Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

21 de dezembro de 2016*

«Reenvio prejudicial — Comunicações eletrónicas — Tratamento de dados pessoais — Confidencialidade das comunicações eletrónicas — Proteção — Diretiva 2002/58/CE — Artigos 5.°, 6.° e 9.° bem como artigo 15.º, n.º 1 — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.°, 8.° e 11.° bem como artigo 52.º, n.º 1 — Legislação nacional — Prestadores de serviços de comunicações eletrónicas — Obrigação que incide sobre a conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização — Autoridades nacionais — Acesso aos dados — Inexistência de um controlo prévio por parte de um órgão jurisdicional ou uma autoridade administrativa independente — Compatibilidade com o direito da União»

Nos processos apensos C-203/15 e C-698/15,

que têm por objeto pedidos de decisão prejudicial nos termos do artigo 267.º TFUE, apresentados pelo Kammarrätten i Stockholm (Tribunal Administrativo de Segunda Instância de Estocolmo, Suécia) e pela Court of Appeal (England & Wales) (Civil Division) [Tribunal de Segunda Instância (Inglaterra e País de Gales) (Secção Cível), Reino Unido], por decisões, respetivamente, de 29 de abril de 2015 e de 9 de dezembro de 2015, entradas no Tribunal de Justiça em 4 de maio de 2015 e em 28 de dezembro de 2015, nos processos

Tele2 Sverige AB (C-203/15)

contra

Post- och telestyrelsen,

e

Secretary of State for the Home Department (C-698/15)

contra

Tom Watson,

Peter Brice,

Geoffrey Lewis,

sendo intervenientes:

Open Rights Group,

Privacy International,

* Línguas de processo: sueco e inglês.

The Law Society of England and Wales,

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: K. Lenaerts, presidente, A. Tizzano, vice-presidente, R. Silva de Lapuerta, T. von Danwitz (relator), J. L. da Cruz Vilaça, E. Juhász e M. Vilaras, presidentes de secção, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen e C. Lycourgos, juízes,

advogado-geral: H. Saugmandsgaard Øe,

secretário: C. Strömholm, administradora,

vista a decisão do presidente do Tribunal de Justiça de 1 de fevereiro de 2016, de submeter o processo C-698/15 à tramitação acelerada prevista no artigo 105.º, n.º 1, do Regulamento de Processo do Tribunal de Justiça,

vistos os autos e após a audiência de 12 de abril de 2016,

vistas as observações apresentadas:

— em representação da Tele2 Sverige AB, por M. Johansson e N. Torgerzon, advokater, E. Lagerlöf e S. Backman,

— em representação de T. Watson, por J. Welch e. E. Norton, solicitors, I. Steele, advocate, B. Jaffey, barrister, e D. Rose, QC,

— em representação de P. Brice e G. Lewis, por A. Suterwalla e R. de Mello, barristers, R. Drabble, QC, e S. Luke, solicitor,

— em representação do Open Rights Group e da Privacy International, por D. Carey, solicitor, R. Mehta e J. Simor, barristers,

— em representação da The Law Society of England and Wales, por T. Hickman, barrister, e N. Turner,

— em representação do Governo sueco, por A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren e por L. Swedenborg, na qualidade de agentes,

— em representação do Governo do Reino Unido, por S. Brandon, L. Christie e V. Kaye, na qualidade de agentes, assistidos por D. Beard, G. Facenna e J. Eadie, QC, e S. Ford, barrister,

— em representação do Governo belga, por J.-C. Halleux, S. Vanrie e C. Pochet, na qualidade de agentes,

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

— em representação do Governo dinamarquês, por C. Thorning e M. Wolff, na qualidade de agentes,

— em representação do Governo alemão, por T. Henze, M. Hellmann e J. Kemper, na qualidade de agentes, assistidos por M. Kottmann e U. Karpenstein, Rechtsanwälte,

— em representação do Governo estónio, por K. Kraavi-Käerdi, na qualidade de agente,

— em representação da Irlanda, por E. Creedon, L. Williams e A. Joyce, na qualidade de agentes, assistidos por D. Fennelly, BL,

— em representação do Governo espanhol, por A. Rubio González, na qualidade de agente,

— em representação do Governo francês, por G. de Bergues, D. Colas, F.-X. Bréchot e C. David, na qualidade de agentes,

— em representação do Governo cipriota, por K. Kleanthous, na qualidade de agente,

— em representação do Governo húngaro, por M. Fehér e G. Koós, na qualidade de agentes,

