C-512/18, EU:C:2020:6), para as quais remete no n.º 24 das Conclusões que apresentou no presente processo, ser interpretado no sentido de que abrange as medidas legislativas previstas no artigo 15.º, n.º 1, dessa diretiva.

44 As disposições do artigo 4.º, n.º 2, TUE, às quais se referiram os Governos mencionados no n.º 32 do presente acórdão, não podem infirmar esta conclusão. Com efeito, em conformidade com jurisprudência constante do Tribunal de Justiça, embora incumba aos Estados-Membros definir os seus interesses essenciais de segurança e adotar as medidas adequadas para garantir a sua segurança interna e externa, o simples facto de uma medida nacional ter sido adotada para efeitos da proteção da segurança nacional não pode levar à inaplicabilidade do direito da União e dispensar os Estados-Membros do respeito necessário desse direito [v., neste sentido, Acórdãos de 4 de junho de 2013, ZZ, C-300/11, EU:C:2013:363, n.º 38 e jurisprudência aí referida; de 20 de março de 2018, Comissão/Áustria (Imprensa do Estado), C-187/16, EU:C:2018:194, n.ºs 75 e 76; e de 2 de abril de 2020, Comissão/Polónia, Hungria e República Checa (Mecanismo temporário de recolocação de requerentes de proteção internacional), C-715/17, C-718/17 e C-719/17, EU:C:2020:257, n.ºs 143 e 170].

45 É certo que, no Acórdão de 30 de maio de 2006, Parlamento/Conselho e Comissão (C-317/04 e C-318/04, EU:C:2006:346, n.ºs 56 a 59), o Tribunal de Justiça declarou que a transferência de dados pessoais por companhias aéreas para as autoridades públicas de um Estado terceiro tendo em vista a prevenção e a luta contra o terrorismo e outros crimes graves não estava abrangida, por força do artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, pelo âmbito de aplicação desta diretiva, uma vez que tal transferência se integrava num quadro instituído pelos poderes públicos que visava a segurança pública.

46 No entanto, tendo em conta as considerações que figuram nos n.ºs 36, 38 e 39 do presente acórdão, essa jurisprudência não é transponível para a interpretação do artigo 1.º, n.º 3, da Diretiva 2002/58. Com efeito, como salientou, em substância, o advogado-geral nos n.ºs 70 a 72 das Conclusões que apresentou nos processos apensos La Quadrature du Net e o. (C-511/18 e C-512/18, EU:C:2020:6), o artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, ao qual se refere essa jurisprudência, excluía do âmbito de aplicação desta última diretiva, de forma geral, o «tratamento de dados que tenha por objeto a segurança pública, a defesa, a segurança do Estado», sem estabelecer uma distinção em função do autor do tratamento de dados em causa. Em contrapartida, no âmbito da interpretação do artigo 1.º, n.º 3, da Diretiva 2002/58, essa distinção revela-se necessária. Com efeito, conforme resulta dos n.ºs 37 a 39 e 42 do presente acórdão, todos os tratamentos de dados pessoais efetuados pelos prestadores de

serviços de comunicações eletrónicas estão abrangidos pelo âmbito de aplicação da referida diretiva, incluindo os tratamentos que decorrem de obrigações que lhes são impostas pelos poderes públicos, ao passo que esses tratamentos podem eventualmente integrar-se no âmbito de aplicação da exceção prevista no artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, tendo em conta a formulação mais ampla desta disposição, que visa todos os tratamentos, independentemente do seu autor, que tenham por objeto a segurança pública, a defesa, a segurança do Estado.

