Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

6 de outubro de 2020*

[Texto retificado por Despacho de 16 de novembro de 2020]

Índice

Quadro jurídico 6
Direito da União 6
Diretiva 95/46 6
Diretiva 97/66 7
Diretiva 2000/31 7
Diretiva 2002/21 9
Diretiva 2002/58 9
Regulamento 2016/679 13
Direito francês 17
Código da Segurança Interna 17
CPCE 22
Lei n.º 2004-575, de 21 de junho de 2004, relativa à Confiança na Economia Digital 24
Decreto n.º 2011-219 25
Direito belga 26
Litígios no processo principal e questões prejudiciais 28
Processo C-511/18 28
Processo C-512/18 31

* Língua do processo: francês.

Processo C-520/18 32

Tramitação do processo no Tribunal de Justiça 34

Quanto às questões prejudiciais 34

Quanto às primeiras questões nos processos C-511/18 e C-512/18 e quanto à primeira e segunda questões no processo C-520/18 34

Observações preliminares 34

Quanto ao âmbito de aplicação da Diretiva 2002/58 35

Quanto à interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58 38

— Quanto às medidas legislativas que preveem a conservação preventiva de dados de tráfego e de dados de localização para efeitos da salvaguarda da segurança nacional 43

— Quanto às medidas legislativas que preveem a conservação preventiva de dados de tráfego e de dados de localização para efeitos da luta contra a criminalidade e da salvaguarda da segurança pública 44

— Quanto às medidas legislativas que preveem a conservação preventiva dos endereços IP e dos dados relativos à identidade civil para efeitos da luta contra a criminalidade e da salvaguarda da segurança pública 46

— Quanto às medidas legislativas que preveem a conservação rápida de dados de tráfego e de dados de localização para efeitos da luta contra a criminalidade grave 48

Quanto à segunda e terceira questões no processo C-511/18 50

Quanto à análise automatizada de dados de tráfego e de dados de localização 51

Quanto à recolha em tempo real de dados de tráfego e de dados de localização 53

Quanto à informação das pessoas cujos dados foram recolhidos ou analisados 54

Quanto à segunda questão no processo C-512/18 55

Quanto à terceira questão no processo C-520/18 58

Quanto às despesas 61

«Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Prestadores de serviços de comunicações eletrónicas — Prestadores de serviços de armazenamento e fornecedores de acesso à Internet — Conservação generalizada e indiferenciada de dados de tráfego e de dados de localização — Análise automatizada de dados — Acesso em tempo real aos dados — Salvaguarda da segurança nacional e luta contra o terrorismo — Luta contra a criminalidade — Diretiva 2002/58/CE — Âmbito de aplicação — Artigo 1.º, n.º 3, e artigo 3.º — Confidencialidade das comunicações eletrónicas — Proteção — Artigo 5.º e artigo 15.º, n.º 1 — Diretiva 2000/31/CE — Âmbito de aplicação — Carta dos Direitos Fundamentais da União Europeia — Artigos 4.º, 6.º a 8.º e 11.º e artigo 52.º, n.º 1 — Artigo 4.º, n.º 2, TUE»

Nos processos apensos C-511/18, C-512/18 e C-520/18,

que têm por objeto pedidos de decisão prejudicial nos termos do artigo 267.º TFUE, apresentados pelo Conseil d'État [Conselho de Estado, em formação jurisdicional, França], por Decisões de 26 de julho de 2018, entradas no Tribunal de Justiça em 3 de agosto de 2018 (C-511/18 e C-512/18), e pela Cour constitutionnelle [Tribunal Constitucional, Bélgica], por Decisão de 19 de julho de 2018, entrada no Tribunal de Justiça em 2 de agosto de 2018 (C-520/18), nos processos

La Quadrature du Net (C-511/18 e C-512/18),

French Data Network (C-511/18 e C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 e C-512/18),

Igwan.net (C-511/18),

contra

Premier ministre (C-511/18 e C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 e C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), sendo intervenientes:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

e

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

contra

Conseil des ministres,

sendo intervenientes:

Child Focus (C-520/18),

O TRIBUNAL DE JUSTIÇA (Grande Secção),

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

advogado-geral: M. Campos Sánchez-Bordona,

secretário: C. Strömholm, administradora,

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

vistas as observações apresentadas:

– em representação da Quadrature du Net, da Fédération des fournisseurs d'accès à Internet associatifs, da Igwan.net e do Center for Democracy and Technology, por A. Fitzjean Ò Cobhthaigh, avocat,

– em representação da French Data Network, por Y. Padova, avocat,

– em representação da Privacy International, H. Roy, avocat,

– em representação da Ordre des barreaux francophones et germanophone, por E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart e J.-F. Henrotte, avocats,

– em representação da Académie Fiscale ASBL e UA, por J.-P. Riquet,

– em representação da Liga voor Mensenrechten ASBL, por J. Vander Velpen, avocat,

– em representação da Ligue des Droits de l'Homme ASBL, por R. Jespers e J. Fermon, avocats,

– em representação de VZ, WY e XX, por D. Pattyn, avocat,

– em representação da Child Focus, por N. Buisseret, K. De Meester e J. Van Cauter, avocat,

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

– em representação do Governo belga, por J.-C. Halleux, P. Cottin e C. Pochet, na qualidade de agentes, assistidos por J. Vanpraet, Y. Peeters, S. Depré e E. de Lophem, avocats,

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

– em representação do Governo dinamarquês, inicialmente por J. Nymann-Lindegren, M. Wolff e P. Ngo e, em seguida, por J. Nymann-Lindegren e M. Wolff, na qualidade de agentes,

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

– em representação do Governo estónio, por N. Grünberg e A. Kalbus, na qualidade de agentes,

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

– em representação do Governo espanhol, inicialmente por L. Aguilera Ruiz e A. Rubio González e, em seguida, por L. Aguilera Ruiz, na qualidade de agente,

– em representação do Governo cipriota, por E. Neofytou, na qualidade de agente,

– em representação do Governo letão, por V. Soņeca, na qualidade de agente,

– em representação do Governo húngaro, inicialmente por M. Z. Fehér e Z. Wagner e, em seguida, por M. Z. Fehér, na qualidade de agente,

– em representação do Governo neerlandês, por M. K. Bulterman e M. A. M. de Ree, na qualidade de agentes,

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

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

– em representação do Governo do Reino Unido, por S. Brandon, na qualidade de agente, assistido por G. Facenna, QC, e de C. Knight, barrister,

– [travessão eliminado por Despacho de 16 de novembro de 2020],

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

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

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

profere o presente

Acórdão

1 Os pedidos de decisão prejudicial têm por objeto a interpretação, por um lado, 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 eletrónica (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), e, por outro, dos artigos 12.º a 15.º da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos

legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO 2000, L 178, p. 1), lidos à luz dos artigos 4.º, 6.º a 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta») e do artigo 4.º, n.º 2, TUE.

2 O pedido no processo C-511/18 foi apresentado no âmbito de litígios que opõem a Quadrature du Net, a French Data Network, a Fédération des fournisseurs d'accès à Internet associatifs e a Igwan.net ao Premier ministre [primeiro-ministro, França], ao Garde des Sceaux, ministre de la Justice [Guarda dos Selos, ministro da Justiça, França], ao ministre de l'Intérieur [ministro da Administração Interna, França] e ao ministre des Armées [ministro da Defesa, França], relativo à legalidade do Decreto n.º 2015-1185, de 28 de setembro de 2015, que Designa os Serviços Especializados de Informação (JORF de 29 de setembro de 2015, texto 1 de 97, a seguir «Decreto n.º 2015-1185»), do Decreto n.º 2015-1211, de 1 de outubro de 2015, relativo ao Contencioso da Aplicação das Técnicas de Informação Sujeitas a Autorização e dos Ficheiros Relevantes para a Segurança do Estado (JORF de 2 de outubro de 2015, texto 7 de 108, a seguir «Decreto n.º 2015-1211»), do Decreto n.º 2015-1639, de 11 de dezembro de 2015, relativo à Designação dos Serviços Autorizados a Recorrer às Técnicas Referidas no Título V do Livro VIII do Código da Segurança Interna, adotado em aplicação do artigo L. 811-4 do Código da Segurança Interna (JORF de 12 de dezembro de 2015, texto 28 de 127, a seguir «Decreto n.º 2015-1639»), assim como do Decreto n.º 2016-67, de 29 de janeiro de 2016, relativo às Técnicas de Recolha de Informação (JORF de 31 de janeiro de 2016, texto 2 de 113, a seguir «Decreto n.º 2016-67»).

3 O pedido no processo C-512/18 foi apresentado no âmbito de litígios que opõem a French Data Network, a Quadrature du Net e a Fédération des fournisseurs d'accès à Internet associatifs ao primeiro-ministro (França) e ao Guarda dos Selos, ministro da Justiça (França), relativo à legalidade do artigo R. 10-13 do Código dos Correios e das Comunicações Eletrónicas (a seguir «CCCE») e do Decreto n.º 2011-219, de 25 de fevereiro de 2011, sobre a Conservação dos Dados que Permitem a Identificação de Qualquer Pessoa que Tenha Contribuído para a Criação de um Conteúdo Oferecido em Linha (JORF de 1 de março de 2011, texto 32 de 170, a seguir «Decreto n.º 2011-219»).

4 O pedido no processo C-520/18 foi apresentado no âmbito de litígios que opõem a Ordre des barreaux francophones et germanophone, a Académie Fiscale ASBL, UA, a Liga voor Mensenrechten ASBL, a Ligue des Droits de l'Homme ASBL, VZ, WY e XX ao Conseil des ministres [Conselho de Ministros, Bélgica], que têm por objeto a legalidade da Lei de 29 de maio de 2016, relativa à Recolha e à Conservação dos Dados no Setor das Comunicações Eletrónicas (*Moniteur belge* de 18 de julho de 2016, p. 44717, a seguir «Lei de 29 de maio de 2016»).

Quadro jurídico

Direito da União

Diretiva 95/46

5 A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31), foi revogada, com efeitos a contar de 25 de maio de 2018, pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de

2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46 (JO 2016, L 119, p. 1). O artigo 3.º, n.º 2, da Diretiva 95/46 dispunha:

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

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

– efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.»

6 O artigo 22.º da Diretiva 95/46, que figura no capítulo III desta, sob a epígrafe «Recursos judiciais, responsabilidade e sanções», tinha a seguinte redação:

«Sem prejuízo de quaisquer garantias graciosas, nomeadamente por parte da autoridade de controlo referida no artigo 28.º, previamente a um recurso contencioso, os Estados-Membros estabelecerão que qualquer pessoa poderá recorrer judicialmente em caso de violação dos direitos garantidos pelas disposições nacionais aplicáveis ao tratamento em questão.»

Diretiva 97/66

7 Nos termos do artigo 5.º da Diretiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações (JO 1997, L 24, p. 1), sob a epígrafe «Confidencialidade das comunicações»:

«1. Os Estados-Membros devem garantir nas suas regulamentações internas a confidencialidade das comunicações através da rede pública de telecomunicações e dos serviços de telecomunicações acessíveis ao público. Designadamente, devem proibir a escuta, a colocação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações por terceiros, sem o consentimento dos utilizadores, exceto quando legalmente autorizados, em conformidade com o n.º 1 do artigo 14.º

2. O disposto no n.º 1 não se aplica às gravações legalmente autorizadas de comunicações no âmbito de práticas comerciais lícitas para o efeito de constituir prova de uma transação comercial ou de outra comunicação de negócios.»

Diretiva 2000/31

8 Os considerandos 14 e 15 da Diretiva 2000/31 preveem:

«(14) A proteção dos indivíduos no que se refere ao tratamento dos dados pessoais é regida exclusivamente pela Diretiva [95/46] e pela Diretiva [97/66], que se aplicam plenamente aos serviços da sociedade da informação. Essas diretivas criam já um quadro legal comunitário no domínio dos dados pessoais, pelo que não é necessário tratar essa questão na presente diretiva para garantir o bom funcionamento do mercado interno, em especial a livre circulação dos dados pessoais entre Estados-Membros. A execução e aplicação da presente diretiva deverão efetuar-se em absoluta conformidade com os princípios respeitantes à proteção dos dados

pessoais, designadamente no que se refere às comunicações comerciais não solicitadas e à responsabilidade dos intermediários. A presente diretiva não pode impedir a utilização anónima de redes abertas, como, por exemplo, a Internet.

(15) A confidencialidade das comunicações está assegurada pelo artigo 5.º da Diretiva [97/66]. Nos termos dessa diretiva, os Estados-Membros devem proibir qualquer forma de interceção ou de vigilância dessas comunicações, por pessoas que não sejam os remetentes ou os destinatários destas, exceto quando legalmente autorizados.»

9 O artigo 1.º da Diretiva 2000/31 tem a seguinte redação:

«1. A presente diretiva tem por objetivo contribuir para o correto funcionamento do mercado interno, garantindo a livre circulação dos serviços da sociedade da informação entre Estados-Membros.

2. A presente diretiva aproxima, na medida do necessário à realização do objetivo previsto no n.º 1, certas disposições nacionais aplicáveis aos serviços da sociedade da informação que dizem respeito ao mercado interno, ao estabelecimento dos prestadores de serviços, às comunicações comerciais, aos contratos celebrados por via eletrónica, à responsabilidade dos intermediários, aos códigos de conduta, à resolução extrajudicial de litígios, às ações judiciais e à cooperação entre Estados-Membros.

3. A presente diretiva é complementar da legislação comunitária aplicável aos serviços da sociedade da informação, sem prejuízo do nível de proteção, designadamente da saúde pública e dos interesses dos consumidores, tal como consta dos atos comunitários e da legislação nacional de aplicação destes, na medida em que não restrinjam a liberdade de prestação de serviços da sociedade da informação.

[…]

5. A presente diretiva não é aplicável:

[…]

b) À[s] questões respeitantes aos serviços da sociedade da informação abrangidas pelas Diretivas [95/46] e [97/66];

[…]»

10 O artigo 2.º da Diretiva 2000/31 tem a seguinte redação:

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

a) "Serviços da sociedade da informação": os serviços da sociedade da informação na aceção do n.º 2 do artigo 1.º da Diretiva 98/34/CE [do Parlamento Europeu e do Conselho, de 22 de junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas (JO 1998, L 204, p. 37)], conforme alterada pela Diretiva 98/48/CE [do Parlamento Europeu e do Conselho, de 20 de julho de 1998 (JO 1998, L 217, p. 18)];

[…]»

11 O artigo 15.º da Diretiva 2000/31 prevê:

«1. Os Estados-Membros não imporão aos prestadores, para o fornecimento dos serviços mencionados nos artigos 12.º, 13.º e 14.º, uma obrigação geral de vigilância sobre as informações que estes transmitam ou armazenem, ou uma obrigação geral de procurar ativamente factos ou circunstâncias que indiciem ilicitudes.

2. Os Estados-Membros podem estabelecer a obrigação, relativamente aos prestadores de serviços da sociedade da informação, de que informem prontamente as autoridades públicas competentes sobre as atividades empreendidas ou informações ilícitas prestadas pelos autores aos destinatários dos serviços por eles prestados, bem como a obrigação de comunicar às autoridades competentes, a pedido destas, informações que permitam a identificação dos destinatários dos serviços com quem possuam acordos de armazenagem.»

Diretiva 2002/21

12 Nos termos do considerando 10 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):

«A definição de "serviço da sociedade da informação" constante do artigo 1.º da Diretiva [98/34, conforme alterada pela Diretiva 98/48], abrange um amplo leque de atividades económicas desenvolvidas em linha. A maior parte dessas atividades não são abrangidas pelo âmbito de aplicação da presente diretiva, dado que não consistem total ou principalmente no envio de sinais através de redes de comunicações eletrónicas. Os serviços de telefonia vocal e de envio de correio eletrónico estão abrangidos pela presente diretiva. A mesma empresa, por exemplo um prestador de serviços Internet, pode oferecer tanto serviços eletrónicos de comunicações, tais como o acesso à Internet, como serviços não abrangidos pela presente diretiva, tais como a prestação de conteúdos em linha.»

13 O artigo 2.º da Diretiva 2002/21 prevê:

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

[…]

c) "Serviço de comunicações eletrónicas", o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações eletrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão, excluindo os serviços que prestem ou exerçam controlo editorial sobre conteúdos transmitidos através de redes e serviços de comunicações eletrónicas; excluem-se igualmente os serviços da sociedade da informação, tal como definidos no artigo 1.º da Diretiva [98/34] que não consistam total ou principalmente no envio de sinais através de redes de comunicações eletrónicas;

[…]»

Diretiva 2002/58

14 Os considerandos 2, 6, 7, 11, 22, 26 e 30 da Diretiva 2002/58 enunciam:

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

[…]

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

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

[…]

(11) Tal como a Diretiva [95/46], a presente diretiva não trata questões relativas à proteção dos direitos e liberdades fundamentais relacionadas com atividades não reguladas pelo direito [da União]. Portanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.º 1 do artigo 15.º da presente diretiva, necessários para a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal. Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, [assinada em Roma em 4 de novembro de 1950], segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais.

[…]

(22) A proibição de armazenamento das comunicações e dos dados de tráfego a elas relativos por terceiros que não os utilizadores ou sem o seu consentimento não tem por objetivo proibir qualquer armazenamento automático, intermédio e transitório de informações, desde que esse armazenamento se efetue com o propósito exclusivo de realizar a transmissão através da rede de comunicação eletrónica e desde que as informações não sejam armazenadas por um período de tempo superior ao necessário para a transmissão e para fins de gestão de tráfego e que durante o período de armazenamento se encontre garantida a confidencialidade das informações. […]

[…]

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

direito do assinante de não dar ou retirar o seu consentimento a esse tratamento. Os dados de tráfego utilizados para comercialização de serviços de comunicações [...] devem igualmente ser eliminados ou tornados anónimos [...]

[...]

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

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

«1. A presente diretiva harmoniza as disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, 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 [TFUE], tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia, e em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em matéria de direito penal.»

16 Segundo o artigo 2.º da Diretiva 2002/58, sob a epígrafe «Definições»:

«Salvo disposição em contrário, são aplicáveis as definições constantes da Diretiva [95/46] e da Diretiva [2002/21].

São também aplicáveis as seguintes definições:

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

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

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

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

[...]»

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

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

18 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.»

19 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.»

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

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

21 O artigo 15.º da referida diretiva, sob a epígrafe «Aplicação de determinadas disposições da Diretiva [95/46]», enuncia:

«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.

[…]

2. O disposto no capítulo III da Diretiva [95/46] relativo a recursos judiciais, responsabilidade e sanções é aplicável no que respeita às disposições nacionais adotadas nos termos da presente diretiva e aos direitos individuais decorrentes da presente diretiva.

[…]»

Regulamento 2016/679

22 O considerando 10 do Regulamento 2016/679 enuncia:

«A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. […]»

23 O artigo 2.º deste regulamento dispõe:

«1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

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

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

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

[…]

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

[…]

4. O presente regulamento não prejudica a aplicação da Diretiva [2000/31], nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12.º a 15.º»

24 O artigo 4.º do referido regulamento prevê:

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

1) "Dados pessoais", informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

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

[…]»

25 O artigo 5.º do Regulamento 2016/679 dispõe:

«1. Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ("licitude, lealdade e transparência");

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 ("limitação das finalidades");

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados ("minimização dos dados");

d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora ("exatidão");

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados ("limitação da conservação");

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas ("integridade e confidencialidade");

[…]»

26 O artigo 6.º deste regulamento tem a seguinte redação:

«1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

[…]

c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

[…]

3. O fundamento jurídico para o tratamento referido no n.º 1, alíneas c) e e), é definido:

a) Pelo direito da União; ou

b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito.