— em representação do Governo neerlandês, por M. Bulterman, M. Gijzen e J. Langer, na qualidade de agentes,

— em representação do Governo polaco, por B. Majczyna, na qualidade de agente,

— em representação do Governo finlandês, por J. Heliskoski, na qualidade de agente,

— em representação da Comissão Europeia, por H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira e J. Vondung, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 19 de julho de 2016,

profere o presente

Acórdão

1 Os pedidos de decisão prejudicial têm por objeto a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 201, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO 2009, L 337, p. 11) (a seguir «Diretiva 2002/58»), lido à luz dos artigos 7.°, 8.°, e 52.°, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

2 Estes pedidos foram apresentados no âmbito de dois litígios que opõem, no primeiro, a Tele2 Sverige AB à Post- och telestyrelsen (autoridade sueca de supervisão dos correios e telecomunicações, a seguir «PTS»), relativamente a uma injunção que esta fez à Tele2 Sverige para proceder à conservação dos dados de tráfego e dos dados de localização dos seus assinantes e utilizadores registados (processo C-203/15), e, no segundo, Tom Watson, Peter Brice e Geoffrey Lewis ao Secretary of State for the Home Department (Ministro da Administração Interna, Reino Unido da Grã-Bretanha e da Irlanda do Norte), relativamente à conformidade com o direito da União da section 1 do Data Retention and Investigatory Powers Act 2014 (Lei de 2014 sobre a conservação de dados e os poderes de investigação, a seguir «DRIPA») (processo C-698/15).

Quadro jurídico

Direito da União

Diretiva 2002/58

3 Os considerandos 2, 6, 7, 11, 21, 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.° e 8.° [desta].

[…]

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

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

[…]

(11) Tal como a Diretiva 95/46/CE [do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31)], a presente diretiva não trata questões relativas à proteção dos direitos e liberdades fundamentais relacionadas com atividades não reguladas pelo direito comunitário. Portanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.º 1 do artigo 15.º da presente diretiva, necessários para a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal. Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais.

[…]

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

(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. […]

[…]

(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. […]»

4 O artigo 1.º da Diretiva 2002/58, intitulado «Âmbito e objetivos», dispõe:

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

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

3. A presente diretiva não é aplicável a atividades fora do âmbito do Tratado que institui a Comunidade Europeia, tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia, e em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em matéria de direito penal.»

5 Nos termos do artigo 2.º da Diretiva 2002/58, intitulado «Definições»:

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

São também aplicáveis as seguintes definições:

[…]

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

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

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

[…]»

6 O artigo 3.º da Diretiva 2002/58, intitulado «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.»

7 O artigo 4.º desta diretiva, intitulado «Segurança do processamento», está redigido nos seguintes termos:

«1. O prestador de um serviço de comunicações eletrónicas publicamente disponível adotará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes.

1-A. Sem prejuízo do disposto na Diretiva [95/46], as medidas referidas no n.º 1 compreendem, no mínimo:

— a garantia de que aos dados pessoais apenas possa ter acesso pessoal autorizado, para fins autorizados a nível legal,

— a proteção dos dados pessoais armazenados ou transmitidos contra a destruição acidental ou ilegal, a perda ou alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizados ou ilegais, e

— a garantia da aplicação de uma política de segurança relativa ao tratamento dos dados pessoais.

[…]»

8 Nos termos do artigo 5.º da Diretiva 2002/58, intitulado «Confidencialidade das comunicações»:

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

[…]

3. Os Estados-Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Diretiva [95/46], nomeadamente sobre os objetivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.»

9 O artigo 6.º da Diretiva 2002/58, intitulado «Dados de tráfego», dispõe:

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

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

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

[…]

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

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

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

11 O artigo 15.º da referida diretiva, intitulado «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.° e 6.°, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva [95/46]. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do Tratado da União Europeia,

[…]

1-B. Os prestadores estabelecem procedimentos internos para responder aos pedidos de acesso aos dados pessoais dos utilizadores com base nas disposições nacionais aprovadas nos termos do n.º 1. Aqueles prestam às autoridades nacionais competentes, a pedido destas, informação sobre esses procedimentos, o número de pedidos recebidos, a justificação jurídica invocada e a resposta dada.

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.

