Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

5 de abril de 2022 *

«Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Confidencialidade das comunicações — Prestadores de serviços de comunicações eletrónicas — Conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização — Acesso aos dados conservados — Fiscalização jurisdicional *ex post* — Diretiva 2002/58/CE — 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 — Possibilidade de um órgão jurisdicional nacional limitar no tempo os efeitos de uma declaração de invalidade de uma legislação nacional incompatível com o direito da União — Exclusão»

No processo C-140/20,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pela Supreme Court (Supremo Tribunal, Irlanda), por Decisão de 25 de março de 2020, que deu entrada no Tribunal de Justiça na mesma data, no processo

G.D.

contra

Commissioner of An Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General,

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: K. Lenaerts, presidente, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis e N. Jääskinen, presidentes de secção, T. von Danwitz (relator), M. Safjan, F. Biltgen, P. G. Xuereb, N. Piçarra, L. S. Rossi e A. Kumin, juízes,

advogado-geral: M. Campos Sánchez-Bordona,

secretário: D. Dittert, chefe de unidade,

vistos os autos e após a audiência de 13 de setembro de 2021,

* Língua do processo: inglês.

vistas as observações apresentadas:

— em representação de G.D., por J. Dunphy, solicitor, R. Kennedy, R. Farrell, SC, e K. McCormack, BL,

— em representação do Commissioner of An Garda Síochána, do Minister for Communications, Energy and Natural Resources e do Attorney General, por M. Browne, S. Purcell, C. Stone, J. Quaney e A. Joyce, na qualidade de agentes, assistidos por S. Guerin, P. Gallagher, SC, D. Fennelly e L. Dwyer, BL,

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

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

— em representação do Governo dinamarquês, inicialmente por J. Nymann-Lindegren, M. Jespersen e M. Wolff, e em seguida por M. Wolff e V. Jørgensen, na qualidade de agentes,

— em representação do Governo estónio, por A. Kalbus e M. Kriisa, na qualidade de agentes,

— em representação do Governo espanhol, por L. Aguilera Ruiz, na qualidade de agente,

— em representação do Governo francês, por E. de Moustier, A. Daniel, D. Dubois, T. Stéhelin e J. Illouz, na qualidade de agentes,

— em representação do Governo cipriota, por I. Neophytou, na qualidade de agente,

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

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

— em representação do Governo português, por L. Inez Fernandes, P. Barros da Costa e I. Oliveira, na qualidade de agentes,

— em representação do Governo finlandês, por M. Pere e A. Laine, na qualidade de agentes,

— em representação do Governo sueco, por O. Simonsson, J. Lundberg, H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson e H. Eklinder, na qualidade de agentes,

— em representação da Comissão Europeia, por S. L. Kalėda, H. Kranenborg, M. Wasmeier e F. Wilman, na qualidade de agentes,

— em representação da Autoridade Europeia para a Proteção de Dados, por D. Nardi, N. Stolič, K. Ujazdowski e A. Buchta, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 18 de novembro de 2021,

profere o presente

Acórdão

1 O pedido de decisão prejudicial tem por objeto a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (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, 8.º, 11.º e 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 G.D. ao Commissioner of An Garda Síochána (Comissário da Polícia Nacional, Irlanda), ao Minister for Communications, Energy and Natural Resources (Ministro das Comunicações, Energia e Recursos Naturais, Irlanda) e ao Attorney General a respeito da validade do Communications (Retention of Data) Act 2011 [Lei das Comunicações (Conservação de Dados) de 2011, a seguir «Lei de 2011»].

Quadro jurídico

Direito da União

3 Os considerandos 2, 6, 7 e 11 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].

[…]

(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/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)], 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.»

4 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 [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 Tratado [FUE], 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.»

5 Nos termos do artigo 2.º da Diretiva 2002/58, intitulado «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” quaisquer dados tratados numa rede de comunicações eletrónicas ou por um serviço 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;

[…]»

6 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 [União], nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação.»

7 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.»

8 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.

[…]»

9 O artigo 9.º desta diretiva, intitulado «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. […]»

10 O artigo 15.º da Diretiva 2002/58, 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.»

Direito irlandês

11 Como resulta do pedido de decisão prejudicial, a Lei de 2011 foi adotada para transpor para a ordem jurídica irlandesa 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).

12 O artigo 1.º da Lei de 2011 define o termo «dados» como visando «os dados de tráfego ou os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador», e o termo «infração grave» como visando uma infração passível de pena de prisão de duração igual ou superior a cinco anos ou uma das outras infrações enumeradas no anexo 1 desta lei.

13 O artigo 3.º, n.º 1, da referida lei impõe a todos os prestadores de serviços de comunicações eletrónicas que conservem os dados referidos no seu anexo 2, parte 1, durante um período de dois anos e os dados referidos no seu anexo 2, parte 2, durante um ano.

14 O anexo 2, parte 1, da mesma lei visa, entre outros, os dados relativos às comunicações telefónicas nas redes fixa e móvel que permitem identificar a fonte e o destino de uma comunicação, determinar a data e a hora do início e do fim de uma comunicação, determinar o tipo de comunicação em causa e identificar o tipo e a localização geográfica do material de comunicação utilizado. Em especial, o ponto 6 deste anexo 2, parte 1, prevê a conservação dos dados necessários para localizar um meio de comunicação eletrónica móvel, sendo estes dados, por um lado, o identificador da célula e, por outro, dados que permitam determinar a localização geográfica das células, referindo-se à sua identidade de localização (identificador da célula), durante o período em que os dados de comunicação são conservados.

15 O anexo 2, parte 2, da Lei de 2011 visa os dados relativos ao acesso à Internet, o correio eletrónico e as comunicações telefónicas através da Internet e abrange, nomeadamente, os números de identificadores e de telefone, os endereços IP, bem como a data e a hora do início e do fim de uma comunicação. O teor das comunicações não está abrangido por este tipo de dados.

16 Por força dos artigos 4.º e 5.º da Lei de 2011, os prestadores de serviços de comunicações eletrónicas devem tomar determinadas medidas para garantir que os dados sejam protegidos contra os acessos não autorizados.

17 O artigo 6.º desta lei, que prevê as condições em que pode ser apresentado um pedido de acesso, dispõe, no seu n.º 1:

«Um agente da Polícia Nacional cuja posição não seja inferior à de superintendente-chefe pode pedir a um prestador de serviços que lhe comunique os dados conservados por esse prestador de serviços em conformidade com o artigo 3.º, se esse funcionário considerar que os dados em questão são necessários para efeitos:

(a) de prevenção, deteção, investigação ou repressão de uma infração grave,

(b) de salvaguarda da segurança do Estado,

(c) de preservação da vida humana.»

18 O artigo 7.º da referida lei obriga os prestadores de serviços de comunicações eletrónicas a deferir os pedidos referidos no seu artigo 6.º

19 Entre os mecanismos de controlo da decisão do agente da Polícia Nacional mencionados no artigo 6.º da Lei de 2011 figuram o procedimento de reclamação previsto no artigo 10.º desta lei, e o procedimento perante o *designated judge* (juiz designado), na aceção do seu artigo 12.º, ao qual incumbe fiscalizar a aplicação das disposições da referida lei.

Litígio no processo principal e questões prejudiciais

20 Em março de 2015, G.D. foi condenado a uma pena de prisão perpétua pelo homicídio de uma pessoa que havia desaparecido em agosto de 2012 e cujo cadáver só foi descoberto em setembro de 2013. No recurso da sua condenação, o interessado acusou nomeadamente o órgão jurisdicional de primeira instância de ter erradamente admitido como meios de prova dados de tráfego e dados de localização relativos a chamadas telefónicas, com o fundamento de que a Lei de 2011, que regulava a conservação desses dados e com base na qual os investigadores da Polícia Nacional tinham tido acesso aos referidos dados, violava os direitos que lhe são conferidos pelo direito da União. Este recurso está atualmente pendente.

21 Para poder impugnar, no âmbito do processo penal, a admissibilidade das referidas provas, G.D. instaurou na High Court (Tribunal Superior, Irlanda) uma ação cível com vista a obter a declaração da invalidade de determinadas disposições da Lei de 2011. Por Decisão de 6 de dezembro de 2018, esse órgão jurisdicional julgou procedente a argumentação de G.D. e considerou que o artigo 6.º, n.º 1, alínea a), desta lei era incompatível com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta. A Irlanda recorreu desta decisão para a Supreme Court (Supremo Tribunal, Irlanda), o órgão jurisdicional de reenvio.

22 O processo penal pendente na Court of Appeal (Tribunal de Recurso, Irlanda) foi suspenso até ser proferida a decisão do órgão jurisdicional de reenvio no âmbito da ação cível no processo principal.