A finalidade do tratamento é determinada com esse fundamento jurídico […]. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas

relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.

[…]»

27 O artigo 23.º do referido regulamento prevê:

«1. O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:

a) A segurança do Estado;

b) A defesa;

c) A segurança pública;

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

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

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

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

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

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

j) A execução de ações cíveis.

2. Em especial, as medidas legislativas referidas no n.º 1 incluem, quando for relevante, disposições explícitas relativas, pelo menos:

a) Às finalidades do tratamento ou às diferentes categorias de tratamento;

b) Às categorias de dados pessoais;

c) Ao alcance das limitações impostas;

d) Às garantias para evitar o abuso ou o acesso ou transferência ilícitos;

e) À especificação do responsável pelo tratamento ou às categorias de responsáveis pelo tratamento;

f) Aos prazos de conservação e às garantias aplicáveis, tendo em conta a natureza, o âmbito e os objetivos do tratamento ou das categorias de tratamento;

g) Aos riscos específicos para os direitos e liberdades dos titulares dos dados; e

h) Ao direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.»

28 Segundo o artigo 79.º, n.º 1, do referido regulamento:

«Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, nomeadamente o direito de apresentar reclamação a uma autoridade de controlo, nos termos do artigo 77.º, todos os titulares de dados têm direito à ação judicial se considerarem ter havido violação dos direitos que lhes assistem nos termos do presente regulamento, na sequência do tratamento dos seus dados pessoais efetuado em violação do referido regulamento.»

29 Nos termos do artigo 94.º do Regulamento 2016/679:

«1. A Diretiva [95/46] é revogada com efeitos a partir de 25 de maio de 2018.

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

30 O artigo 95.º desse regulamento dispõe:

«O presente regulamento não impõe obrigações suplementares a pessoas singulares ou coletivas no que respeita ao tratamento no contexto da prestação de serviços de comunicações eletrónicas disponíveis nas redes públicas de comunicações na União em matérias que estejam sujeitas a obrigações específicas com o mesmo objetivo estabelecidas na Diretiva [2002/58].»

Direito francês

Código da Segurança Interna

31 O livro VIII da parte legislativa do Código da Segurança Interna (a seguir «CSI»), prevê, nos seus artigos L. 801-1 a L. 898-1, as regras relativas à informação.

32 O L. 811-3 do CSI dispõe:

«Para o exercício exclusivo das suas respetivas missões, os serviços especializados de informação podem recorrer às técnicas referidas no título V do presente livro para a recolha das informações relativas à defesa e à promoção dos seguintes interesses fundamentais da nação:

1° A independência nacional, a integridade do território e a defesa nacional;

2° Os interesses fundamentais da política estrangeira, a execução dos compromissos europeus e internacionais da França e a prevenção de qualquer forma de ingerência estrangeira;

3° Os interesses económicos, industriais e científicos fundamentais da França;

4° A prevenção do terrorismo;

5° A prevenção:
a) Dos atentados à forma republicana das instituições;
b) Das ações destinadas a obter a manutenção ou a reconstituição de agrupamentos dissolvidos em aplicação do artigo L. 212-1;
c) Dos atos de violência coletiva suscetíveis de atentar gravemente contra a paz pública;

6° A prevenção da criminalidade e da delinquência organizadas;

7° A prevenção da proliferação das armas de destruição maciça.»

33 O artigo L. 811-4 do CSI enuncia:

«Por decreto do Conseil d'État [(Conselho de Estado)], adotado após parecer da Commission nationale de contrôle des techniques de renseignement [(Comissão nacional de controlo das técnicas de informação)], serão designados os serviços, para além dos serviços especializados de informação, pertencentes aos ministros da Defesa, da Administração Interna e da Justiça e dos ministros responsáveis pelos Assuntos Económicos, Orçamentais e Aduaneiros, que podem ser autorizados a recorrer às técnicas mencionadas no título V do presente livro, nas condições previstas neste livro. O referido decreto deve precisar, para cada serviço, as finalidades mencionadas no artigo L. 811-3 e as técnicas que podem dar lugar a autorização.»

34 O artigo L. 821-1, primeiro parágrafo, do CSI dispõe o seguinte:

«A aplicação no território nacional das técnicas de recolha de informações referidas nos capítulos I a IV do título V do presente livro está sujeita a autorização prévia do primeiro-ministro, emitida após parecer da Comissão nacional de controlo das técnicas de informação.»

35 O artigo L. 821-2 do CSI prevê:

«A autorização referida no artigo L. 821-1 é emitida mediante pedido escrito e fundamentado do ministro da Defesa, do ministro da Administração Interna, do ministro da Justiça e dos ministros responsáveis pelos Assuntos Económicos, Orçamentais e Aduaneiros. Cada ministro só pode delegar esta atribuição individualmente a colaboradores diretos autorizados a lidar com segredos relativos à defesa nacional.

O pedido deve precisar:

1° A técnica ou as técnicas aplicáveis;

2° O serviço em relação ao qual é apresentado;

3° A finalidade ou as finalidades prosseguidas;

4° O fundamento ou os fundamentos das medidas;

5° A duração da validade da autorização;

6° A pessoa ou as pessoas, o local ou os locais ou veículos em causa.

Para efeitos da aplicação do ponto 6, as pessoas cuja identidade não seja conhecida podem ser designadas pelos seus identificadores ou pela sua qualidade e os locais ou veículos podem ser designados tendo por referência as pessoas que são objeto do pedido.

[…]»

36 Nos termos do artigo L. 821-3, primeiro parágrafo, do CSI:

«O pedido é comunicado ao presidente ou, na sua falta, a um dos membros da Comissão nacional de controlo das técnicas de informação entre os que são referidos nos n.os 2 e 3 do artigo L. 831-1, que deve apresentar ao primeiro-ministro um parecer no prazo de vinte e quatro horas. Quando o pedido for apreciado pela formação restrita ou pela sessão plenária da comissão, o primeiro-ministro será imediatamente informado e o parecer será emitido no prazo de setenta e duas horas.»

37 O artigo L. 821-4 do CSI dispõe:

«A autorização de aplicação das técnicas referidas nos capítulos I a IV do título V do presente livro é emitida pelo primeiro-ministro por um período máximo de quatro meses. […] A autorização inclui as fundamentações e menções previstas nos pontos 1 a 6 do artigo L. 821-2. Qualquer autorização é renovável em condições idênticas às previstas no presente capítulo.

Quanto a autorização é emitida após parecer desfavorável da Comissão nacional de controlo das técnicas de informação, deve indicar os motivos pelos quais esse parecer não foi seguido.

[…]»

38 O artigo L. 833-4 do CSI, que figura no capítulo III deste título, dispõe:

«Por sua própria iniciativa ou quando lhe for apresentada uma reclamação por qualquer pessoa que pretenda verificar que não lhe estão a ser aplicadas indevidamente técnicas de inteligência, a comissão procederá ao controlo da técnica ou das técnicas invocadas com vista a verificar se foram ou são aplicadas em conformidade com o presente livro. Deve notificar o autor da reclamação de que se procedeu às verificações necessárias, sem confirmar nem negar a sua aplicação.»

39 O artigo L. 841-1, primeiro e segundo parágrafos, do CSI tem a seguinte redação:

«Sob reserva das disposições específicas previstas no artigo L. 854-9 do presente código, o Conseil d'État [(Conselho de Estado)] é competente para apreciar, nas condições previstas no capítulo III bis do título VII do livro VII do Código da Justiça Administrativa, os pedidos relativos à aplicação das técnicas de informação referidas no título V do presente livro.

Pode apresentar um pedido:

1° Qualquer pessoa que pretenda verificar que não lhe estão a ser aplicadas indevidamente técnicas de inteligência e que demonstre que o procedimento previsto no artigo L. 833-4 foi aplicado previamente;

2° A Comissão nacional de controlo das técnicas de informação, nas condições previstas no artigo L. 833-8.»

40 O título V do livro VIII da parte legislativa do CSI, relativo às «técnicas de recolha de informação sujeitas à autorização», inclui, nomeadamente, um capítulo I, sob a epígrafe «Acessos administrativos aos dados de ligação», do qual constam os artigos L. 851-1 a L. 851-7 do CSI.

41 O artigo L. 851-1 do CSI dispõe:

«Nas condições previstas no capítulo 1 do título II do presente livro, pode ser autorizada, junto dos operadores de comunicações eletrónicas e das pessoas mencionadas no artigo L. 34-1 do [CPCE], bem como das pessoas mencionadas nos pontos 1 e 2 da parte I do artigo 6.º, da loi n.º 2004-575 du 21 juin

2004 pour la confiance dans l'économie numérique [(Lei n.º 2004-575 de 21 de junho de 2004, relativa à Confiança na Economia Digital)] [(JORF de 22 de junho de 2004, p. 11168)], a recolha das informações ou documentos tratados ou conservados pelos respetivos serviços ou redes de comunicações eletrónicas, incluindo os dados técnicos relativos à identificação dos números de assinatura ou de ligação a serviços de comunicações eletrónicas, ao recenseamento de todos os números de assinatura ou de ligação de uma pessoa designada, à localização dos equipamentos terminais e às comunicações de um assinante referentes à lista dos números das chamadas recebidas e efetuadas, duração e data das comunicações.

Em derrogação do artigo L. 821-2, os pedidos escritos e fundamentados relativos aos dados técnicos relativos à identificação dos números de assinatura ou de ligação a serviços de comunicações eletrónicas, ou ao recenseamento de todos os números de assinatura ou de ligação de uma determinada pessoa são diretamente transmitidos à Comissão nacional de controlo das técnicas de informação pelos agentes individualmente designados e habilitados dos serviços de informação referidos nos artigos L. 811-2 e L. 811-4. A comissão emite o seu parecer nas condições previstas no artigo L. 821-3.

Um serviço dependente do primeiro-ministro é responsável pela recolha de informações ou de documentos junto dos operadores e das pessoas referidas no primeiro parágrafo do presente artigo. A Comissão nacional de controlo das técnicas de informação dispõe de acesso permanente, completo, direto e imediato às informações ou documentos recolhidos.

As modalidades de aplicação do presente artigo são fixadas por decreto do Conseil d'État [(Conselho de Estado)], adotado após parecer da Comissão Nacional da Informática e Liberdades e da Comissão nacional de controlo das técnicas de informação.»

42 O artigo L. 851-2 do CSI prevê:

«I. — Nas condições previstas no capítulo I do título II do presente livro e exclusivamente para efeitos de prevenção do terrorismo, pode ser individualmente autorizada a recolha em tempo real, nas redes dos operadores e das pessoas referidas no artigo L. 851-1, das informações ou documentos referidos no mesmo artigo L. 851-1 relativos a uma pessoa previamente identificada como potencialmente ligada a uma ameaça. Quando existam razões sérias para crer que uma ou mais pessoas que pertencem ao círculo da pessoa abrangida pela autorização podem fornecer informações com base na finalidade que justifica a autorização, esta pode ser igualmente concedida individualmente em relação a cada uma dessas pessoas.

I-bis. O número máximo das autorizações concedidas nos termos do presente artigo em vigor simultaneamente é definido pelo primeiro-ministro, após parecer da Comissão nacional de controlo das técnicas de informação. A decisão que fixa este contingente e a sua repartição entre os ministros referidos no primeiro parágrafo do artigo L. 821-2, bem como o número de autorizações de interceção concedidas são transmitidos à comissão.

[…]»

43 O artigo L. 851-3 do CSI prevê:

«I. — Nas condições previstas no capítulo I do título II do presente livro e exclusivamente para efeitos de prevenção do terrorismo, pode ser imposta aos operadores e às pessoas referidas no artigo L. 851-1 a obrigação de aplicarem nas suas redes tratamentos automatizados destinados, em função de parâmetros especificados na autorização, a detetar ligações suscetíveis de constituir uma ameaça terrorista.

Estes tratamentos automatizados utilizam exclusivamente as informações ou documentos referidos no artigo L. 851-1, sem recolher dados distintos dos que respondem aos seus parâmetros de conceção e sem permitir a identificação das pessoas às quais as informações ou documentos dizem respeito.

Em conformidade com o princípio da proporcionalidade, a autorização do primeiro-ministro precisa o âmbito técnico da execução desses tratamentos.

II. — A Comissão nacional de controlo das técnicas de informação emite um parecer sobre o pedido de autorização relativo aos tratamentos automatizados e os parâmetros de deteção considerados. Dispõe de acesso permanente, completo e direto a esses tratamentos, assim como às informações e dados recolhidos. Deve ser informada de quaisquer alterações aos tratamentos e parâmetros e pode formular recomendações.

A primeira autorização de aplicação dos tratamentos automatizados prevista no ponto I do presente artigo é emitida por um período de dois meses. A autorização é renovada nas condições de duração previstas no capítulo I do título II do presente livro. O pedido de renovação contém um resumo do número de identificadores indicados pelo tratamento automatizado e uma análise da relevância dessas indicações.

III. — As condições previstas no artigo L. 871-6 são aplicáveis às operações materiais efetuadas pelos operadores e pelas pessoas referidas no artigo L. 851-1 para efeitos dessa aplicação.

IV. — Quando os tratamentos referidos no ponto I do presente artigo detetem dados suscetíveis de caracterizar a existência de uma ameaça de caráter terrorista, o primeiro-ministro ou uma das pessoas por ele delegadas pode autorizar, após parecer da Comissão nacional de controlo das técnicas de informação emitido nas condições previstas no capítulo I do título II do presente livro, a identificação da pessoa ou das pessoas em causa e a recolha dos respetivos dados. Estes dados deverão ser explorados no prazo de sessenta dias a contar dessa recolha e devem ser destruídos no termo desse prazo, salvo no caso de elementos sérios que confirmem a existência de uma ameaça terrorista ligada a uma ou a mais das pessoas em causa.

[…]»

44 O artigo L. 851-4 do CSI tem a seguinte redação:

«Nas condições previstas no capítulo I do título II do presente livro, os dados técnicos relativos à localização dos equipamentos terminais utilizados referidos no artigo L. 851-1 podem ser recolhidos a pedido da rede e transmitidos em tempo real pelos operadores a um serviço dependente do primeiro-ministro.»

45 O artigo R. 851-5 do CSI, que figura na parte regulamentar deste código, prevê:

«I. — As informações ou documentos referidos no artigo L. 851-1 são, com exclusão do conteúdo da correspondência trocada ou das informações consultadas, os seguintes:

1° Os enumerados nos artigos R. 10-13 e R. 10-14 do [CPCE] e no artigo 1.º do Decreto [n.º 2011-219];

2° Os dados técnicos distintos dos mencionados no ponto 1:

a) Que permitam localizar os equipamentos terminais;

b) Relativos ao acesso dos equipamentos terminais às redes ou aos serviços de comunicação ao público em linha;

c) Relativos ao encaminhamento das comunicações eletrónicas através das redes;

d) Relativos à identificação e à autenticação de um utilizador, de uma ligação, de uma rede ou de um serviço de comunicação ao público em linha;

e) Relativos às características dos equipamentos terminais e aos dados de configuração dos seus programas informáticos.

II. — Só as informações e documentos referidos no ponto 1 da parte I podem ser recolhidos em aplicação do artigo L. 851-1. Essa recolha tem lugar em tempo diferido.

As informações enumeradas no ponto 2 da parte I apenas podem ser recolhidas em aplicação dos artigos L. 851-2 e L. 851-3 nas condições e limites previstos por estes artigos e sob reserva da aplicação do artigo R. 851-9.»

CPCE

46 O artigo L. 34-1 do CPCE dispõe:

«I. — O presente artigo aplica-se ao tratamento de dados pessoais na prestação de serviços de comunicações eletrónicas ao público, aplicando-se, em particular, às redes que albergam os dispositivos de recolha de dados e de identificação.

II. — Os operadores de comunicações eletrónicas e, em especial, as pessoas cuja atividade consiste em oferecer acesso a serviços de comunicação ao público em linha, devem eliminar ou anonimizar todos os dados de tráfego, sem prejuízo do disposto nos pontos III, IV, V e VI.

Quem prestar serviços de comunicações eletrónicas ao público deve instituir, em observância do indicado no ponto anterior, procedimentos internos para dar resposta aos pedidos das autoridades competentes.

Nos termos do presente artigo quem, em razão de uma atividade profissional principal ou acessória, oferecer ao público uma ligação que permita uma comunicação em linha através de um acesso à rede, ainda que de forma gratuita, fica obrigado ao cumprimento das disposições aplicáveis aos operadores de comunicações eletrónicas nos termos do presente artigo.

III. — Para efeitos de investigação, deteção e instauração de ação penal contra crimes ou incumprimento da obrigação definida no artigo L. 336-3 do code de la propriété intellectuelle [(Código da Propriedade Intelectual)] ou para efeitos de prevenção de ataques aos sistemas de tratamento automatizado de dados previstos e punidos pelos artigos 323-1 a 323-3-1 do code pénal [(Código Penal)], e com o único objetivo de permitir, se necessário, a colocação à disposição da autoridade judicial ou da alta autoridade mencionada no artigo L. 331-12 do Código da Propriedade Intelectual ou da autoridade nacional de segurança dos sistemas de informação mencionada no artigo L. 2321-1 du code de la défense [(Código da Defesa)], as operações dirigidas a eliminar ou a anonimizar determinadas categorias de dados técnicos poderão ser adiadas por um período máximo de um ano. Por decreto consultado ao do Conseil d'État [(Conselho de Estado, em formação jurisdicional)], adotado após o parecer da Commission nationale de l'informatique et des libertés [(Comissão Nacional de Informática e Liberdades)], deverão ser especificadas, dentro dos limites previstos no ponto VI, essas categorias de dados e a duração da sua conservação, em função da atividade dos operadores e da natureza das comunicações, bem como as modalidades de indemnização, se for caso disso, dos custos adicionais identificáveis e específicos das prestações garantidas a esse título pelos operadores, por solicitação do Estado.

[…]

VI. — Os dados conservados e tratados nas condições definidas nos pontos III, IV e V serão relativos exclusivamente à identificação dos utilizadores dos serviços fornecidos pelos operadores, às características técnicas das comunicações disponibilizadas por estes últimos e à localização dos equipamentos terminais.

Não podem em caso algum ser relativos ao conteúdo da correspondência trocada ou às informações consultadas no âmbito dessas comunicações, independentemente da forma.

A conservação e o tratamento dos dados realizam-se com respeito pelas disposições da Lei n.º 78-17 de 6 de janeiro de 1978 relativa à Informática, aos Ficheiros e às Liberdades.

Os operadores adotarão as medidas necessárias para impedir a utilização desses dados para fins distintos dos previstos no presente artigo.»

47 O artigo R. 10-13 do CPCE tem a seguinte redação:

«I. — Em aplicação da parte III do artigo L. 34-1, os operadores de comunicações eletrónicas devem conservar, para fins de investigação, de deteção e instauração de ação penal contra as infrações penais:

a) As informações que permitam identificar o utilizador;

b) Os dados relativos aos equipamentos terminais de comunicações utilizados;

c) As características técnicas, bem como a data, hora e duração de cada comunicação;

d) Os dados relativos aos serviços adicionais pedidos ou utilizados e os seus fornecedores;

e) Os dados que permitam identificar o destinatário ou os destinatários da comunicação.