[…]»

Diretiva 95/46

12 O artigo 22.º da Diretiva 95/46, que consta do seu capítulo III, está redigido nos seguintes termos:

«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 2006/24/CE

13 O artigo 1.º da 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), intitulado «Objeto e âmbito de aplicação», previa, no seu n.º 2:

«A presente diretiva é aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares quer a pessoas coletivas, bem como aos dados conexos necessários para identificar o assinante ou o utilizador registado. A presente diretiva não é aplicável ao conteúdo das comunicações eletrónicas, incluindo as informações consultadas utilizando uma rede de comunicações eletrónicas.»

14 Nos termos do artigo 3.º desta diretiva, intitulado «Obrigação de conservação de dados»:

«1. Em derrogação aos artigos 5.°, 6.° e 9.° da Diretiva [2002/58], os Estados-Membros devem tomar medidas para garantir a conservação, em conformidade com as disposições da presente diretiva, dos dados especificados no artigo 5.º da presente diretiva, na medida em que sejam gerados ou tratados no contexto da oferta dos serviços de comunicações em causa por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações quando estes fornecedores estejam sob a sua jurisdição.

2. A obrigação de conservação de dados imposta no n.º 1 inclui a conservação dos dados especificados no artigo 5.º relativos a chamadas telefónicas falhadas, quando gerados ou tratados, e armazenados (no caso de dados telefónicos) ou registados (no caso de dados da Internet) por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis, ou de uma rede pública de comunicações, que estejam sob a jurisdição do Estado-Membro em questão, no contexto da oferta de serviços de comunicação. A presente diretiva não estabelece a conservação de dados relativos a chamadas não estabelecidas.»

Direito sueco

15 Resulta de decisão de reenvio no processo C-203/15 que o legislador sueco, para efeitos de transposição da Diretiva 2006/24 para o direito nacional, alterou a lagen (2003:389) om elektronisk kommunikation [Lei (2003:389) relativa às comunicações eletrónicas, a seguir «LEK»] e o förordningen (2003:396) om elektronisk kommunikation [Regulamento (2003:396) relativo às comunicações eletrónicas]. Os dois diplomas, na sua versão aplicável ao litígio do processo principal, contêm normas que têm por objeto a conservação dos dados relativos às comunicações eletrónicas e o acesso a esses dados pelas autoridades nacionais.

16 Além disso, o acesso aos referidos dados está regulamentado pela lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet [Lei (2012:278) sobre a comunicação de dados relativos a comunicações eletrónicas no âmbito das atividades de informação das autoridades repressivas, a seguir «Lei 2012:278»] e pelo rättegångsbalken (Código de Processo Judicial, a seguir «RB»).

Quanto à obrigação de conservação dos dados relativos às comunicações eletrónicas

17 Segundo as indicações do órgão jurisdicional de reenvio no processo C-203/15, as disposições do § 16 a do capítulo 6 da LEK, conjugadas com o § 1 do capítulo 2 desta lei, preveem uma obrigação de os prestadores de serviços de comunicações eletrónicas conservarem os dados cuja conservação estava prevista na Diretiva 2006/24. Trata-se dos dados relativos às subscrições e a todas as comunicações eletrónicas necessárias para encontrar e identificar a origem e o destino de uma comunicação, para

determinar a data, a hora, a duração e a natureza dessa comunicação, para identificar o equipamento de comunicação utilizado e para localizar o equipamento móvel de comunicação utilizado no início e no fim da comunicação. A obrigação de conservação dos dados abrange os dados gerados ou tratados no âmbito de um serviço telefónico, de um serviço telefónico através de uma ligação móvel, de um sistema de correio eletrónico, de um serviço de acesso à Internet, bem como de um serviço de oferta de capacidade de acesso à Internet (forma de conexão). Esta obrigação também inclui os dados relativos às comunicações falhadas. No entanto, não abrange o conteúdo das comunicações.

18 Os §§ 38 a 43 do Regulamento (2003:396) relativo às comunicações eletrónicas especificam as categorias de dados que devem ser conservados. Relativamente aos serviços telefónicos, devem ser conservados, nomeadamente, os dados relativos às chamadas e aos números chamados, bem como as datas e horas rastreáveis do início e do fim da comunicação. Relativamente aos serviços telefónicos através de uma ligação móvel, aplicam-se obrigações suplementares como, por exemplo, a conservação dos dados de localização do início e do fim da comunicação. Relativamente aos serviços telefónicos através de pacotes IP, devem designadamente ser conservados, para além dos dados acima referidos, os relativos aos endereços IP do chamador e do chamado. Relativamente aos serviços de correio eletrónico, devem ser conservados, nomeadamente, os dados relativos aos números dos emissores e dos destinatários, os endereços IP ou qualquer outro endereço de correio eletrónico. No que se refere aos serviços de acesso à Internet, devem ser conservados, por exemplo, os dados relativos aos endereços IP dos utilizadores e as datas e horas rastreáveis de início e de fim da ligação ao serviço de acesso à Internet.