47 Por outro lado, importa assinalar que a Diretiva 95/46, em causa no processo que deu origem ao Acórdão de 30 de maio de 2006, Parlamento/Conselho e Comissão (C-317/04 e C-318/04, EU:C:2006:346), foi, por força do artigo 94.º, n.º 1, do Regulamento 2016/679, revogada e substituída por este, com efeitos a contar de 25 de maio de 2018. Ora, embora o referido regulamento precise, no seu artigo 2.º, n.º 2, alínea d), que não é aplicável aos tratamentos efetuados «pelas autoridades competentes» para efeitos, nomeadamente, de prevenção e de deteção de infrações penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, resulta do artigo 23.º, n.º 1, alíneas d) e h), do mesmo regulamento que os tratamentos de dados pessoais efetuados para esses mesmos fins por particulares se integram no seu âmbito de aplicação. Daqui resulta que a interpretação do artigo 1.º, n.º 3, do artigo 3.º e do artigo 15.º, n.º 1, da Diretiva 2002/58 que precede é coerente com a delimitação do âmbito de aplicação do Regulamento 2016/679 que esta diretiva completa e precisa.

48 Em contrapartida, quando os Estados-Membros aplicam diretamente medidas que derrogam a confidencialidade das comunicações eletrónicas, sem imporem obrigações de tratamento aos prestadores de serviços de tais comunicações, a proteção dos dados das pessoas em causa não está abrangida pela Diretiva 2002/58, mas apenas pelo direito nacional, sem prejuízo da aplicação da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO 2016, L 119, p. 89), de tal modo que as medidas em causa devem respeitar, nomeadamente, o direito nacional de valor constitucional e os requisitos da CEDH.

49 Tendo em consideração o exposto, deve responder-se à primeira questão que o artigo 1.º, n.º 3, o artigo 3.º e o artigo 15.º, n.º 1, da Diretiva 2002/58, lidos à luz do artigo 4.º, n.º 2, TUE, devem ser interpretados no sentido de que o âmbito de aplicação desta diretiva abrange uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas a transmissão de dados de tráfego e de dados de localização aos serviços de segurança e de informações, para efeitos da salvaguarda da segurança nacional.

### *Quanto à segunda questão*

50 Com a sua segunda questão, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz do artigo 4.º, n.º 2, TUE, e 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 se opõe a uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, a transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações.

51 A título preliminar, importa recordar que, segundo as indicações que figuram no pedido de decisão prejudicial, a section 94 da Lei de 1984 autoriza o ministro a impor aos prestadores de serviços de comunicações eletrónicas, através de instruções, sempre que considere necessário no interesse da segurança nacional ou das relações com um governo estrangeiro, a transmissão, aos serviços de segurança e de informações, de dados relativos às comunicações em massa, incluindo os dados de tráfego e os dados de localização, bem como informações sobre os serviços utilizados, na aceção da

section 21(4) e (6), da RIPA. Esta última disposição abrange, entre outros, os dados necessários para identificar a fonte de uma comunicação e o seu destino, determinar a data, hora, duração e tipo da comunicação, identificar o material utilizado e localizar os equipamentos terminais e as comunicações, dados entre os quais figuram, nomeadamente, o nome e o endereço do utilizador, o número de telefone da pessoa que efetua a chamada e o número marcado, os endereços IP da fonte e do destinatário da comunicação, bem como os endereços dos sítios Internet visitados.

52 Tal comunicação por transmissão de dados diz respeito a todos os utilizadores de meios de comunicações eletrónicas, não sendo precisado se esse envio deve ocorrer em tempo real ou diferido. Uma vez transmitidos, estes dados são, segundo as indicações que figuram no pedido de decisão prejudicial, conservados pelos serviços de segurança e de informação e permanecem à disposição destes para efeitos das suas atividades, à semelhança das outras bases de dados que esses serviços detêm. Em particular, os dados assim recolhidos, que são sujeitos a tratamentos e a análises em massa e automatizados, podem ser cruzados com outras bases de dados que incluem diferentes categorias de dados pessoais em massa ou ser divulgados fora desses serviços e a Estados terceiros. Por último, estas operações não estão sujeitas à autorização prévia de um órgão jurisdicional ou de uma autoridade administrativa independente e não dão lugar a nenhuma informação das pessoas em causa.