II. — No caso das atividades de telefonia, o operador deve conservar os dados referidos na parte II e também os dados que permitam a identificação da origem e da localização da comunicação.

III. — Os dados referidos no presente artigo devem ser conservados durante um ano, a partir do dia do registo.

IV.— Os custos adicionais identificáveis e específicos suportados pelos operadores aos quais as autoridades judiciais impuseram o dever de fornecerem dados abrangidos pelas categorias referidas no presente artigo serão indemnizados de acordo com as modalidades previstas no artigo R. 213-1 do Código de Processo Penal.»

48 O artigo R. 10-14 do CPCE prevê:

«I. — Em aplicação da parte IV do artigo L. 34-1, os operadores de comunicações eletrónicas estão autorizados a conservar, para efeitos das suas operações de faturação e de pagamento, os dados de caráter técnico que permitam identificar o utilizador, bem como os referidos nas alíneas b), c) e d) da parte I do artigo R. 10-13.

II. — No caso das atividades de telefonia, os operadores podem conservar, além dos dados referidos na parte I, os dados com caráter técnico relativos à localização da comunicação, à identificação do destinatário ou dos destinatários da comunicação e os dados que permitam estabelecer a faturação.

III. — Os dados referidos nas partes I e II do presente artigo apenas podem ser conservados se forem necessários para a faturação e para o pagamento dos serviços prestados. A sua conservação deve limitar-se ao tempo estritamente necessário para essa finalidade, sem exceder um ano.

IV. — Para a segurança das redes e das instalações, os operadores podem conservar por um período não superior a três meses:

a) Os dados que permitam identificar a origem da comunicação;

b) As características técnicas, a data, o horário e a duração de cada comunicação;

c) Os dados de caráter técnico que permitam identificar o destinatário ou os destinatários da comunicação;

d) Os dados relativos aos serviços complementares pedidos ou utilizados e os seus fornecedores.»

Lei n.º 2004-575, de 21 de junho de 2004, relativa à Confiança na Economia Digital

49 O artigo 6.º da Lei n.º 2004-575, de 21 de junho de 2004, relativa à Confiança na Economia Digital (JORF de 22 de junho de 2004, p. 11168, a seguir «LCEN»), prevê:

«I.— 1. As pessoas cuja atividade consista em oferecer acesso a serviços de comunicação em linha ao público devem informar os seus assinantes da existência de meios técnicos que permitam restringir o acesso a determinados serviços ou selecioná-los e oferecer-lhes, pelo menos, um desses meios.

[…]

2. As pessoas singulares ou coletivas que armazenem, incluindo a título gratuito, para disponibilização ao público, mediante serviços em linha de comunicação ao público, sinais, textos, imagens, sons ou mensagens de qualquer natureza proporcionados pelos destinatários destes serviços não podem ser civilmente responsabilizadas pelas atividades ou informações armazenadas a pedido de um destinatário de tais serviços caso não tenham efetivamente conhecimento do seu caráter ilícito ou de factos e circunstâncias reveladores desse caráter ou se, a partir do momento em que tiveram conhecimento de tal facto, atuaram rapidamente para remover ou impedir o acesso a esses dados.

[…]

II. — As pessoas referidas nos n.os 1 e 2 da parte I devem manter e conservar os dados de forma que permita a identificação de quem tenha contribuído para a criação do conteúdo ou de algum dos conteúdos dos serviços de que são prestadores.

Devem fornecer às pessoas que editam um serviço de comunicação ao público em linha meios técnicos que lhes permitam satisfazer as condições de identificação previstas na parte III.

A autoridade judicial pode pedir a comunicação aos prestadores referidos nos n.os 1 e 2 da parte I dos dados referidos no primeiro parágrafo.

As disposições dos artigos 226-17, 226-21 e 226-22 do Código Penal são aplicáveis ao tratamento desses dados.

Por decreto do Conseil d'État [(Conselho de Estado)], adotado após parecer da Comissão Nacional da Informática e Liberdades, serão definidos os dados mencionados no parágrafo primeiro e será determinada a duração e as modalidades da sua conservação.

[…]»

Decreto n.º 2011-219

50 O capítulo I do Decreto n.º 2011-219, adotado com base no artigo 6.º, parte II, último parágrafo, da LCEN, inclui os artigos 1.º a 4.º deste decreto.

51 O artigo 1.º do Decreto n.º 2011-219 dispõe:

«Os dados referidos na parte II do artigo 6.º da [LCEN], que as pessoas são obrigadas a conservar por força desta disposição, são os seguintes:

1° Em relação às pessoas referidas no n.º 1 da parte I do mesmo artigo e em relação cada ligação dos seus assinantes:

a) O identificador da ligação;

b) O identificador atribuído por essas pessoas ao assinante;

c) O identificador do terminal utilizado para a ligação quando têm acesso ao mesmo;

d) As datas e hora do início e do fim da conexão;

e) As características da linha do assinante;

2° Em relação às pessoas referidas no n.º 2 da parte I do mesmo artigo e em relação a cada operação de criação:

a) O identificador da ligação que está na origem da comunicação;

b) O identificador atribuído pelo sistema de informação ao conteúdo, objeto da operação;

c) Os tipos de protocolos utilizados para a ligação ao serviço e para a transferência de conteúdos;

d) A natureza da operação;

e) A data e a hora da operação;

f) O identificador utilizado pelo autor da operação quando este o forneceu;

3° Em relação às pessoas referidas nos n.ºs 1 e 2 da parte I do mesmo artigo, as informações prestadas por um utilizador ao subscrever um contrato ou ao criar uma conta:

a) No momento da criação da conta, o identificador dessa ligação;

b) O apelido, o nome próprio ou a razão social;

c) Os endereços postais associados;

d) Os pseudónimos utilizados;

e) Os endereços de correio eletrónico ou de contas associados;

f) Os números de telefone;

g) A palavra-passe atualizada e os dados que permitam a sua confirmação ou alteração;

4° Em relação às pessoas referidas nos n.os 1 e 2 da parte I do mesmo artigo, quando a subscrição do contrato ou da conta for paga, as seguintes informações relativas ao pagamento, no que diz respeito a cada operação de pagamento:

a) O tipo de pagamento utilizado;

b) A referência do pagamento;

c) O montante;

d) A data e a hora da transação.

Os dados referidos nos n.os 3 e 4 apenas devem ser conservados na medida em que as pessoas os recolham habitualmente.»

52 O artigo 2.º deste decreto tem a seguinte redação:

«A contribuição para uma criação de conteúdo inclui as operações que tenham por objeto:

a) As criações iniciais de conteúdos;

b) As alterações dos conteúdos e dos dados relacionados com os conteúdos;

c) A eliminação de conteúdos.»

53 O artigo 3.º do referido decreto prevê:

«O prazo de conservação dos dados referidos no artigo 1.º é de um ano:

a) No que diz respeito aos dados referidos nos n.os 1 e 2, a contar do dia da criação dos conteúdos, relativamente a cada operação que contribua para a criação de um conteúdo tal como definido no artigo 2.º;

b) No que diz respeito aos dados referidos no n.º 3, a contar do dia da rescisão do contrato ou do encerramento da conta;

c) No que diz respeito aos dados referidos no n.º 4, a contar da data da emissão da fatura ou da operação de pagamento, por cada fatura ou operação de pagamento.»

Direito belga

54 A Lei de 29 de maio de 2016 alterou, nomeadamente, a loi du 13 juin 2005 relative aux communications électroniques (Lei das Comunicações Eletrónicas, de 13 de junho de 2005) (*Moniteur belge* de 20 de junho de 2005, p. 28070, a seguir «Lei de 13 de junho de 2005»), o code d'instruction criminelle (Código de Processo Penal) e a loi du 30 novembre 1998 organique des services de renseignement et de sécurité [Lei Orgânica dos Serviços de Informação e de Segurança, de 30 de novembro de 1998] (*Moniteur belge* de 18 de dezembro de 1998, p. 40312, a seguir «Lei de 30 de novembro de 1998»).

55 O artigo 126.º da Lei de 13 de junho de 2005, na sua versão resultante da Lei de 29 de maio de 2016, dispõe:

«§ 1. Sem prejuízo da loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [(Lei da Proteção da Vida Privada no Tratamento de Dados Pessoais, de 8 de dezembro de 1992)], os prestadores de serviços de telefonia ao público, incluindo pela Internet, de acesso à Internet, de correio eletrónico pela Internet, os operadores que fornecem redes públicas de comunicações eletrónicas, bem como os operadores que prestam um desses serviços, devem conservar os dados referidos no n.º 3, que sejam por eles gerados ou tratados no âmbito da prestação dos serviços de comunicação em causa.

O presente artigo não é relativo ao conteúdo das comunicações.

A obrigação de conservar os dados referidos no n.º 3 aplica-se igualmente às chamadas infrutíferas, desde que, no âmbito da prestação dos serviços de comunicações em causa, tais dados sejam:

1° no que diz respeito aos dados de telefonia, gerados ou tratados pelos operadores de serviços de comunicações eletrónicas acessíveis ao público ou de uma rede pública de comunicações eletrónicas, ou

2° no que diz respeito aos dados de Internet, registados por esses prestadores.

§ 2. As seguintes entidades serão as únicas a quem, a seu pedido, poderão ser comunicados pelos prestadores e operadores referidos no n.º 1, primeiro parágrafo, os dados conservados por força do presente artigo, para as finalidades e nas condições a seguir indicadas:

1° as autoridades judiciárias, com vista à investigação, à instrução e à instauração de procedimento criminal em relação a infrações, para a execução das medidas referidas nos artigos 46.ºbis e 88.ºbis do Código de Processo Penal e nas condições fixadas por esses artigos;

2° os serviços de informações e de segurança, a fim de cumprirem as missões de informação, com recurso aos métodos de recolha de dados referidos nos artigos 16.º/2, 18.º/7 e 18.º/8 da Lei Orgânica dos Serviços de Informação e de Segurança, de 30 de novembro de 1998, e nas condições previstas na presente lei;

3° qualquer agente de polícia judiciária do Institut [belge des services postaux et des télécommunications (Instituto Belga dos Serviços Postais e Telecomunicações)], com vista à investigação, à instrução e à instauração de procedimento criminal em relação a infrações previstas nos artigos 114.º, 124.º e no presente artigo;

4° os serviços de urgência que prestam apoio a nível local, quando, na sequência de uma chamada de emergência, não obtenham do prestador ou do operador em causa os dados de identificação da pessoa que efetua a chamada através da base de dados referida no artigo 107.º, § 2, parágrafo 3, ou obtenham dados incompletos ou incorretos. Apenas os dados de identificação da pessoa que efetua a chamada podem ser pedidos e, o mais tardar, durante as 24 horas seguintes à chamada;

5° o agente de polícia judiciária da Divisão de pessoas desaparecidas da Polícia Federal, no âmbito da sua missão de assistência às pessoas em perigo, de procura de pessoas cujo desaparecimento é preocupante e quando existem presunções ou indícios sérios de que a integridade física da pessoa desaparecida se encontra em situação de perigo iminente. Apenas os dados referidos no n.º 3, primeiro e segundo parágrafos, relativos à pessoa desaparecida e conservados durante as 48 horas anteriores ao pedido de obtenção de dados, podem ser solicitados ao operador ou ao prestador em causa por intermédio de um serviço de polícia designado pelo Rei;

6° o Serviço de mediação para as telecomunicações, com vista à identificação da pessoa que utilizou indevidamente uma rede ou um serviço de comunicações eletrónicas, em conformidade com as condições referidas no artigo 43ºbis, § 3, n.º 7, da loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques [(Lei relativa à Reforma de Certas Empresas Públicas Económicas, de 21 de março de 1991)]. Apenas podem ser pedidos os dados de identificação.

Os prestadores e operadores referidos no n.º 1, primeiro parágrafo, devem ter as condições necessárias para que os dados referidos no n.º 3 sejam acessíveis de forma ilimitada a partir da Bélgica e para que esses dados e qualquer outra informação necessária relacionada com eles possam ser transmitidos imediatamente às autoridades referidas no presente número.

Sem prejuízo de outras disposições legais, os prestadores e operadores referidos no n.º 1, primeiro parágrafo, não podem utilizar os dados conservados nos termos do n.º 3 para outras finalidades.

§ 3. Os dados destinados a identificar o utilizador ou o assinante e os meios de comunicação, com exceção dos dados especificamente previstos nos parágrafos 1 a 3, são conservados durante doze meses a contar da data a partir da qual é possível efetuar pela última vez uma comunicação através do serviço utilizado.

Os dados relativos ao acesso e à ligação do equipamento terminal à rede e ao serviço e à localização deste equipamento, incluindo o ponto terminal da rede, são conservados durante doze meses a partir da data da comunicação.

Os dados de comunicações, com exclusão do conteúdo, incluindo a sua origem e o seu destino, são conservados durante doze meses a partir da data da comunicação.

O Rei determina, por decreto aprovado em Conseil des ministres [(Conselho de Ministros)], sob proposta do ministro da Justiça e do ministro [competente em matérias relativas às comunicações eletrónicas], e após parecer da Comissão da proteção da vida privada e do Instituto, os dados a conservar por tipo de categorias referidas nos parágrafos 1 a 3, bem como as exigências que esses dados devem respeitar.

[…]»

Litígios no processo principal e questões prejudiciais

Processo C-511/18

56 Por petições apresentadas em 30 de novembro de 2015 e 16 de março de 2016, apensadas no processo principal, a Quadrature du Net, a French Data Network, a Fédération des fournisseurs d'accès à Internet associatifs e a Igwan.net interpuseram no Conseil d'État (Conselho de Estado, em formação jurisdicional, França) recursos de anulação dos Decretos n.ºs 2015-1185, 2015-1211, 2015-1639 e 2016-67, com o fundamento, nomeadamente, de que estes violavam a Constituição francesa, a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (a seguir «CEDH»), e as Diretivas 2000/31 e 2002/58, lidas à luz dos artigos 7.º, 8.º e 47.º da Carta.

57 No que diz respeito, em particular, aos fundamentos relativos à violação da Diretiva 2000/31, o órgão jurisdicional de reenvio salienta que as disposições do artigo L. 851-3 do CSI impõem aos operadores de comunicações eletrónicas e aos prestadores de serviços técnicos a obrigação de «aplicarem nas suas redes tratamentos automatizados destinados, em função de parâmetros especificados na autorização, a detetar ligações suscetíveis de constituir uma ameaça terrorista». Essa técnica visa apenas recolher, durante um tempo limitado, entre o conjunto dos dados de ligação tratados por esses operadores e

por esses prestadores, os dados de ligação que possam estar relacionados com essa infração grave. Nestas condições, as referidas disposições, que não impõem uma obrigação geral de vigilância ativa, não violam o artigo 15.º da Diretiva 2000/31.

58 No que diz respeito aos fundamentos relativos à violação da Diretiva 2002/58, o órgão jurisdicional de reenvio considera que resulta, nomeadamente, das disposições dessa diretiva e do Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, a seguir «Acórdão Tele2», EU:C:2016:970), que as disposições nacionais que impõem obrigações aos prestadores de serviços de comunicações eletrónicas, tais como a conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização dos seus utilizadores e dos seus assinantes, para os fins mencionados no artigo 15.º, n.º 1, da referida diretiva, entre os quais figuram a salvaguarda da segurança nacional, da defesa e da segurança pública, se integram no âmbito de aplicação da mesma diretiva, visto que essas regulamentações regem a atividade dos referidos prestadores. O mesmo se aplica às regulamentações que regem o acesso das autoridades nacionais aos dados, bem como a sua utilização.

59 O órgão jurisdicional de reenvio deduz daí que se integram no âmbito de aplicação da Diretiva 2002/58 tanto a obrigação de conservação que resulta do artigo L. 851-1 do CSI como os acessos administrativos aos referidos dados, incluindo os dados em tempo real, previstos nos artigos L. 851-1, L. 851-2 e L. 851-4 do referido código. O mesmo se aplica, segundo esse órgão jurisdicional, às disposições do artigo L. 851-3 desse código que, embora não imponham aos operadores em causa uma obrigação geral de conservação, impõem-lhes o dever de aplicarem nas suas redes tratamentos automatizados destinados a detetar ligações suscetíveis de constituir uma ameaça terrorista.

60 Em contrapartida, esse órgão jurisdicional considera que não se integram no âmbito de aplicação da Diretiva 2002/58 as disposições do CSI visadas pelos pedidos de anulação que têm por objeto as técnicas de recolha de informação diretamente aplicadas pelo Estado, sem regularem as atividades dos prestadores de serviços de comunicações eletrónicas mediante a imposição de obrigações específicas. Por conseguinte, não se pode considerar que estas disposições aplicam o direito da União, pelo que os fundamentos relativos à violação da Diretiva 2002/58 por parte destas não podem ser utilmente invocados.

61 Assim, para decidir os litígios relativos à legalidade dos Decretos n.os 2015-1185, 2015-1211, 2015-1639 e 2016-67 à luz da Diretiva 2002/58, uma vez que foram adotados para dar execução aos artigos L. 851-1 a L. 851-4 do CSI, colocam-se três questões de interpretação do direito da União.

62 Quanto à interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, o órgão jurisdicional de reenvio, em primeiro lugar, pretende saber se uma obrigação de conservação generalizada e indiferenciada imposta aos prestadores de serviços de comunicações eletrónicas com base nos artigos L. 851-1 e R. 851-5 do CSI não deve ser considerada, nomeadamente tendo em conta as garantias e os controlos associados aos acessos administrativos aos dados de ligação e à sua utilização, uma ingerência justificada pelo direito à segurança consagrado no artigo 6.º da Carta e pela exigência da segurança nacional, cuja responsabilidade incumbe unicamente aos Estados-Membros por força do artigo 4.º TUE.

63 No que diz respeito, em segundo lugar, às outras obrigações suscetíveis de serem impostas aos prestadores de serviços de comunicações eletrónicas, o órgão jurisdicional de reenvio refere que as disposições do artigo L. 851-2 do CSI autorizam, exclusivamente para efeitos de prevenção do terrorismo, a recolha das informações ou dos documentos previstos no artigo L. 851-1 desse código, junto das mesmas pessoas. Essa recolha, que apenas se aplica a um ou mais indivíduos previamente identificados como possivelmente ligados a uma ameaça terrorista, é realizada em tempo real. O mesmo acontece com as disposições do artigo L. 851-4 do mesmo código, que só autorizam a transmissão em tempo real, pelos operadores, dos dados técnicos relativos à localização dos equipamentos terminais. Estas técnicas regulam, para diferentes fins e segundo diferentes modalidades, os acessos administrativos em tempo real aos dados conservados ao abrigo do CPCE e da

LCEN, mas, no entanto, não impõem aos prestadores em causa uma exigência de conservação adicional em relação ao que é necessário para a faturação e para a prestação dos seus serviços. De igual modo, as disposições do artigo L. 851-3 do CSI, que preveem a obrigação de os prestadores de serviços efetuarem nas suas redes uma análise automatizada das ligações, também não implicam uma conservação generalizada e indiferenciada.