Quanto ao período de conservação dos dados

19 Em conformidade com o § 16 d do capítulo 6 da LEK, os dados referidos no § 16 a deste capítulo devem ser conservados pelos prestadores de serviços de comunicações eletrónicas durante seis meses a contar do dia do fim da comunicação. Salvo disposições em contrário previstas no § 16 d, segundo parágrafo, do referido capítulo, devem em seguida ser imediatamente apagados.

Quanto ao acesso aos dados conservados

20 O acesso aos dados conservados pelas autoridades nacionais é regulado pelas disposições da Lei 2012:278, da LEK e do RB.

– Lei 2012:278

21 No âmbito dos serviços de informações, a polícia nacional, a Säkerhetspolisen (Serviço de Segurança, Suécia) e a Tullverket (Serviços Aduaneiros, Suécia) podem, ao abrigo do § 1 da Lei 2012:278, nas condições estabelecidas nesta lei e sem o conhecimento do operador de uma rede eletrónica de comunicações ou de um serviço de comunicações eletrónicas autorizado ao abrigo da LEK, proceder à recolha de dados respeitantes às mensagens transmitidas numa rede de comunicações eletrónicas, aos equipamentos de comunicação eletrónica presentes numa determinada zona geográfica e na ou nas zonas geográficas onde se situa ou estava situado um equipamento de comunicações eletrónicas.

22 Em conformidade com os §§ 2 e 3 da Lei 2012:278, os dados podem, em princípio, ser recolhidos se, em função das circunstâncias, a medida for particularmente necessária para prevenir, impedir ou constatar uma atividade criminosa que implique uma ou várias infrações sancionadas com uma pena de prisão igual ou superior a dois anos, ou um dos atos enumerados no § 3 desta lei que inclua infrações sancionadas com uma pena de prisão inferior a dois anos. Os motivos que justificam esta medida devem ser superiores às considerações relativas à infração ou ao prejuízo que esta implica para o seu destinatário ou para um interesse que se lhe oponha. Em conformidade com o § 5 da referida lei, a duração da medida não pode ser superior a um mês.

23 A decisão de adotar tal medida compete ao diretor da autoridade em causa ou a uma pessoa com poderes delegados para o efeito. Não está sujeita à fiscalização prévia de uma autoridade judiciária ou de uma autoridade administrativa independente.

24 Nos termos do § 6 da Lei 2012:278, a Säkerhets och integritetsskyddsnämnden (Comissão de segurança e de proteção da integridade, Suécia) deve ser informada de qualquer decisão que autorize a recolha de dados. De acordo com o § 1 da lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet [Lei (2007:980) relativa ao controlo de determinadas atividades repressivas], esta autoridade exerce uma supervisão sobre a aplicação da lei pelas autoridades repressivas.

– LEK

25 Nos termos do § 22, primeiro parágrafo, n.º 2, do capítulo 6, da LEK, todos os prestadores de serviços de comunicações eletrónicas devem comunicar os dados relativos a uma assinatura, a pedido do Ministério Público, da polícia nacional, da polícia de segurança ou de qualquer outra autoridade pública de combate à criminalidade, caso os dados digam respeito a uma suspeita de infração. De acordo com as informações do órgão jurisdicional de reenvio no processo C-203/15, não é necessário que se trate de um crime grave.

– RB

26 O RB regula a comunicação dos dados conservados às autoridades nacionais no âmbito de inquéritos preliminares. Em conformidade com o § 19 do capítulo 27 do RB, a «monitorização de comunicações eletrónicas» sem o conhecimento de terceiros é, em princípio, autorizada no âmbito de inquéritos preliminares que visam, nomeadamente, infrações sancionadas com uma pena de prisão igual ou superior a seis meses. Por «monitorização de comunicações eletrónicas» deve entender-se, em conformidade com o § 19 do capítulo 27 do RB, a obtenção de dados sem o consentimento de terceiros relativamente a uma mensagem transmitida através de uma rede de comunicações eletrónicas, dos equipamentos de comunicação eletrónica presentes ou que tenham estado presentes numa zona geográfica determinada, bem como da ou das zonas geográficas onde está ou esteve presente um determinado equipamento de comunicação eletrónica.