53 A Diretiva 2002/58 tem por finalidade, como resulta, nomeadamente, dos seus considerandos 6 e 7, proteger os utilizadores dos serviços de comunicações eletrónicas contra os riscos para os seus dados pessoais e a sua vida privada resultantes das novas tecnologias, nomeadamente da maior capacidade de armazenamento e tratamento automatizado de dados. Em particular, a referida diretiva visa, como refere o seu considerando 2, assegurar o pleno respeito pelos direitos consignados nos artigos 7.º e 8.º da Carta. A este respeito, resulta da exposição de motivos da proposta de diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas [COM(2000) 385 final], que está na origem da Diretiva 2002/58, que o legislador da União pretendeu «assegurar a continuação de um elevado nível de proteção dos dados pessoais e da privacidade no que diz respeito a todos os serviços de comunicações eletrónicas, independentemente da tecnologia utilizada».

54 Para o efeito, o artigo 5.º, n.º 1, da Diretiva 2002/58 dispõe que «[o]s 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». Esta mesma disposição sublinha igualmente que, «[os Estados-Membros] [p]roibirão, 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», e precisa que «[este] número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.»

55 Assim, este artigo 5.º, n.º 1, consagra o princípio da confidencialidade tanto das comunicações eletrónicas como dos respetivos dados de tráfego e implica, nomeadamente, a proibição de, em princípio, pessoas diferentes dos utilizadores armazenarem, sem o seu consentimento, tais comunicações e tais dados. Tendo em conta o caráter geral da sua redação, esta disposição abrange necessariamente qualquer operação que permita a terceiros tomar conhecimento das comunicações e dos respetivos dados para fins diversos do envio de uma comunicação.

56 A proibição de intercetar as comunicações e os respetivos dados que figura no artigo 5.º, n.º 1, da Diretiva 2002/58 abrange, assim, qualquer forma de disponibilização pelos prestadores de serviços de comunicações eletrónicas de dados de tráfego e de dados de localização às autoridades públicas, tais como serviços de segurança e de informações, bem como a conservação dos referidos dados por essas autoridades, independentemente da sua utilização posterior.

57 Assim, ao adotar essa diretiva, o legislador da União concretizou os direitos consagrados nos artigos 7.º e 8.º da Carta, pelo que os utilizadores dos meios de comunicações eletrónicas têm o direito de esperar, em princípio, que as suas comunicações e os respetivos dados permaneçam, na falta do seu consentimento, anónimos e não possam ser objeto de registo (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, n.º 109).

58 No entanto, o artigo 15.º, n.º 1, da Diretiva 2002/58 permite que os Estados-Membros introduzam exceções à obrigação de princípio, prevista no artigo 5.º, n.º 1, desta diretiva, de garantir a confidencialidade dos dados pessoais, e às obrigações correspondentes, mencionadas, nomeadamente, nos artigos 6.º e 9.º da referida diretiva, sempre que constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional, a defesa e 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. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, por uma destas razões.

59 Assim sendo, a faculdade de derrogar os direitos e as obrigações previstos nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58 não pode justificar que a derrogação à obrigação de princípio de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados e, em especial, a proibição de armazenar esses dados, prevista no artigo 5.º dessa diretiva, se converta na regra (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.ºs 89 e 104, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, n.º 111).

60 Além disso, resulta do artigo 15.º, n.º 1, terceiro período, da Diretiva 2002/58 que os Estados-Membros apenas estão autorizados a adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º, 6.º e 9.º dessa diretiva no respeito dos princípios gerais do direito da União, entre os quais figura o princípio da proporcionalidade, e os direitos fundamentais garantidos pela Carta. A este respeito, o Tribunal de Justiça já declarou que a obrigação imposta por um Estado-Membro aos prestadores de serviços de comunicações eletrónicas, por uma regulamentação nacional, de conservarem os dados de tráfego para, se for caso disso, os disponibilizarem às autoridades nacionais competentes coloca questões relativas ao respeito não apenas dos artigos 7.º e 8.º da Carta, relativos, respetivamente, à proteção da vida privada e à proteção dos dados pessoais, mas igualmente do artigo 11.º da Carta, relativo à liberdade de expressão (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.ºs 25 e 70, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.ºs 91 e 92 e jurisprudência aí referida).