64 Ora, por um lado, o órgão jurisdicional de reenvio considera que tanto a conservação generalizada e indiferenciada como os acessos em tempo real aos dados de ligação apresentam, num contexto marcado por ameaças graves e persistentes à segurança nacional, designadamente pelo risco de terrorismo, uma utilidade operacional ímpar. Com efeito, a conservação generalizada e indiferenciada permite aos serviços de informação acederem aos dados relativos às comunicações antes de serem identificadas as razões pelas quais é possível considerar que a pessoa em causa constitui uma ameaça para a segurança pública, a defesa ou a segurança do Estado. Além disso, os acessos em tempo real aos dados de ligação permitem seguir, com uma alta reatividade, os comportamentos de indivíduos que possam representar uma ameaça imediata para a ordem pública.

65 Por outro lado, a técnica prevista no artigo L. 851-3 do CSI permite detetar, com base em critérios definidos com precisão para o efeito, os indivíduos cujos comportamentos podem, tendo em conta os seus métodos de comunicação, constituir uma ameaça terrorista.

66 Em terceiro lugar, quanto ao acesso das autoridades competentes aos dados conservados, o órgão jurisdicional de reenvio pretende saber se a Diretiva 2002/58, lida à luz da Carta, deve ser interpretada no sentido de que sujeita, em todos os casos, a regularidade dos procedimentos de recolha dos dados de ligação à exigência de informação das pessoas afetadas quando tal informação já não possa comprometer as investigações levadas a cabo pelas autoridades competentes, ou se tais procedimentos podem ser considerados regulares tendo em conta o conjunto das outras garantias processuais existentes, desde que estas últimas garantam a efetividade do direito de recurso.

67 Relativamente a estas outras garantias processuais, o órgão jurisdicional de reenvio precisa, nomeadamente, que qualquer pessoa que pretenda verificar se não lhe estão a ser aplicadas indevidamente técnicas de inteligência pode pedir uma formação especializada do Conseil d'État (Conselho de Estado, em formação jurisdicional) à qual cabe averiguar, à luz dos elementos que lhe foram comunicados fora do procedimento contraditório, se o recorrente é ou não objeto de uma tal técnica e se esta é aplicada nos termos do livro VIII do CSI. Os poderes atribuídos a essa formação para instruir os pedidos garantem a eficácia da fiscalização jurisdicional que exerce. Assim, é competente para analisar os pedidos, declarar oficiosamente quaisquer ilegalidades que constate e ordenar à Administração que adote todas as medidas adequadas para sanar as ilegalidades constatadas. Além disso, cabe à Comissão nacional de controlo das técnicas de informação verificar se as técnicas de recolha de informação são aplicadas, no território nacional, em conformidade com os requisitos decorrentes do CSI. Assim, o facto de as disposições legislativas em causa no processo principal não preverem que as pessoas afetadas devem ser notificadas das medidas de vigilância de que foram objeto não constitui, por si só, uma violação excessiva do direito ao respeito da vida privada.

68 Foi nestas condições que o Conseil d'État (Conselho de Estado, em formação jurisdicional) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Num contexto marcado por ameaças graves e persistentes para a segurança nacional, e em especial pelo risco terrorista, deve a obrigação de conservação generalizada e indiferenciada, imposta aos prestadores com fundamento nas disposições permissivas do artigo 15.º, n.º 1, da Diretiva [2002/58], ser considerada uma ingerência justificada pelo direito das pessoas à segurança, garantido pelo artigo 6.º da [Carta] e pelas exigências de segurança nacional, cuja responsabilidade incumbe unicamente aos Estados-Membros por força do artigo 4.º [TUE]?

2) Deve a Diretiva [2002/58], lida à luz da [Carta], ser interpretada no sentido de que autoriza medidas legislativas, tais como as medidas de recolha em tempo real dos dados relativos ao tráfego e à localização de indivíduos específicos, que, embora afetando os direitos e obrigações dos prestadores de serviços de comunicações eletrónicas, não lhes impõem no entanto uma obrigação específica de conservação dos seus dados?

3) Deve a Diretiva [2002/58], lida à luz da [Carta], ser interpretada no sentido de que sujeita, em todos os casos, a regularidade dos procedimentos de recolha dos dados de ligação à exigência de informação das pessoas afetadas quando tal informação já não possa comprometer as investigações levadas a cabo pelas autoridades competentes, ou podem tais procedimentos ser considerados regulares tendo em conta o conjunto das outras garantias processuais existentes, desde que estas últimas garantam a efetividade do direito de recurso?»

Processo C-512/18

69 Por petição apresentada em 1 de setembro de 2015, a French Data Network, a Quadrature du Net e a Fédération des fournisseurs d'accès à Internet associatifs interpuseram no Conseil d'État (Conselho de Estado, em formação jurisdicional) um recurso de anulação da decisão tácita de indeferimento resultante do silêncio do primeiro-ministro sobre o pedido de revogação do artigo R. 10-13 do CPCE que apresentaram, assim como do Decreto n.º 2011-219, com o fundamento, nomeadamente, de que esses diplomas violam o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º da Carta. Foi admitida a intervenção da Privacy International e do Center for Democracy and Technology no processo principal.

70 Quanto ao artigo R. 10-13 do CPCE e à obrigação de conservação generalizada e indiferenciada dos dados relativos às comunicações aí prevista, o órgão jurisdicional de reenvio, que exprime considerações semelhantes às apresentadas no âmbito do processo C-511/18, observa que tal conservação permite à autoridade judiciária aceder aos dados relativos às comunicações que um indivíduo efetuou antes de ser suspeito de ter cometido uma infração penal, pelo que tal conservação tem uma utilidade ímpar para a investigação, deteção e instauração de ação penal contra as infrações penais.

71 No que diz respeito ao Decreto n.º 2011-219, o órgão jurisdicional de reenvio considera que o artigo 6.º, parte II, da LCEN, que impõe uma obrigação de posse e de conservação apenas quanto aos dados relativos à criação de conteúdo, não se integra no âmbito de aplicação da Diretiva 2002/58, uma vez que este se limita, nos termos do artigo 3.º, n.º 1, desta diretiva, à prestação de serviços de comunicações eletrónicas acessíveis ao público em redes públicas de comunicações na União, mas no âmbito de aplicação da Diretiva 2000/31.

72 No entanto, esse órgão jurisdicional considera que resulta do seu artigo 15.º, n.ºs 1 e 2, que a Diretiva 2000/31 não estabelece uma proibição de princípio quanto à conservação de dados relativos à criação de conteúdo, que apenas poderia ser derrogada por exceção. Assim, coloca-se a questão de saber se os artigos 12.º, 14.º e 15.º da referida diretiva, lidos à luz dos artigos 6.º a 8.º, 11.º e 52.º, n.º 1, da Carta, devem ser interpretados no sentido de que permitem a um Estado-Membro instituir uma legislação nacional, como o artigo 6.º, parte II, da LCEN, que impõe às pessoas em causa a conservação dos dados suscetíveis de permitir a identificação de qualquer pessoa que tenha contribuído para a criação de conteúdos ou de um dos conteúdos dos serviços que prestam, a fim de que a autoridade judiciária possa, sendo caso disso, pedir a sua comunicação para fazer respeitar as regras relativas à responsabilidade civil ou penal.

73 Foi nestas condições que o Conseil d'État (Conselho de Estado, em formação jurisdicional) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Tendo em conta nomeadamente as garantias e os controlos associados à recolha e à utilização dos dados de ligação, deve a obrigação de conservação generalizada e indiferenciada, imposta aos fornecedores com fundamento nas disposições permissivas do artigo 15.º, n.º 1, da Diretiva [2002/58], ser considerada uma ingerência justificada pelo direito das pessoas à segurança, garantido pelo artigo 6.º da [Carta], e pelas exigências de segurança nacional, cuja responsabilidade incumbe unicamente aos Estados-Membros por força do artigo 4.º [TUE]?

2) Devem as disposições da Diretiva [2000/31], lidas à luz dos artigos 6.º, 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da [Carta], ser interpretadas no sentido de que permitem a um Estado-Membro instituir uma regulamentação nacional que impõe às pessoas cuja atividade consiste em proporcionar acesso a serviços em linha de comunicação com o público e às pessoas singulares ou coletivas que asseguram, mesmo a título gratuito, para a colocação à disposição do público através de serviços de comunicação ao público em linha, o armazenamento de sinais, textos, imagens, sons, ou mensagens de qualquer natureza fornecidos por destinatários desses serviços, a conservação dos dados suscetíveis de permitir a identificação de qualquer pessoa que tenha contribuído para a criação de conteúdos ou de um dos conteúdos dos serviços que prestam, a fim de que a autoridade judiciária possa, sendo caso disso, pedir a sua comunicação para fazer respeitar as regras relativas à responsabilidade civil ou penal?»

Processo C-520/18

74 Por petições apresentadas em 10 de janeiro, 16 de janeiro, 17 de janeiro e 18 de janeiro de 2017, apensadas no processo principal, a Ordre des barreaux francophones et germanophone, a Académie Fiscale ASBL e UA, a Liga voor Mensenrechten ASBL e a Ligue des Droits de l'Homme ASBL, VZ, WY e XX interpuseram na Cour constitutionnelle (Tribunal Constitucional, Bélgica) recursos de anulação da Lei de 29 de maio de 2016, com o fundamento de que esta viola os artigos 10.º e 11.º da Constituição belga, em conjugação com os artigos 5.º, 6.º a 11.º, 14.º, 15.º, 17.º e 18.º da CEDH, os artigos 7.º, 8.º, 11.º, 47.º e 52.º, n.º 1, da Carta, o artigo 17.º do Pacto Internacional sobre os Direitos Civis e Políticos, adotado pela Assembleia-Geral das Nações Unidas em 16 de dezembro de 1966 e que entrou em vigor em 23 de março de 1976, os princípios gerais da segurança jurídica, da proporcionalidade e da autodeterminação em matéria de informação, assim como o artigo 5.º, n.º 4, TUE.

75 Em apoio dos seus recursos, os recorrentes no processo principal alegam, em substância, que a ilegalidade da Lei de 29 de maio de 2016 resulta, nomeadamente, do facto de esta ultrapassar os limites do estritamente necessário e não prever garantias de proteção suficientes. Em particular, nem as suas disposições relativas à conservação dos dados nem as suas disposições que regulam o acesso das autoridades aos dados conservados cumprem os requisitos que decorrem do Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, a seguir «Acórdão Digital Rights», EU:C:2014:238), e do Acórdão de 21 de dezembro de 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970). Com efeito, estas disposições geram o risco de serem estabelecidos perfis de personalidade, que podem ser abusivamente utilizados pelas autoridades competentes, e também não preveem um nível adequado de segurança e de proteção dos dados conservados. Por último, essa lei abrange as pessoas sujeitas ao segredo profissional e as pessoas que têm obrigação de confidencialidade e diz respeito a dados de comunicação sensíveis, de caráter pessoal, sem incluir garantias especiais para os proteger.

76 O órgão jurisdicional de reenvio afirma que os dados que devem ser conservados pelos prestadores de serviços de telefonia, incluindo por Internet, de acesso à Internet e de correio eletrónico por Internet, assim como pelos operadores que fornecem redes públicas de comunicações eletrónicas, por força da

Lei de 29 de maio de 2016, são idênticos aos enumerados na 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), não estando prevista uma distinção quanto às pessoas em causa ou em função do objetivo prosseguido. A este respeito, o referido órgão jurisdicional precisa que o objetivo prosseguido pelo legislador através desta lei é não só lutar contra o terrorismo e a pornografia infantil mas também poder utilizar os dados conservados numa grande variedade de situações no âmbito do inquérito penal. Além disso, o órgão jurisdicional de reenvio considera que resulta da exposição de motivos da referida lei que o legislador nacional considerou que era impossível, à luz do objetivo prosseguido, instituir uma obrigação de conservação específica e diferenciada, e que optou por fazer acompanhar a obrigação de conservação geral e indiferenciada de garantias estritas, tanto no plano dos dados conservados como no plano do acesso aos mesmos, a fim de limitar ao mínimo a ingerência no direito ao respeito da vida privada.

77 O órgão jurisdicional de reenvio acrescenta que o artigo 126.º, n.º 2, pontos 1 e 2, da Lei de 13 de junho de 2005, na sua versão resultante da Lei de 29 de maio de 2016, prevê as condições em que, respetivamente, as autoridades judiciárias e os serviços de informação e de segurança podem obter acesso aos dados conservados, pelo que a apreciação da legalidade dessa lei à luz das exigências do direito da União deve ser suspensa até que o Tribunal de Justiça se pronuncie em dois processos prejudiciais pendentes, relativos a tal acesso.

78 Por último, o órgão jurisdicional de reenvio refere que a Lei de 29 de maio de 2016 visa permitir uma instrução penal eficaz e sanções efetivas em caso de abuso sexual de menores, bem como possibilitar a identificação do autor desse crime, mesmo quando são utilizados meios de comunicações eletrónicos. No processo que decide, foi chamada a atenção, a esse respeito, para as obrigações positivas decorrentes dos artigos 3.º e 8.º da CEDH. Essas obrigações podem igualmente decorrer das disposições correspondentes da Carta, suscetíveis de ter repercussões na interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58.

79 Foi nestas condições que a Cour constitutionnelle (Tribunal Constitucional) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Deve o artigo 15.º, n.º 1, da Diretiva [2002/58], lido em conjugação com o direito à segurança, garantido pelo artigo 6.º da [Carta], e o direito ao respeito dos dados pessoais, garantido pelos artigos 7.º, 8.º e 52.º, n.º 1, da [Carta], ser interpretado no sentido de que se opõe a uma regulamentação nacional como a que está em causa, que prevê uma obrigação geral de os operadores e prestadores de serviços de comunicações eletrónicas conservarem os dados de tráfego e de localização na aceção da Diretiva [2002/58], gerados ou tratados por estes no âmbito da prestação de tais serviços, regulamentação nacional que não tem apenas por objetivo a investigação, a deteção e a instauração de procedimento criminal em relação a factos constitutivos de criminalidade grave, mas igualmente a garantia da segurança nacional, a defesa do território e a segurança pública, a investigação, a deteção e a instauração de procedimento criminal em relação a factos não constitutivos de criminalidade grave ou a prevenção de uma utilização proibida dos sistemas de comunicação eletrónica, ou a realização de outro objetivo identificado pelo artigo 23.º, n.º 1, do Regulamento [2016/679] e que, além disso, está sujeita a garantias precisadas nesta regulamentação no plano da conservação dos dados e do acesso aos mesmos?

2) Deve o artigo 15.º, n.º 1, da Diretiva [2002/58], conjugado com os artigos 4.º, 7.º, 8.º, 11.º e 52.º, n.º 1, da [Carta], ser interpretado no sentido de que se opõe a uma regulamentação nacional como a que está em causa, que prevê uma obrigação geral de os operadores e prestadores de serviços de comunicações eletrónicas conservarem os dados de tráfego e de localização na aceção da Diretiva [2002/58], gerados ou tratados por estes no âmbito da prestação de tais serviços, se esta regulamentação tiver designadamente por objeto o cumprimento das obrigações positivas que incumbem à autoridade por força dos artigos 4.º e [7.º] da Carta, que consistem em prever um

quadro legal que permita uma fase de inquérito efetiva e uma repressão efetiva do abuso sexual de menores e que permita efetivamente identificar o autor do crime, mesmo quando são utilizados meios de comunicações eletrónicos?

3) No caso de, com base nas respostas à primeira ou à segunda questão prejudicial, o Tribunal Constitucional concluir que a lei impugnada viola uma ou mais das obrigações decorrentes das disposições referidas nestas questões, pode manter provisoriamente os efeitos da Lei de [29 de maio de 2016], a fim de evitar a insegurança jurídica e permitir que os dados recolhidos e conservados anteriormente possam ainda ser utilizados para efeitos dos objetivos prosseguidos pela lei?»

Tramitação do processo no Tribunal de Justiça

80 Por decisão do presidente do Tribunal de Justiça de 25 de setembro de 2018, os processos C-511/18 e C-512/18 foram apensados para efeitos das fases escrita e oral e do acórdão. O processo C-520/18 foi apensado a esses processos por decisão do presidente do Tribunal de Justiça de 9 de julho de 2020 para efeitos do acórdão.

Quanto às questões prejudiciais

Quanto às primeiras questões nos processos C-511/18 e C-512/18 e quanto à primeira e segunda questões no processo C-520/18

81 Com as primeiras questões nos processos C-511/18 e C-512/18 e com a primeira e segunda questões no processo C-520/18, que devem ser apreciadas em conjunto, os órgãos jurisdicionais pretendem saber, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58 deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que impõe aos prestadores de serviços de comunicações eletrónicas, para os fins previstos neste artigo 15.º, n.º 1, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização.

Observações preliminares

82 Resulta dos autos no Tribunal de Justiça que as regulamentações em causa no processo principal abrangem todos os meios de comunicações eletrónicos e englobam todos os utilizadores destes meios, sem que seja estabelecida uma diferenciação ou uma exceção a este respeito. Além disso, os dados que essas regulamentações obrigam os prestadores de serviços de comunicações eletrónicas a conservar são, designadamente, aqueles que são necessários para encontrar a fonte de uma comunicação e o seu destino, determinar a data, hora, duração e tipo da comunicação, identificar o material de comunicação utilizado e localizar os equipamentos terminais e as comunicações, entre os quais figuram, nomeadamente, o nome e o endereço do utilizador, os números de telefone da pessoa que efetua a chamada e o endereço IP para os serviços de Internet. Em contrapartida, os referidos dados não abrangem o conteúdo das comunicações em causa.

83 Assim, os dados que devem, em virtude das regulamentações nacionais em causa no processo principal, ser conservados durante um ano permitem saber, nomeadamente, qual é a pessoa com a qual o utilizador de um meio de comunicação eletrónica comunicou e através de que meio foi feita essa comunicação, determinar a data, hora e duração das comunicações e das ligações à Internet, bem como o local a partir do qual essas foram feitas, e conhecer a localização dos equipamentos terminais sem que tenha necessariamente sido transmitida uma comunicação. Além disso, oferecem a possibilidade de determinar a frequência das comunicações do utilizador com algumas pessoas durante um certo período. Por último, no que diz respeito à regulamentação nacional em causa nos

processos C-511/18 e C-512/18, verifica-se que, uma vez que abrange igualmente os dados relativos ao encaminhamento das comunicações eletrónicas pelas redes, permite igualmente identificar a natureza das informações consultadas em linha.

84 Quanto às finalidades prosseguidas, importa salientar que as regulamentações em causa nos processos C-511/18 e C-512/18 visam, entre outras finalidades, a investigação, a deteção e a instauração de ação penal contra as infrações penais em geral, a independência nacional, a integridade do território e a defesa nacional, os interesses fundamentais da política estrangeira, a execução dos compromissos europeus e internacionais de França, os interesses económicos, industriais e científicos fundamentais de França, bem como a prevenção do terrorismo, os atentados à forma republicana das instituições e os atos de violência coletiva suscetíveis de atentar gravemente contra a paz pública. Quanto à regulamentação em causa no processo C-520/18, tem por objetivos, nomeadamente, a investigação, a deteção e a instauração de ação penal contra as infrações penais, assim como a salvaguarda da segurança nacional, da defesa do território e da segurança pública.