23 Perante o órgão jurisdicional de reenvio, a Irlanda sustentou que, para determinar se a ingerência no direito ao respeito pela vida privada consagrado no artigo 7.º da Carta, resultante da conservação dos dados de tráfego e dos dados de localização ao abrigo da Lei de 2011, é proporcionada, há que examinar os objetivos do regime implementado por esta lei na sua globalidade. Além disso, segundo este Estado-Membro, a referida lei estabeleceu um quadro detalhado de regulação do acesso aos dados conservados, nos termos do qual a unidade da Polícia Nacional encarregada da apreciação prévia dos pedidos de acesso goza de independência funcional em relação à Polícia Nacional no exercício da sua missão e, por conseguinte, satisfaz o requisito de um controlo prévio dos pedidos de acesso efetuado por uma entidade administrativa independente. Este sistema de controlo é reforçado por um procedimento de reclamação e por uma fiscalização jurisdicional. Por último, o referido Estado-Membro alega que se se considerar, em última instância, que a Lei de 2011 é contrária ao direito da União, qualquer declaração que seja dela deduzida pelo órgão jurisdicional de reenvio deverá ter, do ponto de vista dos seus efeitos, eficácia meramente prospetiva.

24 Por seu turno, G.D. alegou que o regime de conservação generalizada e indiferenciada dos dados instituído pela Lei de 2011, bem como o regime de acesso a esses dados previsto por esta lei, são incompatíveis com o direito da União, conforme interpretado em especial pelo Tribunal de Justiça no n.º 120 do Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970).

25 O órgão jurisdicional de reenvio precisa, a título preliminar, que lhe compete apenas apreciar se a High Court (Tribunal Superior) decidiu corretamente que o artigo 6.º, n.º 1, alínea a), da Lei de 2011 é incompatível com o direito da União e que, em contrapartida, a questão da admissibilidade dos meios de prova invocados no âmbito do processo penal é da exclusiva competência da Court of Appeal (Tribunal de Recurso), chamada a decidir o recurso interposto da decisão de condenação.

26 Neste contexto, o órgão jurisdicional de reenvio interroga-se, antes de mais, sobre os requisitos do direito da União no que respeita à conservação dos dados para efeitos de luta contra a criminalidade grave. A este respeito, considera, em substância, que só uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização permite lutar, de modo efetivo, contra a criminalidade grave, o que uma conservação seletiva e uma conservação rápida (*quick freeze*) não permitem fazer. No que respeita à conservação seletiva, o órgão jurisdicional de reenvio interroga-se sobre a possibilidade de visar grupos ou zonas geográficas determinados para efeitos de luta contra a criminalidade grave, na medida em que certas infrações graves raramente implicam circunstâncias conhecidas das autoridades nacionais competentes que lhes permitam suspeitar da prática de uma infração antes de esta ser cometida. Além disso, uma conservação seletiva pode dar lugar a discriminações. Quanto à conservação rápida, o órgão jurisdicional de reenvio considera que esta só é útil em situações em que exista um suspeito identificável numa fase precoce do inquérito.

27 No que respeita, em seguida, ao acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas, o órgão jurisdicional de reenvio sublinha que a Polícia Nacional instituiu, internamente, um mecanismo de autocertificação dos pedidos de acesso dirigidos a esses prestadores. Assim, resulta dos elementos apresentados na High Court (Tribunal Superior) que o chefe da Polícia Nacional decidiu, a título de medida interna, que os pedidos de acesso apresentados ao abrigo da Lei de 2011 devem ser objeto de um tratamento centralizado por um único agente da Polícia Nacional, com a qualidade de superintendente-chefe, ou seja, o chefe do Departamento de Segurança e Informações. Se este último considerar que os dados em causa são necessários para efeitos, nomeadamente, de prevenção, deteção, investigação ou repressão de uma infração grave, pode apresentar um pedido de acesso aos prestadores de serviços de comunicações eletrónicas. Por outro lado, o chefe da Polícia Nacional instituiu, também internamente, uma unidade independente denominada *Telecommunications Liaison Unit* (Unidade de Ligação das Telecomunicações, a seguir «TLU»), a fim de prestar apoio ao chefe do Departamento de Segurança e Informações no exercício das suas funções e de servir de ponto de contacto único com esses mesmos prestadores de serviços.

28 O órgão jurisdicional de reenvio acrescenta que, durante o período abrangido pelo inquérito penal instaurado contra G.D., todos os pedidos de acesso deviam ser aprovados, em primeiro lugar, por um superintendente ou por um inspetor que atuasse nessa qualidade, antes de serem enviados à TLU com vista ao seu tratamento, e que os investigadores eram aconselhados a incluir nos seus pedidos de acesso detalhes suficientes para que pudesse ser tomada uma decisão informada. Além disso, a TLU e o chefe do Departamento de Segurança e Informações eram obrigados a examinar a legalidade, a necessidade e a proporcionalidade dos pedidos de acesso, tendo em conta o facto de

que esse chefe podia ser chamado a responder pela sua decisão perante um juiz designado pela High Court (Tribunal Superior). Por outro lado, a TLU estava sujeita ao controlo do Data Protection Commissioner (Comissário para a Proteção de Dados, Irlanda).

29 Por último, o órgão jurisdicional de reenvio interroga-se sobre o alcance e os efeitos no tempo de uma eventual declaração de não conformidade da Lei de 2011 com o direito da União. A este respeito, precisa que essa declaração só pode ter efeitos prospetivos, pelo facto de os dados utilizados como provas no processo penal conta G.D. terem sido objeto de conservação e de acesso no final de 2013, ou seja num período em que a Irlanda estava obrigada a aplicar as disposições da Lei de 2011 que transpôs a Diretiva 2006/24. Segundo a Irlanda, essa solução também é adequada na medida em que, caso contrário, a investigação e a repressão das infrações graves na Irlanda, bem como a situação das pessoas já julgadas e condenadas, poderiam ser seriamente afetadas.

30 Foi nestas circunstâncias que a Supreme Court (Supremo Tribunal, Irlanda) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Um regime geral ou universal de conservação de dados, ainda que sujeito a limitações estritas em matéria de conservação e acesso, é, em si mesmo, contrário ao disposto no artigo 15.º da Diretiva [2002/58], conforme interpretado à luz da [Carta]?

2) Ao apreciar a eventual incompatibilidade de uma medida nacional implementada nos termos da Diretiva [2006/24], que prevê um regime geral de conservação de dados (sujeito a controlos rigorosos necessários em matéria de conservação e/ou acesso) e, em especial, ao avaliar a proporcionalidade de tal regime, pode um órgão jurisdicional nacional ter em conta o facto de os dados poderem ser licitamente conservados por prestadores de serviços para os seus próprios fins comerciais, e poderem ter de ser conservados por razões de segurança nacional excluídas [do âmbito de aplicação] das disposições da Diretiva [2002/58]?

3) Ao apreciar a eventual compatibilidade de uma medida nacional de acesso a dados conservados com o direito da União e, em especial, com a [Carta], que critérios deve o órgão jurisdicional nacional aplicar para verificar se esse regime de acesso prevê o controlo prévio independente exigido pelo Tribunal de Justiça em conformidade com a sua jurisprudência? Neste contexto, pode um órgão jurisdicional nacional, no âmbito dessa apreciação, ter em conta a existência de um[a] [fiscalização jurisdicional] ou independente *ex post*?

4) Em qualquer caso, está um órgão jurisdicional nacional obrigado a declarar a incompatibilidade de uma medida nacional com o disposto no artigo 15.º da Diretiva [2002/58], se a medida nacional previr um regime geral de conservação de dados com o objetivo de [luta contra a criminalidade grave], e quando o órgão jurisdicional nacional tiver concluído, com base em todos os meios de prova disponíveis, que essa conservação é simultaneamente indispensável e estritamente necessária à concretização do objetivo de [luta contra a criminalidade grave]?

5) Se um órgão jurisdicional nacional se vir obrigado a concluir que uma medida nacional é incompatível com o disposto no artigo 15.º da Diretiva [2002/58], conforme interpretado à luz da [Carta], pode este limitar os efeitos no tempo dessa declaração, caso considere que não fazê-lo redundaria em «caos e prejuízo para o interesse geral» [em consonância com a

abordagem seguida, por exemplo, no processo R (*National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs* [2018] EWHC 975, n.º 46]?

6) Pode um órgão jurisdicional nacional chamado a declarar a incompatibilidade da legislação nacional com o artigo 15.º da Diretiva [2002/58], e/ou a não aplicar essa legislação, e/ou a declarar que a aplicação dessa legislação violou os direitos de um particular, no contexto de um processo instaurado para promover um debate sobre a admissibilidade de meios de prova no âmbito de um processo penal ou noutras circunstâncias, ser autorizado a julgar improcedente essa pretensão no que respeita aos dados conservados em aplicação da disposição nacional adotada ao abrigo da obrigação prevista no artigo 288.º TFUE de transpor fielmente para o direito nacional as disposições de uma diretiva, ou a limitar os efeitos dessa declaração ao período subsequente ao da declaração da invalidade da Diretiva [2006/24] proferida pelo [Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238)]?»

Quanto às questões prejudiciais

Quanto à primeira, segunda e quarta questões

31 Com a primeira, segunda e quarta questões, que importa examinar em conjunto, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional que prevê uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização para efeitos de luta contra a criminalidade grave.