61 Estas mesmas questões também se colocam relativamente a outros tipos de tratamento de dados, tais como a sua transmissão a pessoas distintas dos utilizadores ou o acesso a esses dados tendo em vista a sua utilização. [v., por analogia, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.ºs 122 e 123 e jurisprudência aí referida].

62 Assim, a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58 deve ter em conta a importância tanto do direito ao respeito da vida privada, garantido pelo artigo 7.º da Carta, como do direito à proteção dos dados pessoais, garantido pelo artigo 8.º da mesma, conforme resulta da jurisprudência do Tribunal de Justiça, bem como do direito à liberdade de expressão, direito fundamental esse, garantido pelo artigo 11.º da Carta, que constitui um dos fundamentos essenciais de uma sociedade democrática e pluralista e faz parte dos valores nos quais, de acordo com o artigo 2.º TUE, se baseia a União (v., neste sentido, Acórdãos de 6 de março de 2001, Connolly/Comissão, C-274/99 P, EU:C:2001:127, n.º 39, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 93 e jurisprudência aí referida).

63 Todavia, os direitos consagrados nos artigos 7.º, 8.º e 11.º da Carta não são prerrogativas absolutas, antes devendo ser tomados em consideração relativamente à sua função na sociedade (v., neste sentido, Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, n.º 172 e jurisprudência aí referida).

64 Com efeito, conforme resulta do seu artigo 52.º, n.º 1, a Carta admite restrições ao exercício desses direitos, desde que essas restrições estejam previstas por lei, respeitem o conteúdo essencial desses direitos e, na observância do princípio da proporcionalidade, sejam necessárias e correspondam efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros.

65 Importa acrescentar que a exigência de qualquer limitação ao exercício de direitos fundamentais ser prevista por lei implica que a própria base jurídica que permite a ingerência nesses direitos deve definir o alcance da limitação do exercício do direito em causa (Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, n.º 175 e jurisprudência aí referida).

66 No que se refere ao princípio da proporcionalidade, o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 dispõe que os Estados-Membros podem adotar uma medida derrogatória do princípio da confidencialidade das comunicações e dos respetivos dados de tráfego quando tal medida seja «necessária, adequada e proporcionada numa sociedade democrática», à luz dos objetivos que essa disposição enuncia. O considerando 11 dessa diretiva precisa que uma medida dessa natureza deve ser «rigorosamente» proporcionada ao objetivo a alcançar.

67 A este respeito, importa recordar que a proteção do direito fundamental à vida privada impõe, em conformidade com a jurisprudência constante do Tribunal de Justiça, que as derrogações à proteção dos dados pessoais e as respetivas limitações ocorram na estrita medida do necessário. Além disso, um objetivo de interesse geral não pode ser prosseguido sem levar em conta o facto de que deve ser conciliado com os direitos fundamentais abrangidos pela medida, efetuando uma ponderação equilibrada entre o objetivo e os interesses e direitos em causa. [v., neste sentido, Acórdãos de 16 de dezembro de 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, EU:C:2008:727, n.º 56; de 9 de novembro de 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, n.ºs 76, 77 e 86; e de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 52; Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 140].

68 Para cumprir o requisito de proporcionalidade, uma regulamentação deve prever normas claras e precisas que regulem o âmbito e a aplicação da medida em causa e impor requisitos mínimos, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. Esta regulamentação deve ser vinculativa no direito interno e, em particular, indicar em que circunstâncias e em que condições uma medida que prevê o tratamento de tais dados pode ser adotada, garantindo assim que a ingerência seja limitada ao estritamente necessário. A necessidade de dispor de tais garantias é ainda mais importante quando os dados pessoais são submetidos a um tratamento automatizado, nomeadamente quando existe um risco significativo de acesso ilícito a tais dados. Estas considerações são particularmente válidas quando está em jogo a proteção dessa categoria específica de dados pessoais, que são os dados sensíveis [v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.ºs 54 e 55, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 117; Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 141].