85 Os órgãos jurisdicionais de reenvio questionam, em particular, as eventuais incidências na interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, do direito à segurança consagrado no artigo 6.º da Carta. De igual modo, perguntam se a ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que a conservação de dados prevista pelas regulamentações em causa no processo principal implica pode ser considerada justificada tendo em conta a existência de regras que restringem o acesso das autoridades nacionais aos dados conservados. Além disso, segundo o Conseil d'État (Conselho de Estado, em formação jurisdicional), uma vez que esta questão é colocada num quadro marcado por ameaças graves e persistentes para a segurança nacional, deve ser igualmente apreciada à luz do artigo 4.º, n.º 2, TUE. A Cour constitutionnelle (Tribunal Constitucional), por sua vez, sublinha que a regulamentação em causa no processo C-520/18 também dá execução a obrigações positivas decorrentes dos artigos 4.º e 7.º da Carta, que consistem na instituição de um quadro legal que permita a repressão efetiva do abuso sexual de menores.

86 Embora tanto o Conseil d'État (Conselho de Estado, em formação jurisdicional) como a Cour constitutionnelle (Tribunal Constitucional) partam da premissa de que as regulamentações nacionais em causa no processo principal, que regulam a conservação de dados de tráfego e de dados de localização, bem como o acesso a estes dados pelas autoridades nacionais para os fins previstos no artigo 15.º, n.º 1, da Diretiva 2002/58, designadamente a salvaguarda da segurança nacional, se integram no âmbito de aplicação desta diretiva, algumas partes no processo principal e alguns dos Estados-Membros que apresentaram observações escritas ao Tribunal de Justiça têm uma opinião diferente a esse respeito, em particular no que se refere ao artigo 1.º, n.º 3, da mesma diretiva. Por conseguinte, antes de mais, importa apreciar se tais regulamentações estão abrangidas pelo âmbito de aplicação da referida diretiva.

Quanto ao âmbito de aplicação da Diretiva 2002/58

87 A Quadrature du Net, a Fédération des fournisseurs d'accès à Internet associatifs, a Igwan.net, a Privacy International e o Center for Democracy and Technology alegam, em substância, invocando a este respeito a jurisprudência do Tribunal de Justiça relativa ao âmbito de aplicação da Diretiva 2002/58, que tanto a conservação de dados como o acesso aos dados conservados se integram nesse âmbito de aplicação, quer esse acesso ocorra em tempo diferido quer em tempo real. Com efeito, uma vez que o objetivo da salvaguarda da segurança nacional está expressamente referido no artigo 15.º, n.º 1, desta diretiva, a sua prossecução não implica a inaplicabilidade da referida diretiva. O artigo 4.º, n.º 2, TUE, invocado pelos órgãos jurisdicionais de reenvio, não afeta esta apreciação.

88 No que diz respeito às medidas de informação que as autoridades francesas competentes aplicam diretamente sem regular a atividade dos prestadores de serviços de comunicações eletrónicas impondo-lhes obrigações específicas, o Center for Democracy and Technology observa que tais

medidas se integram necessariamente no âmbito de aplicação da Diretiva 2002/58 e no âmbito de aplicação da Carta, uma vez que constituem derrogações ao princípio da confidencialidade consagrado no artigo 5.º desta diretiva. Assim, as referidas medidas devem respeitar os requisitos previstos no artigo 15.º, n.º 1, da mesma diretiva.

89 Em contrapartida, os Governos francês, checo e estónio, a Irlanda, os Governos cipriota, húngaro, polaco, sueco e do Reino Unido alegam, em substância, que a Diretiva 2002/58 não é aplicável a regulamentações nacionais como as que estão em causa no processo principal, dado que estas têm por finalidade a salvaguarda da segurança nacional. As atividades dos serviços de informação, uma vez que são relativas à manutenção da ordem pública e à salvaguarda da segurança interna e da integridade territorial, fazem parte das funções essenciais dos Estados-Membros e, por conseguinte, são da exclusiva competência destes últimos, como demonstra, nomeadamente, o artigo 4.º, n.º 2, terceiro período, TUE.

90 Estes Governos, assim como a Irlanda, referem, além disso, o artigo 1.º, n.º 3, da Diretiva 2002/58, que exclui do âmbito de aplicação desta, à semelhança do que já previa o artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, as atividades relativas à segurança pública, à defesa e à segurança do Estado. A este respeito, apoiam-se na interpretação desta última disposição que figura no Acórdão de 30 de maio de 2006, Parlamento/Conselho e Comissão (C-317/04 e C-318/04, EU:C:2006:346).

91 A este respeito, importa referir que, nos termos do seu artigo 1.º, n.º 1, a Diretiva 2002/58 prevê, nomeadamente, a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, e em particular do direito à privacidade e à confidencialidade, no que diz respeito ao tratamento de dados pessoais no setor das comunicações eletrónicas.

92 O artigo 1.º, n.º 3, desta diretiva exclui do seu âmbito de aplicação as «atividades do Estado» nos domínios aí referidos, entre as quais figuram as atividades do Estado no domínio penal e as relacionadas com a segurança pública, a defesa, a segurança do Estado, incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado. As atividades assim referidas a título de exemplo serão, em qualquer caso, atividades próprias dos Estados ou das autoridades estatais, alheias aos domínios de atividade dos particulares (Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 32 e jurisprudência aí referida).

93 Além disso, o artigo 3.º da Diretiva 2002/58 enuncia que esta diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas publicamente disponíveis nas redes públicas de comunicações na União, incluindo as redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação (a seguir «serviços de comunicações eletrónicas»). Por conseguinte, deve considerar-se que a referida diretiva regula as atividades dos prestadores de tais serviços (Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 33 e jurisprudência aí referida).

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

95 Ora, o artigo 15.º, n.º 1, da Diretiva 2002/58 pressupõe necessariamente que as medidas nacionais aí referidas estão abrangidas pelo âmbito de aplicação da referida diretiva, uma vez que esta última só autoriza expressamente os Estados-Membros a adotá-las respeitando as condições nela previstas. Além disso, tais medidas regulam, para os efeitos mencionados nesta disposição, a atividade dos prestadores de serviços de comunicações eletrónicas (Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 34 e jurisprudência aí referida).

96 Em particular, à luz destas considerações, o Tribunal de Justiça declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido em conjugação com o artigo 3.º da mesma, deve ser interpretado no sentido de que está abrangida pelo âmbito de aplicação desta diretiva, não só uma medida legislativa que impõe aos prestadores de serviços de comunicações eletrónicas a conservação de dados de tráfego e de dados de localização, mas também uma medida legislativa que lhes impõe o dever de concederem às autoridades nacionais competentes o acesso a esses dados. Com efeito, tais medidas legislativas implicam obrigatoriamente um tratamento, por estes prestadores, dos referidos dados e, uma vez que regulam as atividades destes mesmos prestadores, não podem ser equiparadas às atividades próprias dos Estados, mencionadas no artigo 1.º, n.º 3, da referida diretiva (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.ºs 35 e 37 e jurisprudência aí referida).

97 Além disso, tendo em conta as considerações que figuram no n.º 95 do presente acórdão e a sistemática geral da Diretiva 2002/58, uma interpretação desta diretiva no sentido de as medidas legislativas referidas no seu artigo 15.º, n.º 1, estarem excluídas do seu âmbito de aplicação devido ao facto de as finalidades às quais tais medidas devem responder coincidirem substancialmente com as finalidades prosseguidas pelas atividades referidas no artigo 1.º, n.º 3, da mesma diretiva, priva este artigo 15.º, n.º 1, de qualquer efeito útil (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.ºs 72 e 73).

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

99 O disposto no artigo 4.º, n.º 2, TUE, a que se referem os Governos mencionados no n.º 89 do presente acórdão, não pode invalidar esta conclusão. Com efeito, em conformidade com jurisprudência constante do Tribunal de Justiça, embora incumba aos Estados-Membros definir os seus interesses essenciais de segurança e adotar as medidas adequadas para garantir a sua segurança interna e externa, o simples facto de uma medida nacional ter sido adotada para efeitos da proteção da segurança nacional não pode implicar a inaplicabilidade do direito da União e dispensar os Estados-Membros do respeito necessário desse direito [v., neste sentido, Acórdãos de 4 de junho de 2013, ZZ, C-300/11, EU:C:2013:363, n.º 38; de 20 de março de 2018, Comissão/Áustria (Imprensa do Estado), C-187/16, EU:C:2018:194, n.ºs 75 e 76; e de 2 de abril de 2020, Comissão/Polónia, Hungria e República checa (Mecanismo temporário de recolocação de requerentes de proteção internacional), C-715/17, C-718/17 e C-719/17, EU:C:2020:257, n.ºs 143 e 170].

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

101 No entanto, tendo em conta as considerações que figuram nos n.ºs 93, 95 e 96 do presente acórdão, esta jurisprudência não é transponível para a interpretação do artigo 1.º, n.º 3, da Diretiva 2002/58. Com efeito, como salientou, em substância, o advogado-geral nos n.ºs 70 a 72 das Conclusões que apresentou nos processos apensos La Quadrature du Net e o. (C-511/18 e C-512/18, EU:C:2020:6), o artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, ao qual se refere essa jurisprudência, excluía do âmbito de aplicação desta última diretiva, de forma geral, o «tratamento de dados que tenha por objeto a segurança pública, a defesa, a segurança do Estado», sem estabelecer uma distinção em função do autor do tratamento de dados em causa. Em contrapartida, no âmbito da interpretação do artigo 1.º, n.º 3, da Diretiva 2002/58, esta distinção revela-se necessária. Com efeito, conforme resulta dos n.ºs 94

a 97 do presente acórdão, todos os tratamentos de dados pessoais efetuados pelos prestadores de serviços de comunicações eletrónicas se integram no âmbito de aplicação da referida diretiva, incluindo os tratamentos que decorrem de obrigações que lhes são impostas pelos poderes públicos, embora, eventualmente, estes tratamentos possam ser abrangidos pelo âmbito de aplicação da exceção prevista no artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, tendo em conta a formulação mais ampla desta disposição, que visa todos os tratamentos, independentemente do seu autor, que tenham por objeto a segurança pública, a defesa, a segurança do Estado.

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

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

104 Resulta das considerações anteriores que uma regulamentação nacional que impõe aos prestadores de serviços de comunicações eletrónicas a conservação de dados de tráfego e de dados de localização para efeitos da proteção da segurança nacional e da luta contra a criminalidade, tal como os que estão em causa no processo principal, se integra no âmbito de aplicação da Diretiva 2002/58.

Quanto à interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58

105 Importa recordar, a título preliminar, que é jurisprudência constante que, para interpretar uma disposição do direito da União, deve ter-se 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 (v., neste sentido, Acórdão de 17 de abril de 2018, Egenberger, C-414/16, EU:C:2018:257, n.º 44).

106 A Diretiva 2002/58 tem por finalidade, como resulta nomeadamente dos seus considerandos 6 e 7, proteger os utilizadores dos serviços de comunicações eletrónicas contra os riscos para os seus dados pessoais e a sua vida privada resultantes das novas tecnologias e, nomeadamente, da maior capacidade de armazenamento e tratamento automatizado de dados. Em particular, como estabelece o seu considerando 2, a referida diretiva visa assegurar o pleno respeito pelos direitos consignados nos artigos 7.º e 8.º da Carta. A este respeito, resulta da exposição de motivos da proposta de diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no 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».

107 Para o efeito, 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 impõe, nomeadamente, que, em princípio, pessoas que não os utilizadores estejam proibidas de armazenar, sem o consentimento destes, essas comunicações e esses dados.

108 No que diz respeito, em especial, ao tratamento e ao armazenamento dos dados de tráfego pelos prestadores de serviços de comunicações eletrónicas, resulta do artigo 6.º e dos considerandos 22 e 26 da Diretiva 2002/58 que tal tratamento só é autorizado na medida e pelo período de tempo necessários para a faturação de serviços, para a comercialização destes e para a prestação de serviços de valor acrescentado. Depois de expirado esse período de tempo, os dados que tenham sido tratados e armazenados devem ser apagados ou tornados anónimos. No que se refere aos dados de localização diferentes dos dados de tráfego, o artigo 9.º, n.º 1, da referida diretiva prevê que esses dados só podem ser tratados sob certas condições e depois de terem sido tornados anónimos ou com o consentimento dos utilizadores ou dos assinantes (Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 86 e jurisprudência aí referida).

109 Assim, ao adotar essa diretiva, o legislador da União concretizou os direitos consagrados nos artigos 7.º e 8.º da Carta, pelo que os utilizadores dos meios de comunicações 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.

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

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

112 Quanto aos objetivos suscetíveis de justificar uma limitação 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, da Diretiva 2002/58 tem caráter taxativo, de modo que uma medida legislativa adotada ao abrigo desta disposição tem que responder efetiva e estritamente a um desses objetivos (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 52 e jurisprudência aí referida).

113 Além disso, resulta do artigo 15.º, n.º 1, terceiro período, da Diretiva 2002/58 que os Estados-Membros apenas estão autorizados a adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º, 6.º e 9.º desta diretiva que respeitem os princípios gerais do direito da União, incluindo o princípio da proporcionalidade e os direitos fundamentais garantidos pela Carta. A este respeito, o Tribunal de Justiça já declarou que a obrigação imposta por um Estado-Membro aos prestadores de serviços de comunicações eletrónicas, 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 (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, n.os 25 e 70, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.os 91 e 92 e jurisprudência aí referida).

114 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 (v., neste sentido, Acórdãos de 6 de março de 2001, Connolly/Comissão, C-274/99 P, EU:C:2001:127, n.º 39, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 93 e jurisprudência aí referida).

115 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 [v., neste sentido, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.os 124 e 126 e jurisprudência aí referida; v., por analogia, no que diz respeito ao artigo 8.º da CEDH, TEDH, 30 de janeiro de 2020, Breyer c. Alemanha, CE:ECHR:2020:0130JUD005000112, § 81].

116 É igualmente irrelevante que os dados conservados sejam ou não utilizados posteriormente (v., por analogia, no que diz respeito ao artigo 8.º da CEDH, TEDH, 16 de fevereiro de 2000, Amann c. Suíça, CE:ECHR:2000:0216JUD002779895, § 69, e de 13 de fevereiro de 2020, Trjakovski e Chipovski c. Macedónia do Norte, CE:ECHR:2020:0213JUD005320513, § 51), uma vez que o acesso a tais dados constitui, independentemente da utilização que deles seja feita posteriormente, uma ingerência distinta nos direitos fundamentais referidos no número anterior [v., neste sentido, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.os 124 e 126].

117 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 forma permanente ou temporária, 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 (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, n.º 27, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 99).

118 Por conseguinte, por um lado, a conservação de dados de tráfego e de dados de localização para fins policiais é suscetível, por si só, de violar o direito ao respeito das comunicações, consagrado no artigo 7.º da Carta, e de produzir efeitos dissuasivos sobre o exercício, pelos utilizadores dos meios de

comunicações eletrónicos, da sua liberdade de expressão, garantida no artigo 11.º da referida Carta (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, n.º 28, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 101). Ora, esses efeitos dissuasivos podem afetar, em especial, as pessoas cujas comunicações estão sujeitas, segundo as regras nacionais, ao segredo profissional, bem como os denunciantes cujas atividades estão protegidas pela Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União (JO 2019, L 305, p. 17). Além disso, esses efeitos são tanto mais graves quanto maiores sejam o número e a variedade dos dados conservados.

119 Por outro lado, tendo em conta a quantidade significativa de dados de tráfego e de dados de localização que podem ser conservados de forma contínua 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.

120 Assim sendo, na medida em que permite aos Estados-Membros introduzir as derrogações referidas no n.º 110 do presente acórdão, o artigo 15.º, n.º 1, da Diretiva 2002/58 reflete o facto 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 (v., neste sentido, Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, n.º 172 e jurisprudência aí referida).

121 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.

122 Assim, a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58 à luz da Carta exige que se tenha igualmente em conta 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.

123 A este respeito, o artigo 6.º da Carta, a que se refere o Conseil d'État (Conselho de Estado, em formação jurisdicional) e a Cour constitutionnelle (Tribunal Constitucional), consagra o direito de qualquer pessoa não apenas à liberdade mas também à segurança e garante direitos correspondentes aos que estão previstos no artigo 5.º da CEDH (v., neste sentido, Acórdãos de 15 de fevereiro de 2016, N., C-601/15 PPU, EU:C:2016:84, n.º 47; de 28 de julho de 2016, JZ, C-294/16 PPU, EU:C:2016:610, n.º 48; e de 19 de setembro de 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, n.º 42 e jurisprudência aí referida).

124 Além disso, importa recordar que o artigo 52.º, n.º 3, da Carta visa assegurar a coerência necessária entre os direitos nela contidos e os direitos correspondentes garantidos pela CEDH, sem pôr em causa a autonomia do direito da União e do Tribunal de Justiça da União Europeia. Assim, há que ter em conta os direitos correspondentes da CEDH para efeitos da interpretação da Carta, enquanto limiar de proteção mínima [v., neste sentido, Acórdãos de 12 de fevereiro de 2019, TC, C-492/18 PPU, EU:C:2019:108, n.º 57, e de 21 de maio de 2019, Comissão/Hungria (Usufruto de terrenos agrícolas), C-235/17, EU:C:2019:432, n.º 72 e jurisprudência aí referida].

125 No que diz respeito ao artigo 5.º da CEDH, que consagra o «direito à liberdade» e o «direito à segurança», este visa, segundo a jurisprudência do Tribunal Europeu dos Direitos do Homem, proteger o indivíduo contra qualquer privação de liberdade arbitrária ou injustificada (v., neste sentido, TEDH, 18 de março de 2008, Ladent c. Polónia, CE:ECHR:2008:0318JUD001103603, §§ 45

e 46; 29 de março de 2010, Medvedyev e outros c. França, CE:ECHR:2010:0329JUD000339403, §§ 76 e 77, e de 13 de dezembro de 2012, El-Masri v. «The former Yugoslav Republic of Macedonia», CE:ECHR:2012:1213JUD003963009, § 239). No entanto, uma vez que esta disposição visa uma privação de liberdade imposta por uma autoridade pública, o artigo 6.º da Carta não pode ser interpretado no sentido de que impõe aos poderes públicos a obrigação de adotarem medidas específicas para instaurarem ação penal contra determinadas infrações penais.

126 Em contrapartida, no que diz respeito, em particular, à luta efetiva contra as infrações penais de que são vítimas, nomeadamente, menores e outras pessoas vulneráveis, evocada pela Cour constitutionnelle (Tribunal Constitucional), importa sublinhar que podem resultar do artigo 7.º da Carta obrigações positivas que incumbem ao poderes públicos, tendo em vista a adoção de medidas jurídicas destinadas a proteger a vida privada e familiar [v., neste sentido, Acórdão de 18 de junho de 2020, Comissão/Hungria (Transparência associativa), C-78/18, EU:C:2020:476, n.º 123 e jurisprudência referida do Tribunal Europeu dos Direitos do Homem]. 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.

127 Ora, tendo em conta estas diferentes obrigações positivas, há que proceder à necessária ponderação dos diferentes interesses e direitos em causa.

128 Com efeito, o Tribunal Europeu dos Direitos do Homem declarou que as obrigações positivas decorrentes dos artigos 3.º e 8.º da CEDH, 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. Assim sendo, 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 e direitos a proteger (TEDH, 28 de outubro de 1998, Osman c. Reino Unido, CE:ECHR:1998:1028JUD002345294, §§ 115 e 116; 4 de março de 2004, M.C. c. Bulgária, CE:ECHR:2003:1204JUD003927298, § 151; 24 de junho de 2004, Von Hannover c. Alemanha, CE:ECHR:2004:0624JUD005932000, §§ 57 e 58, e de 2 de dezembro de 2008, K.U. c. Finlândia, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 e 49).