32 Importa recordar, a título preliminar, que é jurisprudência constante que, para interpretar uma disposição do direito da União, há que ter em conta não só os seus termos mas também o seu contexto e os objetivos prosseguidos pela regulamentação de que a mesma faz parte e, nomeadamente, a génese dessa regulamentação (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 105 e jurisprudência referida).

33 Resulta dos próprios termos do artigo 15.º, n.º 1, da Diretiva 2002/58 que as medidas legislativas que esta autoriza os Estados-Membros a adotar, nas condições nela fixadas, apenas podem ter por objetivo «restringir o âmbito» dos direitos e obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58.

34 No que respeita ao sistema instituído por esta diretiva e no qual se insere o seu artigo 15.º, n.º 1, há que recordar que, nos termos do artigo 5.º, n.º 1, primeira e segunda frases, da referida diretiva, os Estados-Membros são obrigados a garantir, através da respetiva legislação nacional, a confidencialidade das comunicações realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis, bem como a confidencialidade dos respetivos dados de tráfego. 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 da mesma diretiva.

35 A este respeito, o Tribunal de Justiça já declarou que o artigo 5.º, n.º 1, da Diretiva 2002/58 consagra o princípio da confidencialidade tanto das comunicações eletrónicas como dos respetivos dados de tráfego e implica, nomeadamente, que, em princípio, pessoas que não os utilizadores estejam proibidas de armazenar, sem o consentimento destes, essas comunicações e esses dados (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 107).

36 Esta disposição reflete o objetivo prosseguido pelo legislador da União quando da adoção da Diretiva 2002/58. Com efeito, 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 setor 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». A referida diretiva tem assim 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 capacidade crescente em termos de armazenamento e de processamento informático de dados. Em particular, como enuncia o considerando 2 da mesma diretiva, a intenção do legislador da União é de assegurar o pleno respeito pelos direitos consignados nos artigos 7.º e 8.º da Carta (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 83, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 106).

37 Assim, ao adotar a Diretiva 2002/58, o legislador da União concretizou estes direitos, pelo que os utilizadores dos meios de comunicações eletrónicos têm o direito de esperar, em princípio, que, caso não tenham dado consentimento, as suas comunicações e respetivos dados permaneçam 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, EU:C:2020:791, n.º 109).

38 No que respeita ao tratamento e ao armazenamento pelos prestadores de serviços de comunicações eletrónicas dos dados de tráfego relativos a assinantes e utilizadores, o artigo 6.º da Diretiva 2002/58 prevê, no seu n.º 1, que esses dados devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação, e precisa, no seu n.º 2, que os dados de tráfego necessários para efeitos de faturação dos assinantes e de pagamento de interligações só podem ser tratados até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado. No que se refere aos dados de localização para além dos dados de tráfego, o artigo 9.º, n.º 1, da referida diretiva estabelece que esses dados só podem ser tratados em determinadas condições e depois de serem tornados anónimos ou com o consentimento dos utilizadores ou assinantes.

39 Por conseguinte, a Diretiva 2002/58 não se limita a enquadrar o acesso a esses dados através de garantias destinadas a prevenir abusos, mas consagra também, em especial, o princípio da proibição do seu armazenamento por terceiros.

40 Na medida em que o artigo 15.º, n.º 1, da Diretiva 2002/58 permite aos Estados-Membros adotar medidas legislativas destinadas a «restringir o âmbito» dos direitos e obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º desta diretiva, como os que decorrem dos princípios da confidencialidade das comunicações e da proibição de armazenamento dos respetivos dados, recordados no n.º 35 do presente acórdão, esta disposição enuncia uma exceção à regra geral

prevista nomeadamente nestes artigos 5.º, 6.º e 9.º e deve, assim, em conformidade com jurisprudência constante, ser objeto de interpretação estrita. Esta disposição não pode, portanto, justificar que a derrogação da 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 em regra, sob pena de esvaziar em grande medida esta última disposição do seu alcance (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 89, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 111).

41 Quanto aos objetivos suscetíveis de justificar uma restrição dos direitos e das obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58, o Tribunal de Justiça já declarou que a enumeração dos objetivos que figuram no artigo 15.º, n.º 1, primeira frase, desta diretiva tem caráter taxativo, de modo que uma medida legislativa adotada ao abrigo desta disposição tem que responder efetiva e estritamente a um desses objetivos (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 112 e jurisprudência referida).

42 Além disso, resulta do artigo 15.º, n.º 1, terceira frase, da Diretiva 2002/58 que as medidas tomadas pelos Estados-Membros ao abrigo desta disposição devem respeitar os princípios gerais do direito da União, entre os quais figura o princípio da proporcionalidade, e assegurar o respeito dos 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, através de uma regulamentação nacional, de conservarem os dados de tráfego para, se for caso disso, os disponibilizarem às autoridades nacionais competentes coloca questões não apenas quanto ao respeito 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 (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C 512/18 e C 520/18, EU:C:2020:791, n.º 113 e jurisprudência referida).

43 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, assim como do direito à liberdade de expressão, direito fundamental, garantido pelo artigo 11.º da Carta, que constitui um dos fundamentos essenciais de uma sociedade democrática e pluralista, fazendo parte dos valores nos quais, em conformidade com o artigo 2.º TUE, se baseia a União (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C 512/18 e C-520/18, EU:C:2020:791, n.º 114 e jurisprudência referida).

44 Importa precisar, a este respeito, que a conservação de dados de tráfego e de dados de localização constitui, em si mesma, por um lado, uma derrogação da proibição, prevista no artigo 5.º, n.º 1, da Diretiva 2002/58, imposta a qualquer pessoa distinta dos utilizadores de armazenar estes dados e, por outro, uma ingerência nos direitos fundamentais do respeito pela vida privada e da proteção dos dados pessoais, consagrados nos artigos 7.º e 8.º da Carta, não sendo importante 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, ou ainda que os dados conservados sejam ou não utilizados posteriormente (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.ºs 115, 116 e jurisprudência referida).

45 Esta conclusão revela-se ainda mais justificada quando os dados de tráfego e os dados de localização são suscetíveis de revelar informações sobre um número significativo de aspetos da vida privada das pessoas em causa, incluindo informações sensíveis, tais como a orientação sexual, as opiniões políticas, as convicções religiosas, filosóficas, sociais ou outras, bem como o estado de saúde, uma vez que tais dados beneficiam, além disso, de uma proteção especial no direito da União. Considerados no seu todo, estes dados podem permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de modo permanente ou temporário, as deslocações diárias ou outras, as atividades exercidas, as relações sociais dessas pessoas e os meios sociais que frequentam. Em especial, estes dados fornecem os meios para determinar o perfil das pessoas em causa, informação tão sensível, à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 117 e jurisprudência referida).

46 Por conseguinte, por um lado, a conservação de dados de tráfego e de dados de localização para fins policiais é suscetível 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 eletrónicos, da sua liberdade de expressão, garantida no artigo 11.º da referida Carta, efeitos estes que são tanto mais graves quanto maiores sejam o número e a variedade dos dados conservados. Por outro lado, tendo em conta a quantidade significativa de dados de tráfego e de dados de localização que podem ser conservados de modo contínuo através de uma medida de conservação generalizada e indiferenciada, assim 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 (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.ºs 118, 119 e jurisprudência referida).

47 A este respeito, há que sublinhar que a conservação destes dados e o acesso aos mesmos constituem, como resulta da jurisprudência recordada no n.º 44 do presente acórdão, ingerências distintas nos direitos fundamentais garantidos nos artigos 7.º e 11.º da Carta, que necessitam de uma justificação distinta, nos termos do artigo 52.º, n.º 1, da mesma. Daqui decorre que uma legislação nacional que assegura o pleno respeito das condições que resultam da jurisprudência que interpretou a Diretiva 2002/58 em matéria de acesso aos dados conservados não pode, por natureza, ser suscetível de restringir nem sequer de corrigir a ingerência grave, que resultaria da conservação generalizada desses dados prevista por esta legislação nacional, nos direitos garantidos nos artigos 6.º e 5.º desta diretiva e pelos direitos fundamentais de que esses artigos constituem a concretização.

48 Não obstante, na medida em que permite aos Estados-Membros restringir os direitos e obrigações referidos nos n.ºs 34 a 37 do presente acórdão, o artigo 15.º, n.º 1, da Diretiva 2002/58 reflete a circunstância de os direitos consagrados nos artigos 7.º, 8.º e 11.º da Carta não serem prerrogativas absolutas, mas deverem ser tomados em consideração relativamente à sua função na sociedade. 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. Assim, a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58 à luz da Carta exige que se tenha em conta igualmente a importância dos direitos consagrados nos artigos 3.º, 4.º, 6.º e 7.º da Carta e a importância dos objetivos de proteção da segurança nacional e de luta contra a criminalidade grave, contribuindo para a proteção dos

direitos e liberdades de terceiros (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.os 120 a 122 e jurisprudência referida).