69 Quanto à questão de saber se uma regulamentação nacional, como a que está em causa no processo principal, cumpre os requisitos do 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, importa observar que a transmissão de dados de tráfego e de dados de localização a pessoas distintas dos utilizadores, tais como os serviços de segurança e de

informações, derroga o princípio da confidencialidade. Uma vez que essa operação é efetuada, como sucede no caso, de forma generalizada e indiferenciada, tem por efeito tornar na regra a derrogação à obrigação de princípio de garantir a confidencialidade dos dados, ao passo que o sistema instituído pela Diretiva 2002/58 exige que essa derrogação continue a ser a exceção.

70 Além disso, em conformidade com a jurisprudência constante do Tribunal de Justiça, a transmissão dos dados de tráfego e dos dados de localização a um terceiro constitui uma ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, independentemente da utilização posterior desses dados. A este respeito, pouco importa que as informações relativas à vida privada em questão sejam ou não sensíveis, ou que os interessados tenham ou não sofrido inconvenientes em razão dessa ingerência [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 aí referida, e Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, n.os 115 e 116].

71 A ingerência que comporta a transmissão dos dados de tráfego e dos dados de localização aos serviços de segurança e de informações no direito consagrado no artigo 7.º da Carta deve ser considerada particularmente grave, tendo em conta, nomeadamente, o caráter sensível das informações que esses dados possam fornecer, nomeadamente, a possibilidade de estabelecer a partir deles o perfil das pessoas em causa, sendo tal informação tão sensível como o próprio conteúdo das comunicações. Além disso, é suscetível de gerar no espírito das pessoas em causa a sensação de que a sua vida privada é objeto de constante vigilância (v., por analogia, Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.os 27 e 37, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.os 99 e 100).

72 Importa ainda observar que uma transmissão dos dados de tráfego e dos dados de localização às autoridades públicas para fins de segurança é suscetível, por si só, de violar o direito ao respeito das comunicações, consagrado no artigo 7.º da Carta, e de produzir efeitos dissuasivos sobre o exercício, pelos utilizadores dos meios de comunicações eletrónicas, da sua liberdade de expressão, garantida no artigo 11.º da Carta. Estes efeitos dissuasivos podem afetar, em especial, as pessoas cujas comunicações estão sujeitas, segundo as regras nacionais, ao segredo profissional, bem como os denunciantes cujas atividades estão protegidas pela Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União (JO 2019, L 305, p. 17). Além disso, esses efeitos são tanto mais graves quanto maiores sejam o número e a variedade dos dados conservados (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 28; de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 101; e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, n.º 118).

73 Por último, tendo em conta a quantidade significativa de dados de tráfego e de dados de localização suscetíveis de ser conservados de forma contínua através de uma medida de conservação generalizada, bem como o caráter sensível das informações que esses dados podem fornecer, a mera conservação dos referidos dados pelos prestadores de serviços de comunicações eletrónicas comporta riscos de abuso e de acesso ilícito.

74 Quanto aos objetivos suscetíveis de justificar essas ingerências, mais particularmente quanto ao objetivo de salvaguarda da segurança nacional, em causa no processo principal, importa salientar, antes de mais, que o artigo 4.º, n.º 2, TUE estabelece que a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro. Esta responsabilidade corresponde ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da sociedade e inclui a prevenção e a repressão de atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país, em especial de ameaçar diretamente a sociedade, a população ou o Estado enquanto tal, como, nomeadamente, as atividades terroristas (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, n.º 135).