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

130 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 limitações 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 [v., neste sentido, Acórdãos de 16 de dezembro de 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, EU:C:2008:727, n.º 56; de 9 de novembro de 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, n.ºs 76, 77 e 86; e de 8 de abril de 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, n.º 52; Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 140].

131 Mais particularmente, decorre da jurisprudência do Tribunal de Justiça que a possibilidade de os Estados-Membros justificarem uma limitação 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 limitação implica e da verificação de que a importância do objetivo de interesse geral prosseguido por esta limitação está relacionada com essa gravidade. (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 55 e jurisprudência aí referida).

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

133 Assim, uma regulamentação que prevê uma conservação de dados pessoais deve sempre pautar-se por critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido [v., neste sentido, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.os 191 e jurisprudência aí referida, e Acórdão de 3 de outubro de 2019, A e o., C-70/18, EU:C:2019:823, n.º 63].

– Quanto às medidas legislativas que preveem a conservação preventiva de dados de tráfego e de dados de localização para efeitos da salvaguarda da segurança nacional

134 Há que observar que o objetivo de salvaguarda da segurança nacional, evocado pelos órgãos jurisdicionais de reenvio e pelos Governos que apresentaram observações, ainda não foi especificamente apreciado pelo Tribunal de Justiça nos seus acórdãos relativos à interpretação da Diretiva 2002/58.

135 A este respeito, importa começar por assinalar que o artigo 4.º, n.º 2, TUE estabelece que a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro. Esta responsabilidade corresponde ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da sociedade e inclui a prevenção e a repressão de atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país, em especial de ameaçar diretamente a sociedade, a população ou o Estado enquanto tal, como, nomeadamente, as atividades terroristas.

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

137 Assim, em situações como as descritas nos n.os 135 e 136 do presente acórdão, 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, não se opõe, em princípio, a uma medida legislativa que autoriza as autoridades competentes a impor aos prestadores de serviços de comunicações eletrónicas o dever de procederem à conservação de dados de tráfego e de dados de localização de todos os utilizadores de meios de comunicações eletrónicos durante um período limitado, desde que existam circunstâncias suficientemente concretas que permitam considerar que o Estado-Membro em causa enfrenta uma ameaça grave como a referida nos n.os 135 e 136 do presente acórdão para a segurança nacional que se afigure real e atual ou previsível. Embora tal medida vise, de forma indiferenciada, todos os utilizadores de meios de comunicações eletrónicos sem que, à primeira vista, se afigure estarem relacionados, na aceção da jurisprudência referida no n.º 133 do presente acórdão, com uma ameaça para a segurança nacional desse Estado-Membro, há que considerar, no entanto, que a existência de tal ameaça é, por si só, suscetível de demonstrar essa relação.

138 A imposição de conservação preventiva dos dados de todos os utilizadores dos meios de comunicações eletrónicos deve, não obstante, ser temporalmente limitada ao estritamente necessário. Embora não se possa excluir a possibilidade de a imposição aos prestadores de serviços de comunicações eletrónicas de procederem à conservação dos dados, devido à persistência de tal ameaça, ser renovada, a duração de cada imposição não pode ultrapassar um período de tempo previsível. Além disso, tal conservação dos dados deve estar sujeita a limitações e enquadrada por garantias estritas que permitam proteger eficazmente os dados pessoais das pessoas em causa contra os riscos de abuso. Assim, essa conservação não pode ter caráter sistemático.

139 Tendo em conta a gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta resultante dessa medida de conservação generalizada e indiferenciada de dados, há que assegurar que o recurso a esta se limita efetivamente às situações em que exista uma ameaça grave para a segurança nacional, tais como as referidas nos n.os 135 e 136 do presente acórdão. Para o efeito, é essencial que uma decisão que impõe aos prestadores de serviços de comunicações eletrónicas que procedam a tal conservação de dados possa ser objeto de fiscalização efetiva quer por um órgão jurisdicional quer por uma entidade administrativa 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.

– Quanto às medidas legislativas que preveem a conservação preventiva de dados de tráfego e de dados de localização para efeitos da luta contra a criminalidade e da salvaguarda da segurança pública

140 No que diz respeito ao objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais, 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 [v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 102, e de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.os 56 e 57; Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 149].

141 Uma regulamentação nacional que prevê a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, com vista a lutar contra a criminalidade grave, excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática, como exige 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 (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 107).

142 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 tendo em conta, por um lado, os efeitos dissuasivos no exercício dos direitos fundamentais consagrados nos artigos 7.º e 11.º da Carta, referidos no n.º 118 do presente acórdão, que a conservação desses dados pode produzir e, por outro, a 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.

143 Além disso, o Tribunal de Justiça sublinhou que uma regulamentação 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 regulamentação, contrariamente à exigência recordada no n.º 133 do presente acórdão, 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 se encontra prevista e uma ameaça para a segurança pública (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, n.ºs 57 e 58, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 105).

144 Em particular, como já declarou o Tribunal de Justiça, tal regulamentação 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 alguma forma 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 (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, n.º 59, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 106).

145 Ora, mesmo as obrigações positivas dos Estados-Membros que possam decorrer, consoante os casos, dos artigos 3.º, 4.º e 7.º da Carta e relativas, conforme referido nos n.ºs 126 e 128 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 regulamentação 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.

146 Em contrapartida, em conformidade com o que foi referido nos n.ºs 142 a 144 do presente acórdão, e tendo em consideração a necessária ponderação dos direitos e dos interesses em causa, os objetivos de luta contra a criminalidade grave, de prevenção de ofensas graves à segurança pública e, *a fortiori*, de salvaguarda da segurança nacional são suscetíveis de justificar, tendo em conta a sua importância, à luz das obrigações positivas recordadas no número anterior e às quais se referiu, nomeadamente, a Cour constitutionnelle (Tribunal Constitucional), a ingerência particularmente grave que comporta uma conservação selecionada de dados de tráfego e de dados de localização.

147 Assim, como já declarou o Tribunal de Justiça, 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, não se opõe a que um Estado-Membro adote uma regulamentação que permita, a título preventivo, a conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da luta contra a criminalidade grave e da prevenção das ameaças graves contra a segurança pública, tal como para efeitos da salvaguarda da segurança nacional, desde

que tal conservação seja, no que diz respeito às categorias de dados a conservar, aos meios de comunicação visados, às pessoas em causa e à duração de conservação fixada, limitada ao estritamente necessário (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 108).

148 No que diz respeito à delimitação de que é objeto, essa medida de conservação de dados pode, nomeadamente, ser fixada em função das categorias de pessoas em causa, uma vez que o artigo 15.º, n.º 1, da Diretiva 2002/58 não se opõe a uma regulamentação baseada em elementos objetivos, que permitam visar 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 de uma maneira ou outra 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 (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 111).

149 A este respeito, importa precisar que as pessoas assim visadas podem ser, nomeadamente, aquelas que foram previamente identificadas, no âmbito dos processos nacionais aplicáveis e com base em elementos objetivos, como uma ameaça para a segurança pública ou para a segurança nacional do Estado-Membro em causa.

150 A delimitação de uma medida que prevê a conservação de dados de tráfego e de dados de localização pode igualmente assentar num critério geográfico quando as autoridades nacionais competentes considerem, com base em elementos objetivos e não discriminatórios, que existe, numa ou em mais zonas geográficas, uma situação caracterizada por um risco elevado de preparação ou de prática de atos de criminalidade grave (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 111). 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.

151 Para assegurar que a ingerência que as medidas de conservação selecionada descritas nos n.ºs 147 a 150 do presente acórdão comportam respeita o princípio da proporcionalidade, a sua duração 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.

– Quanto às medidas legislativas que preveem a conservação preventiva dos endereços IP e dos dados relativos à identidade civil para efeitos da luta contra a criminalidade e da salvaguarda da segurança pública

152 Importa observar que os endereços IP, apesar de fazerem parte dos dados de tráfego, são gerados sem estarem ligados a uma comunicação específica e servem principalmente para identificar, por intermédio dos prestadores de serviços de comunicações eletrónicas, a pessoa singular proprietária de um equipamento terminal a partir do qual é efetuada uma comunicação através da Internet. Assim, em matéria de correio eletrónico e de telefonia através da Internet, desde que apenas sejam conservados os endereços IP da fonte da comunicação e não os do seu destinatário, esses endereços não revelam, enquanto tais, nenhuma informação sobre terceiros que tenham estado em contacto com a pessoa que está na origem da comunicação. Por conseguinte, esta categoria de dados tem um grau de sensibilidade menor que o dos outros dados de tráfego.

153 No entanto, uma vez que os endereços IP podem ser utilizados para efetuar, nomeadamente, o rastreio exaustivo da navegação de um internauta e, por conseguinte, da sua atividade em linha, esses dados permitem estabelecer o perfil pormenorizado deste último. Assim, a conservação e a análise dos

referidos endereços IP que tal rastreio exige constituem ingerências graves nos direitos fundamentais do internauta consagrados nos artigos 7.º e 8.º da Carta, podendo produzir efeitos dissuasivos como os referidos no n.º 118 do presente acórdão.

154 Ora, para efeitos da necessária ponderação dos direitos e dos interesses em causa exigida pela jurisprudência referida no n.º 130 do presente acórdão, há que ter em conta o facto de, no caso de uma infração cometida em linha, 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. A isto acresce o facto de a conservação dos endereços IP pelos prestadores de serviços de comunicações eletrónicas para lá do período de atribuição destes dados não se afigurar, em princípio, necessária para efeitos da faturação dos serviços em causa, pelo que a deteção das infrações cometidas em linha pode, por esse motivo, como referiram vários Governos nas suas observações apresentadas ao Tribunal de Justiça, revelar-se impossível sem recurso a uma medida legislativa nos termos do artigo 15.º, n.º 1, da Diretiva 2002/58. Isto pode ocorrer, como alegaram esses Governos, com infrações particularmente graves em matéria de pornografia infantil, como a aquisição, a difusão, a transmissão ou a 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).

155 Nestas condições, embora seja verdade que uma medida legislativa que prevê a conservação dos endereços IP de todas as pessoas singulares proprietárias de um equipamento terminal a partir do qual pode ser efetuado um acesso à Internet visa pessoas que, à primeira vista, não têm uma relação, na aceção da jurisprudência referida no n.º 133 do presente acórdão, com os objetivos prosseguidos e que os internautas são titulares, conforme referido no n.º 109 do presente acórdão, do direito de esperar, por força dos artigos 7.º e 8.º da Carta, que a sua identidade não seja, em princípio, revelada, uma medida legislativa que prevê a 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, 11.º e 52.º, n.º 1, da Carta, desde que essa possibilidade esteja sujeita ao estrito respeito das condições materiais e processuais que devem reger a utilização desses dados.

156 Tendo em conta o caráter grave da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que esta conservação comporta, só a luta contra a criminalidade grave e a prevenção das ameaças graves contra a segurança pública são suscetíveis, à semelhança da salvaguarda da segurança nacional, de justificar essa ingerência. Além disso, o período de conservação não pode exceder o estritamente necessário à luz do objetivo prosseguido. Por último, uma medida desta natureza deve prever requisitos e garantias estritas quanto à exploração desses dados, nomeadamente através de um rastreio das comunicações e atividades efetuadas em linha pelas pessoas em causa.

157 No que diz respeito, por último, aos dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicos, estes dados não permitem, por si só, conhecer a data, a hora, a duração e os destinatários das comunicações efetuadas, nem os locais onde estas comunicações decorreram ou a frequência das mesmas com determinadas pessoas durante um determinado período, de modo que não fornecem, com exceção das coordenadas destes, tais como os seus endereços, nenhuma informação sobre as comunicações efetuadas nem, consequentemente, sobre a sua vida privada. Assim, a ingerência que comporta uma conservação destes dados não pode, em princípio, ser qualificada de grave (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.ºs 59 e 60).

158 Daqui decorre que, em conformidade com o que foi referido no n.º 140 do presente acórdão, as medidas legislativas que visam o tratamento desses dados enquanto tais, nomeadamente a sua conservação e o acesso a estes apenas para efeitos da identificação do utilizador em causa, e sem que os referidos dados possam ser associados a informações relativas às comunicações efetuadas, podem

ser justificadas pelo objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral, a que se refere o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 62).

159 Nestas condições, tendo em conta a necessária ponderação dos direitos e interesses em causa e pelas razões que figuram nos n.ºs 131 e 158 do presente acórdão, há que considerar que, mesmo na falta de ligação entre todos os utilizadores dos meios de comunicações eletrónicos e os objetivos prosseguidos, 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, não se opõe a uma medida legislativa que impõe, sem prazo específico, aos prestadores de serviços de comunicações eletrónicas a conservação de dados relativos à identidade civil de todos os utilizadores de meios de comunicações eletrónicos para efeitos de prevenção, investigação, deteção e repressão de infrações penais, assim como da salvaguarda da segurança pública, não sendo necessário que as infrações penais ou que as ameaças ou as ofensas à segurança pública sejam graves.

– Quanto às medidas legislativas que preveem a conservação rápida de dados de tráfego e de dados de localização para efeitos da luta contra a criminalidade grave

160 No que diz respeito aos dados de tráfego e aos 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, da mesma, tais como descritas nos n.ºs 134 a 159 do presente acórdão, importa assinalar 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.

161 No entanto, durante esse tratamento e essa armazenagem, podem ocorrer situações em que é necessário conservar os referidos dados para lá 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 relevantes, se pode razoavelmente suspeitar da sua existência.

162 A este respeito, importa observar que a Convenção sobre a Cibercriminalidade do Conselho da Europa, de 23 de novembro de 2001 (Série de Tratados Europeus — n.º 185), assinada pelos 27 Estados-Membros e ratificada por 25 deles, e cujo objetivo é facilitar a luta contra as infrações penais cometidas através de redes informáticas, prevê, no seu artigo 14.º, que as partes contratantes devem adotar para efeitos de investigações ou de processos penais específicos determinadas medidas quanto aos dados de tráfego já armazenados, tais como a conservação rápida desses dados. Em particular, o artigo 16.º, n.º 1, desta convenção estabelece que as partes contratantes devem adotar as medidas legislativas necessárias para permitir às suas autoridades competentes ordenar ou impor de outra forma a conservação rápida dos dados de tráfego armazenados através de um sistema informático, nomeadamente quando existam razões para pressupor que esses dados são suscetíveis de perda ou de alteração.

163 Numa situação como a referida no n.º 161 do presente acórdão, os Estados-Membros podem, tendo em conta a necessária ponderação dos direitos e interesses em causa referida no n.º 130 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.

164 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. Além disso, a fim de assegurar que a ingerência que uma medida deste tipo comporta se limita ao estritamente necessário, importa, por um lado, que a obrigação de conservação incida apenas sobre os dados de tráfego e dados de localização suscetíveis de contribuir para o esclarecimento da infração penal grave ou da violação da segurança nacional em causa. Por outro, o período de conservação de dados deve ser limitado ao estritamente necessário, podendo, no entanto, ser prolongado quando as circunstâncias e o objetivo prosseguido pela referida medida o justifiquem.

165 A este propósito, importa precisar que tal conservação rápida não deve ser limitada aos dados das pessoas efetivamente suspeitas de terem cometido uma infração penal ou uma ofensa à segurança nacional. 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 133 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, do seu meio social ou profissional ou, ainda, de zonas geográficas determinadas, tais como os locais da prática e da preparação da infração ou da ofensa à segurança nacional em causa. Além disso, o acesso das autoridades competentes aos dados assim conservados deve ser efetuado segundo as condições resultantes da jurisprudência relativa à interpretação da Diretiva 2002/58 (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.ºs 118 a 121 e jurisprudência aí referida).

166 Importa ainda acrescentar que, conforme resulta, nomeadamente, dos n.ºs 115 e 133 do presente acórdão, o acesso aos dados de tráfego e aos 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 apenas pode, em princípio, ser justificado pelo objetivo de interesse geral pelo qual esta conservação foi imposta a tais prestadores. Daqui decorre, em particular, que um acesso a tais dados para efeitos de repressão e de sanção de uma infração penal ordinária não pode, em caso algum, ser concedido quando a sua conservação foi justificada pelo objetivo de luta contra a criminalidade grave ou, *a fortiori*, de salvaguarda da segurança nacional. Em contrapartida, em conformidade com o princípio da proporcionalidade tal como precisado no n.º 131 do presente acórdão, um acesso aos dados conservados tendo em vista a luta contra a criminalidade grave pode, desde que sejam respeitadas as condições materiais e processuais aplicáveis a tal acesso referidas no número anterior, ser justificado pelo objetivo de salvaguarda da segurança nacional.

167 A este respeito, os Estados-Membros têm a possibilidade de prever na sua legislação que um acesso a dados de tráfego e a dados de localização pode, no respeito dessas mesmas condições materiais e processuais, ocorrer para efeitos de luta contra a criminalidade grave ou de salvaguarda da segurança nacional quando os referidos dados são conservados por um fornecedor em conformidade com os artigos 5.º, 6.º e 9.º ou ainda com o artigo 15.º, n.º 1, da Diretiva 2002/58.

168 Tendo em consideração o exposto, deve responder-se às primeiras questões nos processos C-511/18 e C-512/18, assim como à primeira e segunda questões no processo C-520/18 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, para as finalidades previstas nesse

artigo 15.º, n.º 1, a título preventivo, uma conservação generalizada e indiferenciada de dados de tráfego e de 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:

– permitam, para efeitos da 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;

– prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação selecionada 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;

– prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

– prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública, uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, e

– permitam, para efeitos da luta contra a criminalidade grave e, *a fortiori*, da salvaguarda da segurança nacional, impor aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, o dever de procederem, por um determinado período, à conservação rápida de 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 dispõem de garantias efetivas contra os riscos de abuso.

Quanto à segunda e terceira questões no processo C-511/18

169 Com a segunda e terceira questões no processo C-511/18, 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 regulamentação nacional que impõe aos prestadores de serviços de comunicações eletrónicas o dever de aplicarem nas suas redes medidas que permitam, por um lado, a análise automatizada e a recolha em tempo real de dados de tráfego e de dados de localização e, por outro, a recolha em tempo real de dados técnicos relativos à localização dos equipamentos terminais utilizados, sem que esteja prevista a informação das pessoas afetadas por esses tratamentos e por essas recolhas.

170 O órgão jurisdicional de reenvio precisa que as técnicas de recolha de informação previstas nos artigos L. 851-2 a L. 851-4 do CSI não implicam, para os prestadores de serviços de comunicações eletrónicas, uma exigência específica de conservação de dados de tráfego e de dados de localização. No que diz respeito, em particular, à análise automatizada referida no artigo L. 851-3 do CSI, esse órgão jurisdicional afirma que tal tratamento tem por objeto detetar, em função de critérios definidos para o efeito, ligações suscetíveis de constituir uma ameaça terrorista. Quanto à recolha em tempo real prevista no artigo L. 851-2 do CSI, o referido órgão jurisdicional observa que apenas visa uma ou mais pessoas previamente identificadas como potencialmente ligadas a uma ameaça terrorista. Segundo o mesmo órgão jurisdicional, estas duas técnicas só podem ser aplicadas para efeitos de prevenção do terrorismo e são relativas aos dados referidos nos artigos L. 851-1 e R. 851-5 do CSI.