49 Assim, no que no que diz respeito, em particular, à luta efetiva contra as infrações penais de que são vítimas, nomeadamente, menores e outras pessoas vulneráveis, importa ter em conta o facto de que podem resultar do artigo 7.º da Carta obrigações positivas que incumbem aos poderes públicos, tendo em vista a adoção de medidas jurídicas destinadas a proteger a vida privada e familiar. Tais obrigações são igualmente suscetíveis de decorrer do referido artigo 7.º no que diz respeito à proteção do domicílio e das comunicações, bem como dos artigos 3.º e 4.º, relativos à proteção da integridade física e psíquica das pessoas e à proibição da tortura e dos tratos desumanos e degradantes (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.º 126 e jurisprudência referida).

50 Face a estas diferentes obrigações positivas, há, portanto, que proceder a uma conciliação dos diferentes interesses legítimos e direitos em causa. Com efeito, o Tribunal Europeu dos Direitos do Homem declarou que as obrigações positivas decorrentes dos artigos 3.º e 8.º da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, cujas garantias correspondentes figuram nos artigos 4.º e 7.º da Carta, implicam, nomeadamente, a adoção de disposições materiais e processuais, assim como de medidas de ordem prática que permitam combater eficazmente os crimes contra as pessoas através de uma investigação e de processos efetivos, sendo esta obrigação ainda mais importante quando o bem-estar físico e moral de uma criança é ameaçado. Não obstante, as medidas que cabe às autoridades competentes adotar devem respeitar plenamente as vias de recurso e outras garantias suscetíveis de limitar o âmbito dos poderes de investigações penais e as outras liberdades e direitos. Em particular, segundo esse tribunal, deve instituir-se um quadro jurídico que permita conciliar os diferentes interesses legítimos e direitos a proteger (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 127, 128 e jurisprudência referida).

51 Neste quadro, decorre dos próprios termos do artigo 15.º, n.º 1, primeira frase, da Diretiva 2002/58 que os Estados-Membros podem adotar uma medida derrogatória do princípio da confidencialidade evocado no n.º 35 do presente acórdão quando tal medida seja «necessária, adequada e proporcionada numa sociedade democrática», indicando o considerando 11 desta diretiva, a este respeito, que uma medida desta natureza deve ser «rigorosamente» proporcionada ao objetivo a alcançar (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 129).

52 A este respeito, importa recordar que a proteção do direito fundamental ao respeito da vida privada impõe, em conformidade com a jurisprudência constante do Tribunal de Justiça, que as derrogações à proteção dos dados pessoais e as respetivas restrições ocorram na estrita medida do necessário. Além disso, um objetivo de interesse geral não pode ser prosseguido sem se ter em conta o facto de que deve ser conciliado com os direitos fundamentais abrangidos pela medida, mediante uma ponderação equilibrada entre o objetivo e os interesses e direitos em causa (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 130 e jurisprudência referida).

53 Mais particularmente, decorre da jurisprudência do Tribunal de Justiça que a possibilidade de os Estados-Membros justificarem uma restrição aos direitos e às obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58 deve ser apreciada através da medição da gravidade da ingerência que tal restrição implica e da verificação de que a

importância do objetivo de interesse geral prosseguido por esta restrição está relacionada com essa gravidade (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 131 e jurisprudência referida).

54 Para cumprir a exigência de proporcionalidade, uma legislação nacional 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. Essa legislação 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 maior quando os dados pessoais são sujeitos a um processamento informático, nomeadamente quando existe um risco significativo de acesso ilícito a tais dados. Estas considerações são particularmente válidas quando está em jogo a proteção desta categoria específica de dados pessoais, que são os dados sensíveis (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 132 e jurisprudência referida).

55 Assim, uma legislação nacional que preveja uma conservação dos dados pessoais deve responder sempre a critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido. Em particular, no que respeita à luta contra a criminalidade grave, os dados cuja conservação está prevista devem ser suscetíveis de contribuir para a prevenção, a deteção ou a repressão de infrações graves (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 59, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 133).

56 Relativamente aos objetivos de interesse geral suscetíveis de justificar uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, resulta da jurisprudência do Tribunal de Justiça, em especial do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), que, em conformidade com o princípio da proporcionalidade, existe uma hierarquia entre estes objetivos em função da sua importância respetiva e que a importância do objetivo prosseguido por essa medida deve estar relacionada com a gravidade da ingerência daí resultante.

57 A este respeito, o Tribunal de Justiça declarou que 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, incluindo grave, e de salvaguarda da 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 incluem ingerências nos direitos fundamentais mais graves do que aquelas que esses outros objetivos poderiam justificar (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.ºs 135 e 136).

58 É por este motivo que o Tribunal de Justiça declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º e do artigo 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que permitam, para efeitos de salvaguarda da segurança nacional, impor aos prestadores de serviços de comunicações eletrónicas que procedam a uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, quando o Estado-Membro em causa enfrente uma ameaça grave para a segurança nacional que se revele real e atual ou previsível,

quando a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva quer por um órgão jurisdicional quer por uma entidade administrativa efetiva independente, cuja decisão produza efeitos vinculativos, destinada a verificar a existência de uma dessas situações e o respeito dos requisitos e das garantias que devem estar previstos, e quando a referida imposição apenas possa ser aplicada por um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 168).

59 No que diz respeito ao objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais, o Tribunal de Justiça salientou que, em conformidade com o princípio da proporcionalidade, só a luta contra a criminalidade grave e a prevenção das ameaças graves contra a segurança pública são suscetíveis de justificar ingerências graves nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, tais como as que implicam a conservação de dados de tráfego e de dados de localização. Por conseguinte, só as ingerências sem caráter grave nos referidos direitos fundamentais podem ser justificadas pelo objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral regulamentação em causa no processo principal, de prevenção, de investigação, de deteção e perseguição de infrações penais em geral (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.º 140 e jurisprudência referida).

60 Na audiência, a Comissão Europeia sustentou que a criminalidade particularmente grave pode ser equiparada a uma ameaça para a segurança nacional.

61 Ora, o Tribunal de Justiça já declarou que o objetivo de preservação da segurança nacional corresponde ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da sociedade, através da 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, EU:C:2020:791, n.º 135).

62 Além disso, há que salientar que, diversamente da criminalidade, mesmo particularmente grave, uma ameaça para a segurança nacional deve ser real e atual ou, pelo menos, previsível, o que pressupõe a ocorrência de circunstâncias suficientemente concretas, para poder justificar uma medida de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, durante um período limitado. Essa ameaça distingue-se, portanto, pela sua natureza, a sua gravidade e o caráter específico das circunstâncias que a constituem, do risco geral e permanente de ocorrência de tensões ou de perturbações, ainda que graves, à segurança pública ou do risco de infrações penais graves (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.ºs 136 e 137).

63 Assim, a criminalidade, ainda que particularmente grave, não pode ser equiparada a uma ameaça para a segurança nacional. Com efeito, como salientou o advogado-geral nos n.ºs 49 e 50 das suas conclusões, essa equiparação seria suscetível de introduzir uma categoria intermédia entre a segurança nacional e a segurança pública, para aplicar à segunda as exigências inerentes à primeira.

64 Daqui resulta igualmente que a circunstância, mencionada na segunda questão prejudicial, de os dados de tráfego e de os dados de localização terem sido legalmente objeto de uma conservação para efeitos de salvaguarda da segurança nacional não tem incidência na licitude da sua conservação para efeitos da luta contra a criminalidade grave.

65 No que respeita ao objetivo de luta contra a criminalidade grave, o Tribunal de Justiça declarou que uma legislação nacional que prevê, para este efeito, a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática. Com efeito, tendo em conta o caráter sensível das informações que os dados de tráfego e os dados de localização podem fornecer, a sua confidencialidade é essencial para o direito ao respeito da vida privada. Assim, e atendendo, por um lado, aos efeitos dissuasivos no exercício dos direitos fundamentais consagrados nos artigos 7.º e 11.º da Carta, referidos no n.º 46 do presente acórdão, que a conservação desses dados pode produzir e, por outro, à gravidade da ingerência que tal conservação implica, é necessário, numa sociedade democrática, que esta seja a exceção e não a regra, como prevê o sistema instituído pela Diretiva 2002/58, e que esses dados não possam ser objeto de uma conservação sistemática e contínua. Esta conclusão impõe-se mesmo em relação aos objetivos de luta contra a criminalidade grave e de prevenção das ameaças graves contra a segurança pública, bem como à importância que lhes deve ser reconhecida (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.ºs 141, 142 e jurisprudência referida).

66 Além disso, o Tribunal de Justiça sublinhou que uma legislação nacional que prevê a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização abrange as comunicações eletrónicas de quase toda a população sem que seja estabelecida nenhuma diferenciação, limitação ou exceção em função do objetivo prosseguido. Tal legislação afeta globalmente todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que essas pessoas se encontrem, mesmo indiretamente, numa situação suscetível de justificar um procedimento penal. 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 este objetivo de luta contra os atos de criminalidade grave e, em particular, sem que se estabeleça uma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública. Em particular, como já declarou o Tribunal de Justiça, tal legislação não está limitada a uma conservação que tenha por objeto dados relativos a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de algum modo numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus dados, podiam contribuir para a luta contra a criminalidade grave (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.ºs 143, 144 e jurisprudência referida).