75 Ora, a importância do objetivo de salvaguarda da segurança nacional, lido à luz do artigo 4.º, n.º 2, TUE, ultrapassa a dos outros objetivos referidos no artigo 15.º, n.º 1, da Diretiva 2002/58, nomeadamente os objetivos de luta contra a criminalidade em geral, mesmo grave, e de salvaguarda da segurança pública. Com efeito, ameaças como as referidas no número anterior distinguem-se, pela sua natureza e particular gravidade, do risco geral de ocorrência de tensões ou de perturbações, ainda que graves, à segurança pública. Sem prejuízo do respeito dos outros requisitos previstos no artigo 52.º, n.º 1, da Carta, o objetivo de salvaguarda da segurança nacional é, por conseguinte, suscetível de justificar medidas que incluam ingerências nos direitos fundamentais mais graves do que aquelas que esses outros objetivos poderiam justificar (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, n.º 136).

76 No entanto, para cumprir o requisito de proporcionalidade recordado no n.º 67 do presente acórdão, segundo o qual as exceções à proteção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário, uma regulamentação nacional que inclui uma ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta deve respeitar os requisitos decorrentes da jurisprudência referida nos n.ºs 65, 67 e 68 do presente acórdão.

77 Em particular, no que diz respeito ao acesso de uma autoridade aos dados pessoais, uma regulamentação não se pode limitar a exigir que o acesso das autoridades aos dados responda à finalidade prosseguida por esta regulamentação, devendo igualmente prever as condições materiais e processuais que regulam essa mesma utilização [v., por analogia, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 192 e jurisprudência aí referida].

78 Assim, e uma vez que um acesso generalizado a todos os dados conservados, na falta de qualquer relação, mesmo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário, a regulamentação nacional relativa ao acesso aos dados de tráfego e aos dados de localização 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 em causa (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 119 e jurisprudência aí referida).

79 Estes requisitos são aplicáveis, *a fortiori*, a uma medida legislativa, como a que está em causa no processo principal, com base na qual a autoridade nacional competente pode impor aos prestadores de serviços de comunicações eletrónicas que procedam à comunicação por transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informação. Com efeito, tal transmissão tem por efeito colocar esses dados à disposição das autoridades públicas [v., por analogia, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 212].

80 Uma vez que a transmissão de dados de tráfego e de dados de localização ocorre de forma generalizada e indiferenciada, afeta globalmente todas as pessoas que utilizam serviços de comunicações eletrónicas. Por conseguinte, aplica-se inclusivamente a pessoas em relação às quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com o objetivo de salvaguarda da segurança nacional e, em particular, sem que seja estabelecida uma relação entre os dados cuja transmissão está prevista e uma ameaça para a segurança nacional (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.ºs 57 e 58, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 105). Tendo em conta que a transmissão desses dados às autoridades públicas equivale a um acesso, de acordo com o que se observa no n.º 79 do presente acórdão, há que considerar que uma regulamentação que permite uma transmissão generalizada e indiferenciada dos dados às autoridades públicas implica um acesso geral.

81 Daqui resulta que uma regulamentação nacional que impõe aos prestadores de serviços de comunicações eletrónicas que procedam à comunicação por transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática, conforme exige o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz do artigo 4.º, n.º 2, TUE, e dos artigos 7.º, 8.º e 11.º e do artigo 52.º, n.º 1, da Carta.

82 Tendo em consideração o exposto, deve responder-se à segunda questão que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz do artigo 4.º, n.º 2, TUE, e dos artigos 7.º, 8.º e 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, a transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações.

## Quanto às despesas

83 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:

1) **O artigo 1.º, n.º 3, o artigo 3.º e 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 sector 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, lidos à luz do artigo 4.º, n.º 2, TUE, devem ser interpretados no sentido de que o âmbito de aplicação desta diretiva abrange uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas a transmissão de dados de tráfego e de dados de localização aos serviços de segurança e de informações para efeitos da salvaguarda da segurança nacional.**

2) **O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz do artigo 4.º, n.º 2, TUE e dos artigos 7.º, 8.º e 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, a transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações.**

Assinaturas