171 A título preliminar, importa precisar que, segundo o artigo L. 851-3 do CSI, o facto de a análise automatizada que prevê não permitir, enquanto tal, a identificação dos utilizadores cujos dados estão sujeitos a essa análise não impede que tais dados sejam qualificados de «dados pessoais». Com efeito, uma vez que o procedimento previsto no ponto IV dessa mesma disposição permite, numa fase posterior, a identificação da pessoa ou das pessoas afetadas pelos dados cuja análise automatizada revelou serem suscetíveis de constituir uma ameaça terrorista, todas as pessoas cujos dados são objeto da análise automatizada continuam a ser identificáveis a partir destes dados. Ora, segundo a definição de dados pessoais constante do artigo 4.º, ponto 1, do Regulamento 2016/679, entende-se por tais dados as informações relativas, nomeadamente, a uma pessoa identificável.

Quanto à análise automatizada de dados de tráfego e de dados de localização

172 Resulta do artigo L. 851-3 do CSI que a análise automatizada que prevê corresponde, em substância, a uma filtragem da totalidade dos dados de tráfego e dos dados de localização conservados pelos prestadores de serviços de comunicações eletrónicas, efetuada por estes a pedido das autoridades nacionais competentes e em aplicação dos parâmetros que estas fixaram. Daqui decorre que todos os dados dos utilizadores dos meios de comunicações eletrónicos são verificados se corresponderem a esses parâmetros. Assim, deve considerar-se que tal análise automatizada implica que os prestadores de serviços de comunicações eletrónicas em causa efetuem, por conta da autoridade competente, um tratamento generalizado e indiferenciado, sob a forma de uma utilização por meio de um processo automatizado, na aceção do artigo 4.º, ponto 2, do Regulamento 2016/679, que abranja o conjunto dos dados de tráfego e dos dados de localização de todos os utilizadores de meios de comunicações eletrónicos. Este tratamento é independente da posterior recolha dos dados relativos às pessoas identificadas na sequência da análise automatizada, recolha que é autorizada com base no artigo L. 851-3, IV, do CSI.

173 Ora, uma regulamentação nacional que autoriza tal análise automatizada de dados de tráfego e de dados de localização derroga a obrigação de princípio, imposta pelo artigo 5.º da Diretiva 2002/58, de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados. Tal regulamentação constitui igualmente uma ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, independentemente da posterior utilização que seja feita destes dados. Por último, tal regulamentação pode, em conformidade com a jurisprudência referida no n.º 118 do presente acórdão, produzir efeitos dissuasivos no exercício da liberdade de expressão consagrada no artigo 11.º da Carta.

174 Além disso, a ingerência resultante de uma análise automatizada de dados de tráfego e de dados de localização, como a que está em causa no processo principal, revela-se particularmente grave, uma vez que abrange de forma generalizada e indiferenciada os dados das pessoas que utilizam meios de comunicações eletrónicos. Esta constatação impõe-se ainda mais quando, como resulta da regulamentação nacional em causa no processo principal, os dados objeto da análise automatizada são suscetíveis de revelar a natureza das informações consultadas em linha. Além disso, tal análise automatizada é aplicável de forma global a todas as pessoas que utilizam meios de comunicações

eletrónicos e, por conseguinte, também àquelas em relação às quais não existam indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com atividades de terrorismo.

175 Quanto à justificação de tal ingerência, há que precisar que a exigência, imposta pelo artigo 52.º, n.º 1, da Carta, de que qualquer restrição ao exercício de direitos fundamentais deve ser prevista por lei implica que a própria base jurídica que permite a ingerência nesses direitos deve definir o alcance da limitação do exercício do direito em causa (v., neste sentido, Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, n.º 175 e jurisprudência aí referida).

176 Além disso, para satisfazer a exigência de proporcionalidade recordada nos n.ºs 130 e 131 do presente acórdão, segundo a qual as derrogações à proteção de dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário, uma regulamentação nacional que regula o acesso das autoridades competentes aos dados de tráfego e aos dados de localização conservados deve respeitar os requisitos decorrentes da jurisprudência referida no n.º 132 do presente acórdão. Em particular, tal regulamentação não se pode limitar a exigir que o acesso das autoridades aos dados responda à finalidade prosseguida por esta regulamentação, devendo igualmente prever as condições materiais e processuais que regulam essa utilização [v., por analogia, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 192 e jurisprudência aí referida].

177 A este respeito, importa recordar que a ingerência particularmente grave que uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização comporta, referida nas considerações que figuram nos n.ºs 134 a 139 do presente acórdão, bem como a ingerência particularmente grave que constitui a sua análise automatizada apenas podem satisfazer a exigência de proporcionalidade em situações em que um Estado-Membro se encontra perante uma ameaça grave para a segurança nacional que se revele real e atual ou previsível, e desde que a duração dessa conservação seja limitada ao estritamente necessário.

178 Em situações como as que são referidas no número anterior, a aplicação de uma análise automatizada de dados de tráfego e de dados de localização de todos os utilizadores de meios de comunicações eletrónicos, durante um período estritamente limitado, pode ser considerada justificada à luz dos requisitos decorrentes 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.

179 Assim sendo, para garantir que o recurso a tal medida se limita efetivamente ao estritamente necessário à proteção da segurança nacional, e mais particularmente à prevenção do terrorismo, é essencial, em conformidade com o que se observa no n.º 139 do presente acórdão, que a decisão que autoriza a análise automatizada possa ser objeto de fiscalização efetiva quer por um órgão jurisdicional quer por uma entidade administrativa independente cuja decisão produza efeitos vinculativos, destinada a verificar a existência de uma situação que justifica a referida medida e o respeito das garantias que devem estar previstas.

180 A este respeito, importa precisar que os modelos e os critérios preestabelecidos em que assenta este tipo de tratamento de dados devem ser, por um lado, específicos e fiáveis, permitindo alcançar resultados que identifiquem as pessoas sobre as quais possa recair uma suspeita razoável de participação em infrações terroristas ou de criminalidade transnacional grave e, por outro, não discriminatórios [v., neste sentido, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 172].

181 Além disso, importa recordar que qualquer análise automatizada efetuada em função de modelos e critérios baseados no pressuposto de que a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, a saúde e a vida sexual de uma pessoa poderiam, em si mesmas e independentemente do comportamento individual desta pessoa, ser relevantes à luz da prevenção do terrorismo violaria os direitos garantidos pelos artigos 7.º e 8.º da Carta, conjugados

com o seu artigo 21.º Assim, os modelos e os critérios preestabelecidos para efeitos de uma análise automatizada destinada a prevenir atividades terroristas que constituem uma ameaça grave para a segurança nacional não se podem basear apenas nesses dados sensíveis [v., neste sentido, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 165].

182 Por outro lado, uma vez que as análises automatizadas de dados de tráfego e de dados de localização comportam necessariamente uma certa taxa de erro, qualquer resultado positivo obtido na sequência de um tratamento automatizado dos referidos dados deve estar sujeito a um reexame individual, através de meios não automatizados, antes da adoção de uma medida individual que afete de forma negativa as pessoas em causa, tal como a posterior recolha de dados de tráfego e de dados de localização em tempo real, visto que tal medida não se pode basear única e decisivamente no resultado de um tratamento automatizado. De igual modo, para garantir que, na prática, os modelos e os critérios preestabelecidos, a respetiva utilização e as bases de dados utilizadas não são discriminatórios e se limitam ao estritamente necessário à luz do objetivo de prevenir as atividades terroristas que constituem uma ameaça grave para a segurança nacional, a fiabilidade e a atualidade desses modelos e desses critérios preestabelecidos assim como das bases de dados utilizadas devem ser objeto de reexame periódico [v., neste sentido, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.ºs 173 e 174].

Quanto à recolha em tempo real de dados de tráfego e de dados de localização

183 Quanto à recolha em tempo real de dados de tráfego e de dados de localização prevista no artigo L. 851-2 do CSI, importa assinalar que pode ser individualmente autorizada no que diz respeito a «uma pessoa previamente identificada como potencialmente ligada a uma ameaça [terrorista]». De igual modo, segundo esta disposição, «[q]uando existirem razões sérias para crer que uma ou várias pessoas que pertencem ao círculo da pessoa abrangida pela autorização podem fornecer informações com base na finalidade que justifica a autorização, esta pode ser igualmente concedida individualmente a cada uma dessas pessoas».

184 Os dados objeto de uma medida desta natureza permitem às autoridades nacionais competentes vigiar, durante o período da autorização, de forma contínua e em tempo real, os interlocutores com os quais as pessoas em causa comunicam, os meios que utilizam, a duração das comunicações que passam, bem como os lugares onde estiveram e as suas deslocações. De igual modo, afiguram-se suscetíveis de revelar a natureza das informações consultadas em linha. Considerados no seu conjunto, estes dados permitem, como resulta do n.º 117 do presente acórdão, extrair conclusões muito precisas sobre a vida privada das pessoas em causa e fornecem os meios para determinar o perfil destas, sendo tal informação tão sensível, à luz do direito ao respeito da vida privada, como o próprio conteúdo das comunicações.

185 Quanto à recolha de dados em tempo real prevista no artigo L. 851-4 do CSI, esta disposição autoriza a recolha de dados técnicos relativos à localização de equipamentos terminais e à transmissão em tempo real para um serviço dependente do primeiro-ministro. Verifica-se que esses dados permitem ao serviço competente, em qualquer momento durante o período da autorização, localizar, de forma contínua e em tempo real, equipamentos terminais utilizados, como telefones móveis.

186 Ora, uma regulamentação nacional que autoriza tais recolhas em tempo real derroga, à semelhança da que autoriza a análise automatizada dos dados, a obrigação de princípio, imposta pelo artigo 5.º da Diretiva 2002/58, de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados. Assim, constitui igualmente uma ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta e é suscetível de produzir efeitos dissuasivos no exercício da liberdade de expressão garantida no artigo 11.º da Carta.

187 Importa sublinhar que a ingerência que comporta a recolha em tempo real de dados que permitam localizar um equipamento terminal afigura-se particularmente grave, uma vez que estes dados fornecem às autoridades nacionais competentes um meio de acompanhamento preciso e permanente das deslocações dos utilizadores dos telefones móveis. Na medida em que, assim, esses dados devem ser considerados particularmente sensíveis, o acesso das autoridades competentes a tais dados em tempo real deve distinguir-se de um acesso em tempo diferido aos mesmos, sendo o primeiro mais intrusivo, uma vez que permite uma vigilância quase perfeita desses utilizadores (v., por analogia, no que diz respeito ao artigo 8.º da CEDH, TEDH, 8 de fevereiro de 2018, Ben Faiza c. França, CE:ECHR:2018:0208JUD003144612, § 74). Além disso, a intensidade dessa ingerência é agravada quando a recolha em tempo real abrange igualmente os dados de tráfego das pessoas em causa.

188 Embora o objetivo de prevenção do terrorismo prosseguido pela regulamentação nacional em causa no processo principal seja suscetível, atendendo à sua importância, de justificar a ingerência que comporta a recolha em tempo real de dados de tráfego e de dados de localização, tal medida, tendo em conta o seu caráter particularmente intrusivo, apenas pode ser aplicada às pessoas em relação às quais existe uma razão válida para suspeitar que estão de alguma forma envolvidas em atividades terroristas. Quanto aos dados das pessoas não pertencentes a essa categoria, apenas podem ser objeto de acesso em tempo diferido, uma vez que este só pode ocorrer, em conformidade com a jurisprudência do Tribunal de Justiça, em situações específicas, como aquelas em que estão em causa atividades terroristas, e quando existam elementos objetivos que permitam considerar que esses dados podem, num caso concreto, trazer uma contribuição efetiva para a luta contra o terrorismo (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 119 e jurisprudência aí referida).

189 Além disso, uma decisão que autoriza a recolha de dados de tráfego e de dados de localização em tempo real deve basear-se nos critérios objetivos previstos na legislação nacional. Em particular, esta legislação deve definir, de acordo com a jurisprudência referida no n.º 176 do presente acórdão, as circunstâncias e as condições em que tal recolha pode ser autorizada e prever que, conforme foi precisado no número anterior, apenas podem ser afetadas as pessoas com uma ligação ao objetivo de prevenção do terrorismo. Além disso, uma decisão que autoriza a recolha em tempo real de dados de tráfego e de dados de localização deve basear-se nos critérios objetivos e não discriminatórios previstos na legislação nacional. Para garantir, na prática, o cumprimento destas condições, é essencial que a aplicação da medida que autoriza a recolha em tempo real seja sujeita a uma fiscalização prévia por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos, devendo esse órgão jurisdicional ou essa entidade assegurar, nomeadamente, que tal recolha em tempo real apenas é autorizada no limite do estritamente necessário (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 120). Em caso de urgência devidamente justificada, a fiscalização deve ser efetuada rapidamente.

Quanto à informação das pessoas cujos dados foram recolhidos ou analisados

190 Importa que as autoridades nacionais competentes que procedem à recolha em tempo real de dados de tráfego e de dados de localização informem desse facto as pessoas em causa, no âmbito dos processos nacionais aplicáveis, desde que e a partir do momento em que essa comunicação não seja suscetível de comprometer as missões que incumbem a estas autoridades. Com efeito, essa informação é, de facto, necessária para permitir que estas pessoas exerçam os seus direitos, decorrentes dos artigos 7.º e 8.º da Carta, de pedir o acesso aos seus dados pessoais que são objeto dessas medidas e, sendo caso disso, a retificação ou a eliminação destes e de intentar, nos termos do artigo 47.º, primeiro parágrafo, da Carta, uma ação perante um tribunal, direito este que, de resto, se encontra expressamente garantido no artigo 15.º, n.º 2, da Diretiva 2002/58, lido em conjugação com o artigo 79.º, n.º 1, do Regulamento 2016/679 [v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.º 121 e jurisprudência referida, e Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.ºs 219 e 220].

191 No que diz respeito à informação exigida no âmbito de uma análise automatizada de dados de tráfego e de dados de localização, a autoridade nacional competente está obrigada a publicar informações de natureza geral relativas a esta análise, não tendo de proceder a uma informação individual das pessoas em causa. Em contrapartida, no caso de os dados responderem aos parâmetros estabelecidos na medida que autoriza a análise automatizada e de esta autoridade proceder à identificação da pessoa em causa para analisar mais aprofundadamente os dados que lhe dizem respeito, a informação individual dessa pessoa é necessária. No entanto, tal informação só deve ocorrer desde que e a partir do momento em que não seja suscetível de comprometer as missões que incumbem à referida autoridade [v., por analogia, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.os 222 a 224].

192 Tendo em consideração o exposto, deve responder-se à segunda e terceira questões no processo C-511/18 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 não se opõe a uma regulamentação nacional que impõe aos prestadores de serviços de comunicações eletrónicas que recorram, por um lado, à análise automatizada e à recolha em tempo real de dados de tráfego e de dados de localização e, por outro, à recolha em tempo real de dados técnicos relativos à localização dos equipamentos terminais utilizados, quando

– o recurso à análise automatizada esteja limitado a situações em que um Estado-Membro se encontra confrontado com uma ameaça grave para a segurança nacional que se revele real e atual ou previsível, podendo o recurso a essa análise ser objeto de fiscalização efetiva, quer por um órgão jurisdicional quer por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos, destinada a verificar a existência de uma situação que justifique a referida medida, bem como o respeito das condições e das garantias que devem estar previstas, e quando

– o recurso a uma recolha em tempo real de dados de tráfego e de dados de localização esteja limitado às pessoas em relação às quais existe uma razão válida para suspeitar que estão de alguma forma envolvidas em atividades terroristas e esteja sujeito a fiscalização prévia, quer por um órgão jurisdicional quer por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos, a fim de assegurar que tal recolha em tempo real apenas é autorizada no limite do estritamente necessário. Em caso de urgência devidamente justificada, a fiscalização deve ser efetuada rapidamente.

Quanto à segunda questão no processo C-512/18

193 Com a segunda questão no processo C-512/18, o órgão jurisdicional de reenvio pretende saber, em substância, se as disposições da Diretiva 2000/31, lidas à luz dos artigos 6.º a 8.º, 11.º e 52.º, n.º 1, da Carta, devem ser interpretadas no sentido de que se opõem a uma regulamentação nacional que impõe aos fornecedores de acesso a serviços de comunicação ao público em linha e aos prestadores de serviços de armazenamento a conservação generalizada e indiferenciada dos dados pessoais relativos a estes serviços.

194 Embora considere que tais serviços estão abrangidos pelo âmbito de aplicação da Diretiva 2000/31, e não pelo da Diretiva 2002/58, o órgão jurisdicional de reenvio entende que o artigo 15.º, n.os 1 e 2, da Diretiva 2000/31, lido em conjugação com os seus artigos 12.º e 14.º, não estabelece, por si só, uma proibição de princípio de conservação de dados relativos à criação de conteúdo que só pode ser derrogada a título excecional. Não obstante, esse órgão jurisdicional pergunta se tal apreciação deve ser aceite, tendo em conta o necessário respeito dos direitos fundamentais consagrados nos artigos 6.º a 8.º e 11.º da Carta.

195 Além disso, o órgão jurisdicional de reenvio precisa que a sua questão visa a obrigação de conservação prevista no artigo 6.º da LCEN, lido em conjugação com o Decreto n.º 2011-219. Os dados que os prestadores de serviços em causa devem conservar a este título incluem, nomeadamente, os dados relativos à identidade civil das pessoas que utilizaram esses serviços, tais como o apelido, o nome próprio, os seus endereços postais associados, os seus endereços de correio eletrónico ou de conta associados, as suas palavras-passe, quando a subscrição do contrato ou da conta for paga, o modo de pagamento utilizado, a referência do pagamento, o montante, bem como a data e hora da transação.

196 De igual modo, os dados visados pela obrigação de conservação abrangem os identificadores dos assinantes, as ligações e os equipamentos terminais utilizados, os identificadores atribuídos aos conteúdos, as datas e horas de início e de fim das ligações e das operações, bem como os tipos de protocolos utilizados para a ligação ao serviço e para a transferência de conteúdos. O acesso a esses dados, cujo período de conservação é de um ano, pode ser solicitado no âmbito de processos penais e civis, para efeitos do cumprimento das regras relativas à responsabilidade civil ou penal, bem como no âmbito de medidas de recolha de informações às quais se aplica o artigo L. 851-1 do CSI.

197 A este respeito, importa salientar que, em conformidade com o seu artigo 1.º, n.º 2, a Diretiva 2000/31 aproxima certas disposições nacionais aplicáveis aos serviços da sociedade da informação referidos no seu artigo 2.º, alínea a).

198 É verdade que esses serviços abrangem os que são prestados à distância através de equipamentos eletrónicos de tratamento e de armazenamento de dados, a pedido individual de um destinatário de serviços e, normalmente, mediante remuneração, como os serviços de acesso à Internet ou a uma rede de comunicações, bem como os serviços de armazenamento (v., neste sentido, Acórdãos de 24 de novembro de 2011, Scarlet Extended, C-70/10, EU:C:2011:771, n.º 40; de 16 de fevereiro de 2012, SABAM, C-360/10, EU:C:2012:85, n.º 34; de 15 de setembro de 2016, Mc Fadden, C-484/14, EU:C:2016:689; n.º 55; e de 7 de agosto de 2018, SNB-REACT, C-521/17, EU:C:2018:639, n.º 42 e jurisprudência aí referida).