67 Em contrapartida, no n.º 168 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791), o Tribunal de Justiça precisou que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 8.º, 7.º e 11.º e do artigo 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,

— uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

— uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

— uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos; e

— uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida (*quick freeze*) dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem;

desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.

68 No presente pedido prejudicial, que deu entrada no Tribunal de Justiça antes da prolação dos Acórdãos de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), e de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152), o órgão jurisdicional de reenvio considerou, contudo, que só a conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização de dados de tráfego permitia lutar, de maneira efetiva, contra a criminalidade grave. Na audiência de 13 de setembro de 2021, foi defendido, nomeadamente pela Irlanda e pelo Governo francês, que essa conclusão não era infirmada pelo facto de os Estados-Membros poderem recorrer às medidas referidas no número anterior.

69 A este respeito, importa salientar, em primeiro lugar, que a eficácia de processos penais depende geralmente não de um único instrumento de investigação, mas de todos os instrumentos de investigação de que dispõem as autoridades nacionais competentes para esses efeitos.

70 Em segundo lugar, há que sublinhar que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e do artigo 52.º, n.º 1, da Carta, conforme interpretado pela jurisprudência recordada no n.º 67 do presente acórdão, permite que os Estados-Membros adotem, para efeitos da luta contra a criminalidade grave e a prevenção de ameaças graves contra a segurança pública, não só medidas que instituam uma conservação seletiva e uma conservação rápida, mas também medidas que prevejam uma conservação generalizada e indiferenciada, por um lado, de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos e, por outro, de endereços IP atribuídos à fonte de uma ligação.

71 A este respeito, é pacífico que a conservação dos dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicas é suscetível de contribuir para a luta contra a criminalidade grave, desde que esses dados permitam identificar as pessoas que utilizaram esses meios no contexto da preparação ou da prática de um ato de criminalidade grave.

72 Ora, como resulta da jurisprudência resumida no n.º 67 do presente acórdão, a Diretiva 2002/58 não se opõe, para efeitos da luta contra a criminalidade em geral, à conservação generalizada dos dados relativos à identidade civil. Nestas condições, há que precisar que nem esta diretiva nem nenhum outro ato do direito da União se opõem a uma legislação nacional que tenha por objeto a luta contra a criminalidade grave, nos termos da qual a aquisição de um meio de comunicação eletrónica, como um cartão SIM pré-pago, esteja sujeita à verificação de documentos oficiais que

comprovem a identidade do comprador e ao registo, pelo vendedor, das informações daí resultantes, sendo o vendedor obrigado, se for caso disso, a dar acesso a essas informações às autoridades nacionais competentes.

73 Além disso, há que recordar que a conservação generalizada dos endereços IP atribuídos à fonte da ligação constitui uma ingerência grave nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, uma vez que esses endereços IP podem permitir tirar conclusões precisas sobre a vida privada do utilizador do meio de comunicação eletrónica em causa e ter efeitos dissuasivos no exercício da liberdade de expressão garantida no artigo 11.º da mesma. Todavia, no que respeita a essa conservação, o Tribunal de Justiça declarou que, para efeitos da necessária conciliação dos direitos e dos interesses em causa exigida pela jurisprudência referida nos n.os 50 a 53 do presente acórdão, há que ter em conta o facto de, no caso de uma infração cometida em linha e, em especial, no caso da aquisição, da difusão, da transmissão ou da colocação à disposição em linha de pornografia infantil, na aceção do artigo 2.º, alínea c), da Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO 2011, L 335, p. 1), o endereço IP poder constituir o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática dessa infração (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.os 153 e 154).

74 Por conseguinte, o Tribunal de Justiça declarou que essa conservação generalizada e indiferenciada apenas dos endereços IP atribuídos à fonte de uma ligação não se afigura, em princípio, contrária ao artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º da Carta, desde que essa possibilidade esteja sujeita ao estrito respeito das condições materiais e processuais que devem reger a utilização desses dados referidos nos n.os 155 e 156 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791).

75 Em terceiro lugar, no que respeita às medidas legislativas que preveem uma conservação seletiva e uma conservação rápida dos dados de tráfego e dos dados de localização, as indicações que figuram no pedido de decisão prejudicial revelam um entendimento mais estreito do alcance destas medidas do que o acolhido pela jurisprudência recordada no n.º 67 do presente acórdão. Com efeito, embora, em conformidade com o que foi recordado no n.º 40 do presente acórdão, estas medidas de conservação devam apresentar um caráter derrogatório no sistema instituído pela Diretiva 2002/58, esta, lida à luz dos direitos fundamentais consagrados nos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não subordina a possibilidade de impor uma conservação seletiva à condição de serem conhecidos, antecipadamente, os locais suscetíveis de serem a cena de um ato de criminalidade grave nem as pessoas suspeitas de estar implicadas nesse ato. Do mesmo modo, a referida diretiva não exige que a imposição de uma conservação rápida seja limitada a suspeitos identificados previamente a essa imposição.

76 No que respeita, em primeiro lugar, à conservação seletiva, o Tribunal de Justiça declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58 não se opõe a uma legislação nacional baseada em elementos objetivos, que permitam visar, por um lado, as pessoas cujos dados de tráfego e dados de localização são suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, de contribuir para a luta contra a criminalidade grave ou de prevenir um risco grave para a

segurança pública ou ainda um risco para a segurança nacional (Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 111, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 148).

77 O Tribunal de Justiça precisou, a este respeito que, embora esses elementos objetivos possam variar em função de medidas adotadas para efeitos da prevenção, da investigação, da deteção e da repressão da criminalidade grave, as pessoas assim visadas podem ser, nomeadamente, aquelas que foram previamente identificadas, no âmbito dos processos nacionais aplicáveis e com base em elementos objetivos, e não discriminatórios, como uma ameaça para a segurança pública ou para a segurança nacional do Estado-Membro em causa (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 110, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 149).

78 Os Estados-Membros têm assim, nomeadamente, a faculdade de adotar medidas de conservação contra pessoas que, a título dessa identificação, sejam objeto de um inquérito ou de outras medidas de vigilância atuais ou de inscrição no registo criminal nacional que mencione uma condenação anterior por atos de criminalidade grave que possam implicar um risco elevado de reincidência. Ora, quando essa identificação se baseia em elementos objetivos e não discriminatórios, definidos pelo direito nacional, a conservação seletiva dirigida a pessoas assim identificadas é justificada.

79 Por outro lado, uma medida de conservação seletiva dos dados de tráfego e dos dados de localização pode, segundo a escolha do legislador nacional e no estrito respeito do princípio da proporcionalidade, assentar igualmente num critério geográfico quando as autoridades nacionais competentes considerem, com base em elementos objetivos e não discriminatórios, que existe, numa ou em várias zonas geográficas, uma situação caracterizada por um risco elevado de preparação ou de prática de atos de criminalidade grave. Essas zonas podem ser, nomeadamente, locais caracterizados por um elevado número de atos de criminalidade grave, locais particularmente expostos à prática de atos de criminalidade grave, tais como locais ou infraestruturas frequentados regularmente por um número muito grande de pessoas, ou ainda locais estratégicos, como aeroportos, estações ou zonas de portagens (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 150 e jurisprudência referida).

80 Importa sublinhar que, segundo esta jurisprudência, as autoridades nacionais competentes podem adotar, relativamente às zonas referidas no número anterior, uma medida de conservação seletiva baseada num critério geográfico, como, nomeadamente, a taxa média de criminalidade numa zona geográfica, sem disporem necessariamente de indícios concretos relativos à preparação ou à prática, nas zonas em causa, de atos de criminalidade grave. Na medida em que uma conservação seletiva baseada nesse critério é suscetível de afetar, em função das infrações penais graves visadas e da situação específica dos respetivos Estados-Membros, simultaneamente locais caracterizados por um elevado número de atos de criminalidade grave e locais particularmente expostos à prática de tais atos, também não é, em princípio, suscetível de dar lugar a discriminações, uma vez que o critério relativo à taxa média de criminalidade grave não apresenta, por si só, nenhuma ligação com elementos potencialmente discriminatórios.

81 Além disso, e sobretudo, uma medida de conservação seletiva dirigida a locais ou infraestruturas regularmente frequentados por um número muito elevado de pessoas ou a locais estratégicos, como aeroportos, estações, portos marítimos ou zonas de portagens, permite às autoridades

competentes recolher dados de tráfego e, nomeadamente, dados de localização de todas as pessoas que utilizam, num determinado momento, um meio de comunicação eletrónica num desses locais. Assim, essa medida de conservação seletiva é suscetível de permitir às referidas autoridades obter, através do acesso aos dados assim conservados, informações sobre a presença dessas pessoas nos locais ou nas zonas geográficas visados por essa medida, bem como sobre as suas deslocações entre ou no interior destes e daí retirar, para efeitos da luta contra a criminalidade grave, conclusões sobre a sua presença e a sua atividade nesses locais ou zonas geográficas num dado momento durante o período de conservação.