27 De acordo com as indicações do órgão jurisdicional de reenvio no processo C-203/15, dados relativos ao conteúdo de uma mensagem não podem ser recolhidos com base no § 19 do capítulo 27 do RB. Em princípio, a monitorização de comunicações eletrónicas só pode ser ordenada, nos termos do § 20 do capítulo 27 do RB, quando haja indícios plausíveis que permitam suspeitar que uma pessoa é a autora de um crime e que a medida é especialmente necessária para a investigação, devendo esta última, além disso, dizer respeito a um crime punido com uma pena de prisão igual ou superior a dois anos ou sendo a tentativa também punida, a preparação ou a conspiração para a prática desse crime. Em conformidade com o § 21 do capítulo 27 de RB, o Ministério Público deve, salvo em situações de urgência, pedir ao juiz competente autorização para proceder à monitorização de comunicações eletrónicas.

Quanto à segurança e à proteção dos dados conservados

28 Nos termos do § 3 a do capítulo 6 da LEK, os prestadores de serviços de comunicações eletrónicas obrigados a proceder à conservação dos dados devem adotar as medidas de ordem técnica e de organização adequadas para garantir a proteção dos dados durante o seu tratamento. No entanto, segundo as informações do órgão jurisdicional de reenvio no processo C-203/15, o direito sueco não prevê disposições relativas ao local de conservação dos dados.

Direito do Reino Unido

DRIPA

29 A section 1 da DRIPA, intitulada «Poderes para conservar dados pertinentes relativos a comunicações, sujeitos a garantias», dispõe:

«1) O [Ministro da Administração Interna] pode, mediante notificação [a seguir «notificação que ordena a conservação»] exigir que um operador público de telecomunicações conserve dados pertinentes relativos a comunicações caso entenda que essa exigência é necessária e proporcionada à prossecução de um ou mais dos objetivos mencionados nas alíneas (a) a (h) da section 22(2), do Regulation of Investigatory Powers Act 2000 [Lei de 2000 relativa à regulamentação dos poderes de investigação] (objetivos para os quais os dados relativos a comunicações podem ser obtidos).

(2) A notificação que ordena a conservação pode:

(a) ter por destinatário um determinado operador ou uma categoria de operadores;

(b) exigir a conservação de todos os dados ou de uma categoria de dados;

(c) especificar o período ou os períodos durante os quais os dados devem ser conservados;

(d) conter outros requisitos ou restrições em relação à conservação de dados;

(e) prever disposições diferentes para finalidades diferentes;

(f) dizer respeito a dados, existentes ou não existentes na data em que a notificação é emitida, ou na data em que entrou em vigor.

(3) O [Ministro da Administração Interna] pode, por via de regulamentos, aprovar mais disposições sobre a conservação de dados pertinentes relativos a comunicações.

(4) Essas disposições podem, em especial, ter por objeto:

(a) as condições prévias da emissão de uma notificação que ordena a conservação;

(b) o período máximo durante o qual os dados devem ser conservados em aplicação de uma notificação que ordena a conservação;

(c) o conteúdo, a emissão, a entrada em vigor, a reapreciação, a alteração ou a revogação de uma notificação que ordena a conservação;

(d) a integridade, a segurança ou a proteção dos dados conservados nos termos da presente section, o acesso a esses dados bem como a sua divulgação ou a sua destruição;

(e) a aplicação dos requisitos ou das restrições pertinentes ou a verificação desses requisitos ou restrições;

(f) um código de boas práticas relativas a exigências, restrições ou poderes pertinentes;

(g) o reembolso pelo [Ministro da Administração Interna] (sob determinadas condições ou não) das despesas incorridas pelos operadores públicos de telecomunicações no cumprimento das exigências ou das restrições pertinentes;

(h) o facto de o [Data Retention (EC Directive) Regulations 2009 (Regulamento de 2009 relativo à conservação dos dados na aceção da Diretiva CE)] cessar a sua vigência e a transição para a conservação dos dados ao abrigo da presente section.

(5) O período máximo estabelecido ao abrigo do n.º 4 (b), não pode exceder 12 meses a contar da data especificada relativamente aos dados visados pelos regulamentos referidos no n.º 3.