199 No entanto, o artigo 1.º, n.º 5, da Diretiva 2000/31 dispõe que esta não é aplicável às questões respeitantes aos serviços da sociedade da informação abrangidas pelas Diretivas 95/46 e 97/66. A este propósito, resulta dos considerandos 14 e 15 da Diretiva 2000/31 que a proteção da confidencialidade das comunicações e dos indivíduos no que se refere ao tratamento dos dados pessoais no âmbito dos serviços da sociedade de informação é regida exclusivamente pelas Diretivas 95/46 e 97/66, sendo que esta última proíbe, no seu artigo 5.º, para efeitos da proteção da confidencialidade das comunicações, qualquer forma de interceção ou de vigilância das comunicações.

200 Assim, as questões ligadas à proteção da confidencialidade das comunicações e dos dados pessoais devem ser apreciadas à luz da Diretiva 2002/58 e do Regulamento 2016/679, tendo estes substituído respetivamente a Diretiva 97/66 e a Diretiva 95/46, devendo salientar-se que a proteção que a Diretiva 2000/31 visa assegurar não pode, em todo o caso, prejudicar as exigências resultantes da Diretiva 2002/58 e do Regulamento 2016/679 (v., neste sentido, Acórdão de 29 de janeiro de 2008, Promusicae, C-275/06, EU:C:2008:54, n.º 57).

201 A obrigação imposta pela regulamentação nacional referida no n.º 195 do presente acórdão aos fornecedores de acesso a serviços de comunicação ao público em linha e aos prestadores de serviços de armazenamento de conservarem os dados pessoais relativos a estes serviços deve, assim, como salientou, em substância, o advogado-geral no n.º 141 das Conclusões que apresentou nos processos apensos La Quadrature du Net e o. (C-511/18 e C-512/18, EU:C:2020:6), ser apreciada à luz da Diretiva 2002/58 ou do Regulamento 2016/679.

202 Assim, consoante a prestação dos serviços abrangidos por esta regulamentação nacional esteja ou não abrangida pela Diretiva 2002/58, será regulada por esta última diretiva, nomeadamente pelo seu 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, ou pelo Regulamento 2016/679, nomeadamente, pelo artigo 23.º, n.º 1, do referido regulamento, lido à luz das mesmas disposições da Carta.

203 No caso, não se pode excluir, como salientou a Comissão Europeia nas suas observações escritas, que alguns dos serviços aos quais se aplica a regulamentação nacional referida no n.º 195 do presente acórdão constituam serviços de comunicações eletrónicas, na aceção da Diretiva 2002/58, o que cabe ao órgão jurisdicional de reenvio verificar.

204 A este respeito, importa sublinhar que a Diretiva 2002/58 abrange os serviços de comunicações eletrónicas que cumprem os requisitos estabelecidos no artigo 2.º, alínea c), da Diretiva 2002/21, para o qual remete o artigo 2.º da Diretiva 2002/58 e que define o serviço de comunicações eletrónicas como «o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações eletrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão». No que diz respeito aos serviços da sociedade de informação, como os referidos nos n.os 197 e 198 do presente acórdão e abrangidos pela Diretiva 2000/31, estes constituem serviços de comunicações eletrónicas quando consistam total ou principalmente no envio de sinais através de redes de comunicações eletrónicas (v., neste sentido, Acórdão de 5 de junho de 2019, Skype Comunicações, C-142/18, EU:C:2019:460, n.os 47 e 48).

205 Assim, os serviços de acesso à Internet, que se afigurem abrangidos pela regulamentação nacional referida no n.º 195 do presente acórdão, constituem, como confirmado pelo considerando 10 da Diretiva 2002/21, serviços de comunicações eletrónicas, na aceção desta diretiva (v., neste sentido, Acórdão de 5 de junho de 2019, Skype Comunicações, C-142/18, EU:C:2019:460, n.º 37). É isto que sucede igualmente quanto aos serviços de correio eletrónico na Internet, relativamente aos quais não parece excluído que também estejam abrangidos por essa regulamentação nacional, uma vez que, no plano técnico, implicam total ou principalmente o envio de sinais através de redes de comunicações eletrónicas (v., neste sentido, Acórdão de 13 de junho de 2019, Google, C-193/18, EU:C:2019:498, n.os 35 e 38).

206 Quanto às exigências decorrentes 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, há que remeter para todas as constatações e apreciações efetuadas no âmbito da resposta dada às primeiras questões nos processos C-511/18 e C-512/18, assim como para a primeira e segunda questões no processo C-520/18.

207 Quanto às exigências decorrentes do Regulamento 2016/679, importa recordar que este visa, nomeadamente, como resulta do seu considerando 10, assegurar um nível de proteção coerente e elevado das pessoas singulares na União e, para o efeito, assegurar em toda a União uma aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais dessas pessoas no que diz respeito ao tratamento de dados pessoais (v., neste sentido, Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, n.º 101).

208 Para o efeito, qualquer tratamento de dados pessoais deve, sem prejuízo das derrogações admitidas no artigo 23.º do Regulamento 2016/679, respeitar os princípios que regulam os tratamentos de dados pessoais, assim como os direitos da pessoa em causa enunciados, respetivamente, nos capítulos II e III deste regulamento. Em particular, qualquer tratamento de dados pessoais deve, por um lado, respeitar os princípios consagrados no artigo 5.º do referido regulamento e, por outro, cumprir as condições de licitude enumeradas no artigo 6.º desse mesmo regulamento (v., por analogia, no que diz respeito à Diretiva 95/46, Acórdão de 30 de maio de 2013, Worten, C-342/12, EU:C:2013:355, n.º 33 e jurisprudência aí referida).

209 No que diz respeito, mais particularmente, ao artigo 23.º, n.º 1, do Regulamento 2016/679, importa observar que este, à semelhança do que está previsto no artigo 15.º, n.º 1, da Diretiva 2002/58, permite aos Estados-Membros limitarem, tendo em conta as finalidades que prevê e através de medidas legislativas, o alcance das obrigações e dos direitos aí referidos, «desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar» a finalidade prosseguida. Qualquer medida legislativa adotada com esse fundamento deve, em especial, respeitar as exigências específicas estabelecidas no artigo 23.º, n.º 2, deste regulamento.

210 Assim, o artigo 23.º, n.ºs 1 e 2, do Regulamento 2016/679 não pode ser interpretado no sentido de que pode conferir aos Estados-Membros o poder de atentarem contra o respeito da vida privada, em violação do artigo 7.º da Carta, ou das outras garantias nela previstas (v., por analogia, no que diz respeito à Diretiva 95/46, Acórdão de 20 de maio de 2003, Österreichischer Rundfunk e o., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, n.º 91). Em particular, à semelhança do que é válido para o artigo 15.º, n.º 1, da Diretiva 2002/58, o poder que o artigo 23.º, n.º 1, do Regulamento n.º 2016/679 confere aos Estados-Membros apenas pode ser exercido se for respeitado o requisito da proporcionalidade, segundo o qual as derrogações à proteção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário (v., por analogia, no que diz respeito à Diretiva 95/46, Acórdão de 7 de novembro de 2013, IPI, C-473/12, EU:C:2013:715, n.º 39 e jurisprudência aí referida).

211 Daqui decorre que as constatações e as apreciações efetuadas no âmbito da resposta dada às primeiras questões nos processos C-511/18 e C-512/18, assim como à primeira e segunda questões no processo C-520/18 são aplicáveis *mutatis luxemmutandis* ao artigo 23.º do Regulamento 2016/679.

212 Tendo em consideração o exposto, há que responder à segunda questão no processo C-512/18 que a Diretiva 2000/31 deve ser interpretada no sentido de que não é aplicável em matéria de proteção da confidencialidade das comunicações e das pessoas singulares no que diz respeito ao tratamento de dados pessoais no âmbito dos serviços da sociedade de informação, sendo esta proteção regulada, consoante o caso, pela Diretiva 2002/58 ou pelo Regulamento 2016/679. O artigo 23.º, n.º 1, do Regulamento 2016/679, 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 regulamentação nacional que impõe aos fornecedores de acesso a serviços de comunicação ao público em linha e aos prestadores de serviços de armazenamento a conservação generalizada e indiferenciada, nomeadamente, dos dados pessoais relativos a esses serviços.

Quanto à terceira questão no processo C-520/18

213 Com a terceira questão no processo C-520/18, o órgão jurisdicional de reenvio pretende saber, em substância, se um órgão jurisdicional nacional pode aplicar uma disposição do seu direito nacional que o habilita a limitar no tempo os efeitos de uma declaração de ilegalidade para a qual é competente, por força desse direito, em relação a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas, tendo em vista, designadamente, a prossecução dos objetivos de salvaguarda da segurança nacional e de luta contra a criminalidade, uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, devido ao facto de tal legislação ser incompatível com 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.

214 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 normas da União, não podendo o direito dos Estados-Membros afetar o efeito reconhecido a essas diferentes normas no território dos referidos Estados [Acórdãos de

15 de julho de 1964, Costa, 6/64, EU:C:1964:66, pp. 1159 e 1160, e 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 e 158 e jurisprudência aí referida].

215 Por força do princípio do primado, na impossibilidade de proceder a uma interpretação da regulamentação 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 [Acórdãos de 22 de junho de 2010, Melki e Abdeli, C-188/10 e C-189/10, EU:C:2010:363, n.º 43 e jurisprudência aí referida; de 24 de junho de 2019, Popławski, C-573/17, EU:C:2019:530, n.º 58, e 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.º 160].

216 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 de 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 [v., neste sentido, Acórdãos de 23 de outubro de 2012, Nelson e o., C-581/10 e C-629/10, EU:C:2012:657, n.os 89 e 91; de 23 de abril de 2020, Herst, C-401/18, EU:C:2020:295, n.os 56 e 57; e de 25 de junho de 2020, A e o. (Turbinas eólicas em Aalter e em Nevele), C-24/19, EU:C:2020:503, n.º 84 e jurisprudência aí referida].

217 Se os órgãos jurisdicionais nacionais pudessem, ainda que a título provisório, dar primado sobre o direito da União a disposições nacionais a ele contrárias, ficariam comprometidos o primado e a aplicação uniforme do direito da União (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.º 177 e jurisprudência aí referida).

218 No entanto, o Tribunal de Justiça declarou, 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 do impacto de um projeto no ambiente e num local protegido, que um órgão jurisdicional nacional pode, se o direito interno o permitir, excecionalmente manter os efeitos de medidas quando esta manutenção seja 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).

219 Ora, contrariamente à omissão de uma obrigação processual como a avaliação prévia do impacto de um projeto 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. Com efeito, a manutenção dos efeitos de uma legislação nacional, como a que está em causa no processo principal, significa 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.

220 Por conseguinte, o órgão jurisdicional de reenvio não pode aplicar uma disposição do seu direito nacional que o habilite a limitar no tempo os efeitos de uma declaração de ilegalidade, para a qual é competente por força desse direito, da legislação nacional em causa no processo principal.

221 Dito isto, nas observações que apresentaram no Tribunal de Justiça, VZ, WY e XX alegam que a terceira questão suscita, implícita, mas necessariamente, a questão de saber se o direito da União se opõe a uma exploração, no âmbito de um processo penal, das informações e dos elementos de prova obtidos através de uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização incompatível com esse direito.

222 A este respeito e para dar uma resposta útil ao órgão jurisdicional de reenvio, importa recordar que, na fase atual do direito da União, em princípio, cabe exclusivamente ao direito nacional determinar as regras relativas à admissibilidade e à apreciação, no âmbito de um processo penal instaurado contra pessoas suspeitas de atos de criminalidade grave, de informações e de elementos de prova obtidos através de tal conservação de dados contrária ao direito da União.

223 Com efeito, é jurisprudência constante que, na falta de regras da União na matéria, cabe à ordem jurídica interna de cada Estado-Membro, por força do princípio da autonomia processual, regular as modalidades processuais dos recursos judiciais para salvaguarda dos direitos dos particulares decorrentes do direito da União, desde que, no entanto, não sejam menos favoráveis do que as que regulam situações semelhantes submetidas ao direito interno (princípio da equivalência) e não tornem impossível na prática ou excessivamente difícil o exercício dos direitos conferidos pelo direito da União (princípio da efetividade) (v., neste sentido, Acórdãos de 6 de outubro de 2015, Târşia, C-69/14, EU:C:2015:662, n.os 26 e 27; de 24 de outubro de 2018, XC e o., C-234/17, EU:C:2018:853, n.os 21 e 22 e jurisprudência aí referida; e de 19 de dezembro de 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, n.º 33).

224 No que diz respeito ao princípio da equivalência, cabe ao órgão jurisdicional nacional chamado a pronunciar-se num processo penal baseado em informações ou em elementos de prova obtidos em violação dos requisitos decorrentes da Diretiva 2002/58 verificar se o direito nacional que regula esse processo prevê regras menos favoráveis no que diz respeito à admissibilidade e à exploração de tais informações e de tais elementos de prova do que as que regulam as informações e os elementos de prova obtidos em violação do direito interno.

225 Quanto ao princípio da efetividade, importa assinalar que as regras nacionais relativas à admissibilidade e à exploração de informações e de elementos de prova têm por objetivo, em virtude das opções efetuadas pelo direito nacional, evitar que informações e elementos de prova obtidos de forma ilegal prejudiquem indevidamente uma pessoa suspeita de ter cometido infrações penais. Ora, este objetivo, segundo o direito nacional, pode ser atingido não só por uma proibição de exploração de tais informações e de tais elementos de prova, mas igualmente por regras e práticas nacionais que regulam a apreciação e a ponderação das informações e dos elementos de prova, ou mesmo através de uma consideração do seu caráter ilegal no âmbito da determinação da pena.

226 Assim sendo, resulta da jurisprudência do Tribunal de Justiça que a necessidade de excluir as informações e os elementos de prova obtidos em violação das disposições do direito da União deve ser apreciada à luz, nomeadamente, do risco que a admissibilidade de tais informações e elementos de prova comporta para o respeito do princípio do contraditório e, portanto, do direito a um processo equitativo (v., neste sentido, Acórdão de 10 de abril de 2003, Steffensen, C-276/01, EU:C:2003:228, n.os 76 e 77). Ora, um órgão jurisdicional que considera que uma parte não está em condições de comentar eficazmente um meio de prova que diz respeito a um domínio que escape ao conhecimento dos juízes e seja suscetível de influenciar de modo preponderante a apreciação dos factos deve declarar uma violação do direito a um processo equitativo e excluir esse meio de prova a fim de evitar tal violação (v., neste sentido, Acórdão de 10 de abril de 2003, Steffensen, C-276/01, EU:C:2003:228, n.os 78 e 79).

227 Por conseguinte, o princípio da efetividade impõe que o tribunal penal nacional rejeite as informações e elementos de prova obtidos através de uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização incompatível com o direito da União, no âmbito de um processo

penal instaurado contra pessoas suspeitas da prática de crimes, se essas pessoas não estiverem em condições de se pronunciarem eficazmente sobre essas informações e elementos de prova, provenientes de um domínio que escapa ao conhecimento dos juízes e que são suscetíveis de influenciar de forma preponderante a apreciação dos factos.

228 Tendo em consideração o exposto, deve responder-se à terceira questão no processo C-520/18 que um órgão jurisdicional não pode aplicar uma disposição do seu direito nacional que o habilita a limitar no tempo os efeitos de uma declaração de ilegalidade para a qual é competente, por força desse direito, em relação a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas, tendo em vista, designadamente, a salvaguarda da segurança nacional e a luta contra a criminalidade, uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização incompatível com 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. Este artigo 15.º, n.º 1, interpretado à luz do princípio da efetividade, impõe que o tribunal criminal nacional afaste as informações e elementos de prova obtidos através de uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização incompatível com o direito da União, no âmbito de um processo penal instaurado contra pessoas suspeitas de atos de criminalidade, se essas pessoas não estiverem em condições de se pronunciarem eficazmente sobre essas informações e elementos de prova, provenientes de um domínio que escapa ao conhecimento dos juízes e que são suscetíveis de influenciar de forma preponderante a apreciação dos factos.

Quanto às despesas

229 Revestindo o processo, quanto às partes na causa principal, a natureza de incidente suscitado perante os órgãos jurisdicionais de reenvio, compete a estes 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 eletrónica (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, para as finalidades previstas nesse artigo 15.º, n.º 1, a título preventivo, uma conservação generalizada e indiferenciada de dados de tráfego e de 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:**

   – **permitam, para efeitos da 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;**

– **prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação selecionada 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;**

– **prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;**

– **prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública, uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, e**

– **permitam, para efeitos da luta contra a criminalidade grave e, *a fortiori*, da salvaguarda da segurança nacional, impor aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, o dever de procederem, por um determinado período, à conservação rápida de 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 dispõem 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 não se opõe a uma regulamentação nacional que impõe aos prestadores de serviços de comunicações eletrónicas que recorram, por um lado, à análise automatizada e à recolha em tempo real de dados de tráfego e de dados de localização e, por outro, à recolha em tempo real de dados técnicos relativos à localização dos equipamentos terminais utilizados, quando**

– **o recurso à análise automatizada esteja limitado a situações em que um Estado-Membro se encontra confrontado com uma ameaça grave para a segurança nacional que se revele real e atual ou previsível, podendo o recurso a essa análise ser objeto de fiscalização efetiva, quer por um órgão jurisdicional quer por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos, destinada a verificar a existência de uma situação que justifique a referida medida, bem como o respeito das condições e das garantias que devem estar previstas, e quando**

– **o recurso a uma recolha em tempo real de dados de tráfego e de dados de localização esteja limitado às pessoas em relação às quais existe uma razão válida para suspeitar que estão de alguma forma envolvidas em atividades terroristas e esteja sujeito a fiscalização prévia, quer por um órgão jurisdicional quer por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos, a fim de assegurar que tal recolha em tempo real apenas é autorizada no limite do estritamente necessário. Em caso de urgência devidamente justificada, a fiscalização deve ser efetuada rapidamente.**

3) **A Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico»), deve ser interpretada no sentido de que não é aplicável em matéria de proteção da confidencialidade das comunicações e das pessoas singulares no que diz respeito ao tratamento de dados pessoais no âmbito dos serviços da sociedade de informação, sendo esta proteção regulada, consoante o caso, pela Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, ou pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46. O artigo 23.º, n.º 1, do Regulamento 2016/679, 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 regulamentação nacional que impõe aos fornecedores de acesso a serviços de comunicação ao público em linha e aos prestadores de serviços de armazenamento a conservação generalizada e indiferenciada, nomeadamente, dos dados pessoais relativos a esses serviços.**

4) **Um órgão jurisdicional não pode aplicar uma disposição do seu direito nacional que o habilita a limitar no tempo os efeitos de uma declaração de ilegalidade para a qual é competente, por força desse direito, em relação a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas, tendo em vista, designadamente, a salvaguarda da segurança nacional e a luta contra a criminalidade, uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização incompatível com 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. Este artigo 15.º, n.º 1, interpretado à luz do princípio da efetividade, impõe que o tribunal criminal nacional afaste as informações e elementos de prova obtidos através de uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização incompatível com o direito da União, no âmbito de um processo penal instaurado contra pessoas suspeitas de atos de criminalidade, se essas pessoas não estiverem em condições de se pronunciarem eficazmente sobre essas informações e elementos de prova, provenientes de um domínio que escapa ao conhecimento dos juízes e que são suscetíveis de influenciar de forma preponderante a apreciação dos factos.**

Assinaturas