82 Importa ainda salientar que as zonas geográficas visadas por essa conservação seletiva podem e, se for caso disso, devem ser alteradas em função da evolução das condições que justificaram a sua seleção, permitindo assim, nomeadamente, reagir às evoluções da luta contra a criminalidade grave. Com efeito, o Tribunal de Justiça já declarou que a duração das medidas de conservação seletiva descritas nos n.os 76 a 81 do presente acórdão não pode ultrapassar a estritamente necessária à luz do objetivo prosseguido e das circunstâncias que as justificam, sem prejuízo de uma eventual renovação devido ao facto de continuar a ser necessário proceder a essa conservação (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 151).

83 No que respeita à possibilidade de prever critérios distintivos diferentes de um critério pessoal ou geográfico para aplicar uma conservação seletiva dos dados de tráfego e dos dados de localização, não se pode excluir que outros critérios, objetivos e não discriminatórios, possam entrar em linha de conta para garantir que o âmbito de uma conservação seletiva se limite ao estritamente necessário e estabelecer uma ligação, pelo menos indireta, entre os atos de criminalidade grave e as pessoas cujos dados são conservados. Não obstante, uma vez que o artigo 15.º, n.º 1, da Diretiva 2002/58 visa medidas legislativas dos Estados-Membros, é a estes últimos e não ao Tribunal de Justiça que incumbe identificar esses critérios, entendendo-se que não pode ser reinstituída por este meio uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização.

84 Em todo o caso, como salientou o advogado-geral M. Campos Sánchez-Bordona no n.º 50 das suas Conclusões nos processos apensos SpaceNet e Telekom Deutschland (C-793/19 e C-794/19, EU:C:2021:939), a eventual existência de dificuldades para definir precisamente as hipóteses e as condições em que pode ser efetuada uma conservação seletiva não pode justificar que os Estados-Membros, fazendo da exceção uma regra, prevejam uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização.

85 Em segundo lugar, no que diz respeito à conservação rápida dos dados de tráfego e dos dados de localização tratados e armazenados pelos prestadores de serviços de comunicações eletrónicas com base nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58, ou nas medidas legislativas adotadas ao abrigo do artigo 15.º, n.º 1, desta diretiva, importa recordar que esses dados devem ser, em princípio, consoante o caso, apagados ou tornados anónimos no termo dos prazos legais em que devem ser realizados, em conformidade com as disposições nacionais que transpõem essa diretiva, o seu tratamento e a sua armazenagem. No entanto, o Tribunal de Justiça declarou que, durante esse tratamento e essa armazenagem, podem ocorrer situações em que é necessário conservar os referidos dados para além desses prazos para efeitos do esclarecimento de infrações penais graves ou de ofensas à segurança nacional, tanto na situação em que essas infrações ou essas ofensas já foram detetadas como na situação em que, após uma apreciação objetiva de todas

as circunstâncias pertinentes, se pode razoavelmente suspeitar da sua existência (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 160 e 161).

86 Nessa situação, os Estados-Membros podem, tendo em conta a necessária conciliação dos direitos e interesses legítimos em causa referida nos n.os 50 a 53 do presente acórdão, prever, numa legislação adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, a possibilidade, através de uma decisão da autoridade competente sujeita a uma fiscalização jurisdicional efetiva, de impor aos prestadores de serviços de comunicações eletrónicas o dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que dispõem.

87 Na medida em que a finalidade de tal conservação rápida deixe de corresponder às finalidades para as quais os dados foram inicialmente recolhidos e conservados e na medida em que qualquer tratamento de dados deve, nos termos do artigo 8.º, n.º 2, da Carta, responder a determinados objetivos, os Estados-Membros devem precisar, na sua legislação, a finalidade que justifica a conservação rápida de dados. Tendo em conta o caráter grave da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que tal conservação pode comportar, só a luta contra a criminalidade grave e, *a fortiori*, a salvaguarda da segurança nacional são suscetíveis de justificar essa ingerência, desde que essa medida e o acesso aos dados assim conservados respeitem os limites do estritamente necessário, conforme enunciados nos n.os 164 a 167 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791).

88 O Tribunal de Justiça precisou que uma medida de conservação desta natureza não deve ser limitada aos dados das pessoas identificadas previamente como apresentando uma ameaça para a segurança pública ou para a segurança nacional do Estado-Membro em causa ou das pessoas concretamente suspeitas de terem praticado um ato de criminalidade grave ou uma ofensa à segurança nacional. Com efeito, segundo o Tribunal de Justiça, embora deva respeitar o quadro instituído pelo artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, e tendo em conta as considerações que figuram no n.º 55 do presente acórdão, tal medida pode, se for essa a escolha do legislador e respeitando os limites do estritamente necessário, ser alargada aos dados de tráfego e aos dados de localização relativos a pessoas diferentes das que são suspeitas de ter planeado ou cometido uma infração grave ou uma ofensa à segurança nacional, desde que tais dados possam, com base em elementos objetivos e não discriminatórios, contribuir para o esclarecimento dessa infração ou dessa ofensa à segurança nacional, tais como os dados da vítima desta e do seu meio social ou profissional (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 165).

89 Assim, uma medida legislativa pode autorizar que se imponha aos prestadores de serviços de comunicações eletrónicas a conservação rápida dos dados de tráfego e dos dados de localização, nomeadamente, das pessoas com as quais, antes da ocorrência de uma ameaça grave para a segurança pública ou da prática de um ato de criminalidade grave, uma vítima tenha estado em contacto utilizando os seus meios de comunicações eletrónicas.

90 Tal conservação rápida pode, segundo a jurisprudência do Tribunal de Justiça recordada no n.º 88 do presente acórdão e nas mesmas condições visadas nesse número, igualmente ser alargada a zonas geográficas determinadas, como os locais da prática e da preparação da infração ou da ofensa à segurança nacional em causa. Importa precisar que podem ainda ser objeto dessa medida os dados de tráfego e os dados de localização relativos ao local onde uma pessoa,

potencialmente vítima de um ato de criminalidade grave, desapareceu, desde que essa medida e o acesso aos dados assim conservados respeitem os limites do estritamente necessário para efeitos da luta contra a criminalidade grave ou a salvaguarda da segurança nacional, conforme enunciados nos n.os 164 a 167 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791).

91 Por outro lado, importa precisar que o artigo 15.º, n.º 1, da Diretiva 2002/58 não se opõe a que as autoridades nacionais competentes ordenem uma medida de conservação rápida desde a primeira fase do inquérito sobre uma ameaça grave para a segurança pública ou sobre um eventual ato de criminalidade grave, a saber, a partir do momento em que, segundo as disposições pertinentes do direito nacional, essas autoridades podem dar início a esse inquérito.

92 No que respeita à variedade das medidas de conservação dos dados de tráfego e dos dados de localização referidos no n.º 67 do presente acórdão, importa precisar que estas diferentes medidas podem, consoante a escolha do legislador nacional e respeitando os limites do estritamente necessário, ser aplicadas conjuntamente. Nestas condições, o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, conforme interpretado pela jurisprudência decorrente do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), não se opõe a uma combinação destas medidas.

93 Em quarto e último lugar, importa sublinhar que a proporcionalidade das medidas adotadas ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58 exige, segundo a jurisprudência constante do Tribunal de Justiça, como recapitulada no Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), o respeito não apenas dos requisitos de adequação e de necessidade, como também do requisito relativo ao caráter proporcional destas medidas relativamente ao objetivo prosseguido.

94 Neste contexto, há que recordar que, no n.º 51 do seu Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238), o Tribunal de Justiça declarou que, embora a luta contra a criminalidade grave tenha uma importância primordial para garantir a segurança pública e embora a sua eficácia possa depender em larga medida da utilização das técnicas modernas de investigação, esse objetivo de interesse geral, por muito fundamental que seja, não pode, por si só, justificar que uma medida de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, como a que foi instituída pela Diretiva 2006/24, seja considerada necessária.

95 No mesmo sentido, o Tribunal de Justiça precisou, no n.º 145 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), que mesmo as obrigações positivas dos Estados-Membros que possam decorrer, consoante o caso, dos artigos 3.º, 4.º e 7.º da Carta e relativas, conforme referido no n.º 49 do presente acórdão, à aplicação de regras que permitem uma luta efetiva contra as infrações penais não podem justificar ingerências tão graves como as que comporta uma legislação nacional que prevê uma conservação de dados de tráfego e de dados de localização nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta de quase toda a população, sem que os dados das pessoas em causa sejam suscetíveis de revelar uma ligação, no mínimo indireta, com o objetivo prosseguido.

96 Na audiência, o Governo dinamarquês sustentou que as autoridades nacionais competentes deveriam poder aceder, para efeitos da luta contra a criminalidade grave, aos dados de tráfego e aos dados de localização que foram conservados de maneira generalizada e indiferenciada, em

conformidade com a jurisprudência decorrente do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 135 a 139), para dar resposta a uma ameaça grave para a segurança nacional que se revele real e atual ou previsível.