[…]»

30 Nos termos da section 2 da DRIPA entende-se por «dados pertinentes relativos a comunicações» os «dados pertinentes relativos a comunicações do tipo das comunicações mencionadas no anexo ao Regulamento de 2009 relativo à conservação dos dados na aceção da diretiva CE, na medida em que esses dados sejam gerados ou tratados no Reino Unido por operadores de telecomunicações públicas, no âmbito da prestação dos serviços de telecomunicações em causa».

RIPA

31 A section 21 da Lei de 2000 relativa à regulamentação dos poderes de investigação (a seguir «RIPA»), que consta do capítulo II desta lei, intitulado «Recolha e divulgação dos dados relativos a comunicações», precisa, no seu n.º 4:

«Para efeitos do presente capítulo, entende-se por "dados relativos a comunicações" qualquer um dos conceitos seguintes:

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

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

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

32 Segundo as indicações constantes da decisão de reenvio no processo C-698/15, estes dados incluem os «dados de localização de um utilizador», mas não os relativos ao conteúdo de uma comunicação.

33 Quanto ao acesso aos dados conservados, a section 22 da RIPA dispõe:

«(1) Esta section é aplicável sempre que uma pessoa responsável para efeitos deste capítulo considere que é necessário, pelas razões abrangidas no n.º 2 da presente section, obter a totalidade dos dados da comunicação.

(2) Pelas razões abrangidas pelo presente número, devem ser obtidos dados relativos a comunicações, se forem necessários:

(a) no interesse da segurança nacional;

(b) para efeitos de prevenção ou de deteção da criminalidade ou de prevenção da perturbação da ordem pública;

(c) no interesse do bem-estar económico do Reino Unido;

(d) no interesse da segurança pública;

(e) para efeitos de proteção da saúde pública;

(f) para efeitos de liquidação ou de cobrança de impostos, direitos, taxas ou outra tributação, contribuição ou encargo devidos à administração pública;

(g) para efeitos de prevenção, em caso de urgência, de morte, de lesões ou de qualquer dano para a saúde física ou mental de uma pessoa, ou de minimização de lesões ou danos para a saúde física ou mental de uma pessoa;

(h) para qualquer outro fim [não abrangido pelas alíneas (a) a (g)] estabelecido por despacho do [Ministro da Administração Interna].

[…]

(4) Sem prejuízo do disposto no n.º 5, quando considerar que um operador de telecomunicações ou um operador postal está, poderá estar, ou poderá reunir as condições para estar na posse de dados, a pessoa responsável pode exigi-los por meio de requerimento enviado a esse operador para que este operador:

(a) obtenha os dados, se não estiverem já na sua posse, e

(b) divulgue, em qualquer hipótese, todos os dados que estejam na sua posse ou que venha a obter posteriormente.

(5) A pessoa responsável não deve dar autorização em conformidade com o n.º 3 ou fazer um requerimento nos termos do n.º 4, salvo se considerar que a obtenção dos dados em questão resultante de um comportamento autorizado ou exigido por força de uma autorização ou de um requerimento é proporcionada à finalidade pretendida com a obtenção dos dados.»

34 Em conformidade com a section 65 da RIPA, podem ser apresentadas queixas ao Investigatory Powers Tribunal (Tribunal com competências de Instrução, Reino Unido) se existirem razões para crer que determinados dados foram obtidos de forma inapropriada.

Data Retention Regulations 2014

35 O Data Retention Regulations 2014 (Regulamento de 2014 relativo à conservação de dados), aprovado ao abrigo da DRIPA, está dividido em três partes, a segunda das quais compreende as sections 2 a 14 deste regulamento. A section 4, intitulada «Requerimentos em matéria de conservação», prevê:

«(1) os requerimentos em matéria de conservação devem precisar:

(a) o operador público de telecomunicações (ou a descrição dos operadores) a quem se dirigem,

(b) os dados relativos às comunicações pertinentes que devem ser conservados,

(c) o período ou períodos durante os quais os dados devem ser conservados,

(d) qualquer outro requisito ou restrição relacionado com a conservação dos dados.

(2) Um requerimento em matéria de conservação não pode exigir que um dado seja conservado mais do que 12 meses a partir:

(a) no caso dos dados de tráfego ou dos dados relativos à utilização do serviço, do dia da comunicação em causa e

(b) no caso dos dados relativos aos assinantes, do dia em que a pessoa em causa pôs termo ao serviço de comunicações em causa ou do dia em que o dado foi alterado (se este for anterior).