97 Importa, desde logo, salientar que o facto de autorizar o acesso, para efeitos da luta contra a criminalidade grave, a dados de tráfego e a dados de localização que foram conservados de maneira generalizada e indiferenciada faz depender esse acesso de circunstâncias alheias a esse objetivo, em função da existência ou não, no Estado-Membro em causa, de uma ameaça grave para a segurança nacional conforme referida no número anterior, quando, à luz apenas do objetivo de luta contra a criminalidade grave que deve justificar a conservação desses dados e o acesso aos mesmos, nada justifica uma diferença de tratamento, em particular entre os Estados-Membros.

98 Como o Tribunal de Justiça já declarou, o acesso a dados de tráfego e a dados de localização conservados pelos prestadores em aplicação de uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, que deve ser efetuado no pleno respeito das condições resultantes da jurisprudência que interpretou a Diretiva 2002/58, apenas pode, em princípio, ser justificado pelo objetivo de interesse geral pelo qual essa conservação foi imposta a esses prestadores. Só assim não será se a importância do objetivo prosseguido pelo acesso ultrapassar a do objetivo que justificou a conservação (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 165 e 166).

99 Ora, a argumentação do Governo dinamarquês visa uma situação em que o objetivo do pedido de acesso pretendido, a saber a luta contra a criminalidade grave, é de menor importância, na hierarquia dos objetivos de interesse geral, do que o que justificou a conservação, a saber a salvaguarda da segurança nacional. Autorizar, em tal situação, um acesso aos dados conservados iria contra essa hierarquia dos objetivos de interesse geral recordada no número anterior e nos n.os 53, 56, 57 e 59 do presente acórdão.

100 Além disso, e sobretudo, em conformidade com a jurisprudência recordada no n.º 65 do presente acórdão, os dados de tráfego e os dados de localização não podem ser objeto de uma conservação generalizada e indiferenciada para efeitos da luta contra a criminalidade grave e, portanto, um acesso a esses dados não pode ser justificado para esses mesmos efeitos. Ora, quando esses dados foram excecionalmente conservados de maneira generalizada e indiferenciada, para efeitos de salvaguarda da segurança nacional contra uma ameaça que se revela real e atual ou previsível, nas condições referidas no n.º 58 do presente acórdão, as autoridades nacionais competentes em matéria de investigações penais não podem aceder aos referidos dados no âmbito de ações penais, sob pena de privar de qualquer efeito útil a proibição de proceder a essa conservação para efeitos da luta contra a criminalidade grave, recordada no referido n.º 65.

101 Tendo em conta todas as considerações precedentes, há que responder à primeira, segunda e quarta questões que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a medidas legislativas que preveem, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização. Em contrapartida, o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,

— uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

— uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

— uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos; e

— uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem;

desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.

Quanto à terceira questão

102 Com a sua terceira questão, 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, 8.º, 11.º e 52.º, n.º l, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados, que emanam da polícia no âmbito da investigação e da repressão de infrações penais graves, incumbe a um agente de polícia, assistido por uma unidade instituída no âmbito da polícia que goza de um certo grau de autonomia no exercício da sua missão e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional.

103 A título preliminar, importa recordar que, embora caiba ao direito nacional determinar as condições em que os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes o acesso aos dados de que dispõem, uma legislação nacional deve, para satisfazer a exigência de proporcionalidade, conforme recordada no n.º 54 do presente acórdão, prever regras claras e precisas que regulem o alcance e a aplicação da medida em causa e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente esses dados contra os riscos de abuso [v., neste sentido, Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 48 e jurisprudência referida].

104 Em especial, uma legislação nacional que regula o acesso das autoridades competentes a dados de tráfego e a dados de localização conservados, adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, não se pode limitar a exigir que o acesso das autoridades aos dados responda à finalidade prosseguida por essa legislação, mas deve igualmente prever as condições materiais e processuais que regem essa utilização [Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 49 e jurisprudência referida].

105 Assim, quando um acesso geral a todos os dados conservados, independentemente de qualquer ligação, no mínimo indireta, com o objetivo prosseguido, não puder ser considerado limitado ao estritamente necessário, a legislação nacional em causa deve basear-se em critérios objetivos para definir as circunstâncias e as condições em que o acesso aos dados em causa deve ser concedido às autoridades nacionais competentes. A este respeito, tal acesso só poderá, em princípio, ser concedido, em relação com o objetivo de luta contra a criminalidade, aos dados de pessoas que se suspeita estarem a planear, a cometer ou terem cometido uma infração grave ou, ainda, estarem envolvidas de uma maneira ou de outra nessa infração. Todavia, em situações especiais, como aquelas em que os interesses vitais da segurança nacional, da defesa ou da segurança pública sejam ameaçados por atividades terroristas, o acesso aos dados de outras pessoas poderá igualmente ser concedido quando existam elementos objetivos que permitam considerar que esses dados poderiam, num caso concreto, contribuir efetivamente para a luta contra essas atividades [Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 50 e jurisprudência referida].

106 A fim de garantir, na prática, o pleno respeito destas condições, é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente e que a decisão desse órgão jurisdicional ou dessa entidade seja tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal [Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 51 e jurisprudência referida].

107 Esse controlo prévio exige, designadamente, que o órgão jurisdicional ou a entidade administrativa independente encarregada de o efetuar disponha de todas as atribuições e apresente todas as garantias necessárias com vista a assegurar uma conciliação dos diferentes interesses e direitos em causa. No que respeita, mais especificamente, a um inquérito penal, tal controlo exige que esse órgão jurisdicional ou essa entidade possa assegurar um justo equilíbrio entre, por um lado, os interesses legítimos ligados às necessidades do inquérito no âmbito da luta contra a criminalidade e, por outro, os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas às quais o acesso diz respeito [Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 52].

108 Quando esse controlo não é efetuado por um órgão jurisdicional, mas por uma entidade administrativa independente, esta deve gozar de um estatuto que lhe permita agir, quando desempenha as suas missões, de maneira objetiva e imparcial, devendo, para esse efeito, estar ao abrigo de qualquer influência externa. Assim, a exigência de independência que deve satisfazer a entidade encarregada de exercer o controlo prévio impõe que esta tenha a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, de modo a que a referida entidade possa exercer esse controlo de maneira objetiva e imparcial, ao abrigo de qualquer influência externa. Em especial, no domínio penal, a exigência de independência implica que a autoridade encarregada desse controlo prévio, por um lado, não esteja implicada na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal [v., neste sentido, Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.ºs 53 e 54].

109 Assim, o Tribunal de Justiça considerou, nomeadamente, que não se pode reconhecer a um Ministério Público que dirige o processo de inquérito e exerce, sendo caso disso, a ação pública, a qualidade de terceiro em relação aos interesses legítimos em causa, uma vez que o mesmo não tem por missão decidir com total independência um litígio, mas submetê-lo, sendo caso disso, ao órgão jurisdicional competente, enquanto parte no processo que exerce a ação penal. Por conseguinte, esse Ministério Público não está em condições de efetuar o controlo prévio dos pedidos de acesso aos dados conservados [v., neste sentido, Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.os 55 e 57].

110 Por último, o controlo independente exigido em conformidade com o artigo 15.º, n.º 1, da Diretiva 2002/58 deve ser efetuado previamente a qualquer acesso aos dados em causa, salvo em caso de urgência devidamente justificada, devendo, nesse caso, o controlo ser efetuado em prazos curtos. Com efeito, um controlo posterior não permitiria responder ao objetivo de um controlo prévio, que consiste em impedir que seja autorizado um acesso aos dados em causa que ultrapasse os limites do estritamente necessário [v., neste sentido, Acórdãos de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 189, e de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 58].

111 No caso em apreço, resulta, desde logo, do pedido de decisão prejudicial que a Lei de 2011 atribui a um agente de polícia, cuja posição não seja inferior à de superintendente chefe, a competência para exercer o controlo prévio dos pedidos de acesso aos dados que emanam dos serviços de investigação policial e para solicitar aos prestadores de serviços de comunicações eletrónicas que lhe comuniquem os dados por eles conservados. Na medida em que este agente não tem a qualidade de terceiro em relação a esses serviços, não cumpre as exigências de independência e de imparcialidade recordadas no n.º 108 do presente acórdão, não obstante a circunstância de ser assistido nessa missão por uma unidade da polícia, neste caso, a TLU, que beneficia de um certo grau de autonomia no exercício da sua missão.

112 Em seguida, embora seja verdade que a Lei de 2011 prevê mecanismos de fiscalização *ex post* da decisão do agente de polícia competente, sob a forma de um procedimento de reclamação e de um processo perante um juiz encarregado de verificar a aplicação das disposições da referida lei, resulta da jurisprudência recordada no n.º 110 do presente acórdão que uma fiscalização exercida *ex post* não pode substituir a exigência, recordada no n.º 106 do presente acórdão, de controlo independente e, salvo caso de urgência devidamente justificada, prévio.

113 Por último, a Lei de 2011 não prevê critérios objetivos que definam com precisão as condições e as circunstâncias em que deve ser concedido às autoridades nacionais o acesso aos dados, uma vez que o agente de polícia encarregado do tratamento dos pedidos de acesso aos dados conservados é o único competente, conforme confirmou a Irlanda na audiência, para apreciar as suspeitas que recaem sobre as pessoas em causa e a necessidade de um acesso aos dados relativos a estas últimas.

114 Por conseguinte, há que responder à terceira questão que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º l, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas, que emanam da polícia no âmbito da investigação e da repressão de infrações penais graves, incumbe a um agente

de polícia, assistido por uma unidade instituída no âmbito da polícia que goza de um certo grau de autonomia no exercício da sua missão e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional.

Quanto à quinta e sexta questões

115 Com a quinta e sexta questões, que devem ser examinadas em conjunto, o órgão jurisdicional de reenvio pretende saber, em substância, se o direito da União deve ser interpretado no sentido de que um órgão jurisdicional nacional pode limitar no tempo os efeitos de uma declaração de invalidade, que lhe incumbe por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz da Carta.

116 Resulta das informações fornecidas pelo órgão jurisdicional de reenvio que a legislação nacional em causa no processo principal, a saber, a Lei de 2011, foi adotada para transpor para o direito nacional a Diretiva 2006/24, que foi posteriormente declarada inválida pelo Tribunal de Justiça no seu Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238).

117 Além disso, o órgão jurisdicional de reenvio salienta que, embora o exame da admissibilidade dos meios de prova baseados em dados conservados ao abrigo da Lei de 2011 e invocados contra G.D. no âmbito do processo penal incumba ao juiz penal, é, no entanto, a ele que cabe decidir, no âmbito da ação cível, sobre a validade das disposições em causa desta lei e sobre os efeitos no tempo de uma declaração de invalidade das mesmas. Assim, embora a única questão que se coloca ao órgão jurisdicional de reenvio seja a da validade das disposições da Lei de 2011, o referido órgão jurisdicional considera, todavia, necessário interrogar o Tribunal de Justiça quanto à incidência de uma eventual declaração de invalidade sobre a admissibilidade dos meios de prova obtidos através da conservação generalizada e indiferenciada dos dados que esta lei permitiu.

118 A título preliminar, importa recordar que o princípio do primado do direito da União consagra a prevalência do direito da União sobre o direito dos Estados-Membros. Este princípio impõe, assim, a todas as instâncias dos Estados-Membros que confiram pleno efeito às diferentes disposições do direito da União, não podendo o direito dos Estados-Membros afetar o efeito reconhecido a essas disposições no território dos referidos Estados. Por força deste princípio, na impossibilidade de proceder a uma interpretação da legislação nacional conforme com as exigências do direito da União, o juiz nacional encarregado de aplicar, no âmbito da sua competência, as disposições do direito da União tem a obrigação de garantir o pleno efeito das mesmas, não aplicando, se necessário e por sua própria iniciativa, qualquer disposição contrária da legislação nacional, mesmo que posterior, sem ter de pedir ou de esperar pela sua revogação prévia por via legislativa ou por qualquer outro procedimento constitucional [v., neste sentido, Acórdãos de 15 de julho de 1964, Costa, 6/64, EU:C:1964:66, pp. 1159 e 1160; de 19 de novembro de 2019, A. K. e o. (Independência da Secção Disciplinar do Supremo Tribunal), C-585/18, C-624/18 e C-625/18, EU:C:2019:982, n.os 157, 158 e 160; e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 214 e 215].

119 Só o Tribunal de Justiça pode, a título excecional e com base em considerações imperiosas de segurança jurídica, conceder uma suspensão provisória do efeito de exclusão exercido por uma regra do direito da União relativamente ao direito nacional a ela contrário. Essa limitação no tempo dos efeitos da interpretação deste direito dada pelo Tribunal de Justiça apenas pode ser

concedida no próprio acórdão que decide sobre a interpretação pedida. O primado e a aplicação uniforme do direito da União ficariam comprometidos se os órgãos jurisdicionais nacionais pudessem, ainda que a título provisório, dar primazia às disposições nacionais sobre o direito da União (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 216, 217 e jurisprudência referida).

120 É certo que o Tribunal de Justiça considerou, num processo em que estava em causa a legalidade de medidas adotadas em violação da obrigação, imposta pelo direito da União, de ser efetuada uma avaliação prévia das incidências de um projeto sobre o ambiente e sobre um sítio protegido, que um órgão jurisdicional nacional pode, se o direito interno o permitir, excecionalmente manter os efeitos de medidas se essa manutenção for justificada por considerações imperiosas ligadas à necessidade de afastar uma ameaça real e grave de rutura do abastecimento em eletricidade do Estado-Membro em causa, à qual não se pode fazer face por outros meios e alternativas, nomeadamente no âmbito do mercado interno, só podendo a referida manutenção abranger o período de tempo estritamente necessário para sanar essa ilegalidade (v., neste sentido, Acórdão de 29 de julho de 2019, Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, n.os 175, 176, 179 e 181).

121 Ora, contrariamente à omissão de uma obrigação processual como a avaliação prévia das incidências de um projeto, que se inscreve no domínio específico da proteção do ambiente, uma violação do artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não pode ser objeto de regularização por meio de um procedimento comparável ao mencionado no número anterior (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 219).

122 Com efeito, a manutenção dos efeitos de uma legislação nacional como a Lei de 2011 significaria que esta legislação continua a impor aos prestadores de serviços de comunicações eletrónicas obrigações contrárias ao direito da União e que comportam ingerências graves nos direitos fundamentais das pessoas cujos dados foram conservados (v., por analogia, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 219).

123 Por conseguinte, o órgão jurisdicional de reenvio não pode limitar no tempo os efeitos de uma declaração de ilegalidade que lhe compete, por força do direito nacional, da legislação nacional em causa no processo principal (v., por analogia, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 220).

124 A este respeito, conforme salientou o advogado-geral, em substância, no n.º 75 das suas conclusões, a circunstância de esta legislação nacional ter sido adotada para efeitos de transposição para o direito nacional da Diretiva 2006/24 não é pertinente, dado que, em razão da invalidação desta diretiva pelo Tribunal de Justiça, invalidação cujos efeitos remontam à data da sua entrada em vigor (v., neste sentido, Acórdão de 8 de fevereiro de 1996, FMC e o., C-212/94, EU:C:1996:40, n.º 55), a validade desta legislação nacional deve ser apreciada pelo órgão jurisdicional de reenvio à luz da Diretiva 2002/58 e da Carta, conforme interpretadas pelo Tribunal de Justiça.

125 No que respeita, mais especificamente, à interpretação da Diretiva 2002/58 e da Carta adotada pelo Tribunal de Justiça nomeadamente nos seus Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970), e de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), há que recordar que,

segundo jurisprudência constante, a interpretação que o Tribunal de Justiça faz de uma regra do direito da União, no exercício da competência que lhe é conferida pelo artigo 267.º TFUE, clarifica e precisa o significado e o alcance dessa regra, tal como deve ou deveria ter sido entendida e aplicada desde a data da sua entrada em vigor. Daqui decorre que a regra assim interpretada pode e deve ser aplicada a relações jurídicas surgidas e constituídas antes do acórdão que se pronuncia sobre o pedido de interpretação, se estiverem também reunidas as condições que permitem submeter aos órgãos jurisdicionais competentes um litígio relativo à aplicação da referida regra (Acórdão de 16 de setembro de 2020, Romenergo e Aris Capital, C-339/19, EU:C:2020:709, n.º 47 e jurisprudência referida).

126 A este respeito, importa ainda precisar que não se procedeu a uma limitação no tempo dos efeitos da interpretação adotada nos Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970), e de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), pelo que, em conformidade com a jurisprudência recordada no n.º 119 do presente acórdão, a mesma não pode ter lugar num acórdão do Tribunal de Justiça posterior a eles.

127 Por último, no que respeita à incidência da constatação da eventual incompatibilidade da Lei de 2011 com a Diretiva 2002/58, lida à luz da Carta, na admissibilidade das provas apresentadas contra G.D. no âmbito do processo penal, basta remeter para a jurisprudência do Tribunal de Justiça a ela relativa, em particular para os princípios recordados nos n.os 41 a 44 do Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152), do qual decorre que esta admissibilidade cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade.

128 Tendo em conta as considerações precedentes, há que responder à quinta e sexta questões que o direito da União deve ser interpretado no sentido de que se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe, por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz da Carta. A admissibilidade dos meios de prova obtidos através dessa conservação cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade.

Quanto às despesas

129 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 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º, 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 medidas legislativas que preveem, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização. Em contrapartida, o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,**

   — **uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;**

   — **uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;**

   — **uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos; e**

   — **uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem,**

   desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.

2) **O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas, que emanam da polícia no âmbito da investigação e da repressão de infrações penais graves, incumbe a um agente de polícia, assistido por uma unidade instituída no âmbito da polícia que goza de um certo grau de autonomia no exercício da sua missão e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional.**

3) **O direito da União deve ser interpretado no sentido de que se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe, por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com o artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz da Carta dos Direitos Fundamentais. A admissibilidade dos meios de prova obtidos através dessa conservação cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade.**

Assinaturas