[…]»

36 Nos termos da section 7 deste regulamento, intitulada «Integridade e segurança dos dados»:

«(1) Um operador público de telecomunicações que conserve dados nos termos da section 1 da [DRIPA] deve:

(a) assegurar-se de que os dados têm a mesma integridade e estão submetidos, pelo menos, ao mesmo nível de segurança e de proteção que os dados dos sistemas de que provêm,

(b) assegurar-se, por meios técnicos e de organização adequados, que apenas o pessoal especialmente autorizado pode ter acesso aos dados, e

(c) proteger, por meios técnicos e de organização adequados, os dados contra a destruição ilícita, as perdas ou os danos de origem acidental, ou contra a conservação, o tratamento, o acesso ou a divulgação ilícitos ou não autorizados.

(2) Um operador público de telecomunicações que conserve dados relativos a comunicações nos termos da section 1 da [DRIPA] deve destruir os dados se a conservação dos dados deixar de estar autorizada por esta section e não estiver de outra forma autorizada por lei.

(3) A exigência de destruição dos dados prevista no n.º 2 consiste em apagar os dados de forma a tornar impossível o acesso aos mesmos.

(4) Basta que o operador adote disposições para que o apagamento dos dados ocorra mensalmente ou a intervalos mais curtos, consoante a capacidade, na prática, do operador.»

37 A section 8 do referido regulamento, intitulada «Divulgação dos dados conservados», dispõe:

«(1) Um operador público de telecomunicações deve implementar sistemas de segurança adequados (incluindo medidas técnicas e de organização) que determinem o acesso aos dados relativos a comunicações conservadas nos termos da section 1 da [DRIPA] para prevenir qualquer divulgação que não se enquadre na section 1, n.º 6, alínea (a), da [DRIPA].

(2) Um operador público de telecomunicações que conserve dados nos termos da section 1 da [DRIPA] deve conservar os dados de forma a poder transmiti-los, sem atraso injustificado, em resposta a requerimentos.»

38 A section 9 deste mesmo regulamento, intitulada «Controlo pelo comissário responsável pela informação», enuncia:

«O comissário responsável pela informação deve controlar o cumprimento das exigências ou restrições, previstas nesta parte, relacionadas com a integridade, a segurança e a destruição dos dados conservados nos termos do artigo 1.º da [DRIPA].»

Código das boas práticas

39 O Acquisition and Disclosure of Communications Data Code of Practice (Código das boas práticas relativas à obtenção e à divulgação de dados relativos a comunicações, a seguir «código das boas práticas») contém, nos seus n.os 2.5 a 2.9 e 2.36 a 2.45, orientações sobre a necessidade e a proporcionalidade da obtenção dos dados relativos a comunicações. De acordo com as indicações do órgão jurisdicional de reenvio no processo C-698/15, deve ser dada, em conformidade com os n.os 3.72 a 3.77 deste código, uma atenção especial à necessidade e à proporcionalidade sempre que os pedidos de dados relativos a comunicações digam respeito a uma pessoa que é membro de uma profissão que beneficia de informações protegidas pelo segredo profissional ou que de outro modo sejam confidenciais.

40 Nos termos dos n.os 3.78 a 3.84 do referido código, é necessário um despacho judicial no caso específico de um pedido que diga respeito a dados relativos a comunicações, apresentado com o objetivo de identificar a fonte jornalística. De acordo com os n.os 3.85 a 3.87 do mesmo código, é necessária uma autorização judicial no caso de um pedido de acesso apresentado por autoridades locais. Em contrapartida, o acesso a dados relativos a comunicações protegidos por lei pelo sigilo profissional ou a dados relativos a comunicações respeitantes a médicos, deputados ou ministros de culto não está sujeito a autorização judicial ou a autorização de uma entidade independente.

41 O n.º 7.1 do código das boas práticas prevê que os dados relativos a comunicações adquiridos ou obtidos nos termos das disposições da RIPA, bem como todos os extratos, resumos e cópias desses dados devem ser tratados e armazenados de forma segura. Além disso, devem ser respeitados os requisitos que figuram no Data Protection Act (Lei relativa à proteção de dados).

42 Em conformidade com o n.º 7.18 do código das boas práticas, sempre que uma autoridade pública do Reino Unido considerar a possibilidade de divulgação de dados relativos a comunicações a autoridades estrangeiras, deve, designadamente, verificar se esses dados vão estar protegidos adequadamente. Todavia, resulta do n.º 7.22 deste código que pode ocorrer uma transferência de dados para países terceiros quando essa transferência for necessária por razões relacionadas com um interesse público importante, ainda que o país terceiro não garanta um nível de proteção adequado. De acordo com as indicações do órgão jurisdicional de reenvio no processo C-698/15, o Ministro da Administração Interna pode emitir um certificado de segurança nacional que isente determinados dados do cumprimento das disposições previstas na lei.

43 No n.º 8.1 do referido código, recorda-se que a RIPA instituiu o Interception of Communications Commissioner (Comissário para a interceção de comunicações, Reino Unido), cujas atribuições consistem, designadamente, em supervisionar de forma independente o exercício e a execução dos poderes e deveres enunciados no capítulo II da parte I da RIPA. Como resulta do n.º 8.3 deste mesmo código, este comissário está autorizado, quando puder «provar que alguém foi prejudicado por uma falha intencional ou por negligência», a informar essa pessoa de que existe a suspeita de exercício ilícito de poderes.

Litígios nos processos principais e questões prejudiciais

Processo C-203/15

44 Em 9 de abril de 2014, a Tele2 Sverige, prestador de serviços de comunicações eletrónicas estabelecido na Suécia, notificou a PTS de que, na sequência da declaração de invalidade da Diretiva 2006/24 pelo 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), deixaria, a partir de 14 de abril de 2014, de conservar os dados relativos às comunicações eletrónicas, abrangidos pela LEK, e que procederia à supressão dos dados conservados até essa data.

45 Em 15 de abril de 2014, a Rikspolisstyrelsen (Direção Geral da Polícia Nacional, Suécia) apresentou uma queixa na PTS pelo facto de a Tele2 Sverige ter deixado de lhe comunicar os dados em causa.

46 Em 29 de abril de 2014, o justitieminister (Ministro da Justiça, Suécia) designou um relator especial para analisar a regulamentação sueca em causa à luz do acórdão Digital Rights. Num relatório de 13 de junho de 2014, intitulado «Datalagring, EU-rätten och svensk rätt, n.º Ds 2014:23» (Conservação de dados, direito da União e direito sueco, a seguir «relatório de 2014»), o relator especial concluiu que a regulamentação nacional relativa à conservação dos dados, conforme prevista nos §§ 16 a a 16 f da LEK, não era contrária ao direito da União nem à Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, assinada em Roma em 4 de novembro de 1950 (a seguir «CEDH»). O relator especial sublinhou que o acórdão Digital Rights não podia ser interpretado no sentido de que censurava o princípio em si mesmo de uma conservação generalizada e indiferenciada dos dados. Do seu ponto de vista, o acórdão Digital Rights também não devia ser entendido no sentido de que o Tribunal de Justiça nele tinha estabelecido uma série de critérios que deviam ser integralmente cumpridos para que uma regulamentação pudesse ser considerada proporcionada. Deviam ser apreciadas todas as circunstâncias para determinar a conformidade da regulamentação sueca com o direito da União, como o alcance da conservação dos dados à luz das disposições relativas ao acesso aos dados, à duração da sua conservação, à sua proteção e à sua segurança.

47 Com este fundamento, em 19 de junho de 2014, a PTS informou a Tele2 Sverige de que esta não cumpria as obrigações previstas na regulamentação nacional por não conservar os dados abrangidos pela LEK durante seis meses para efeitos de luta contra a criminalidade. Por injunção de 27 de junho de 2014, a PTS ordenou-lhe em seguida que procedesse, o mais tardar até 25 de julho de 2014, à conservação desses dados.

48 Considerando que o relatório de 2014 se baseava numa interpretação errada do acórdão Digital Rights e que a obrigação de conservação dos dados era contrária aos direitos fundamentais garantidos pela Carta, a Tele2 Sverige intentou uma ação no Förvaltningsrätten i Stockholm (Tribunal Administrativo de Estocolmo, Suécia) contra a decisão de injunção de 27 de junho de 2014. Tendo este último órgão jurisdicional julgado o pedido improcedente por decisão de 13 de outubro de 2014, a Tele2 Sverige interpôs recurso desta decisão no órgão jurisdicional de reenvio.

49 De acordo com o órgão jurisdicional de reenvio, a compatibilidade da regulamentação sueca com o direito da União deve ser apreciada à luz do artigo 15.º, n.º 1, da Diretiva 2002/58. Com efeito, embora esta diretiva consagre o princípio segundo o qual os dados relativos ao tráfego e os dados de localização devem ser apagados ou tornados anónimos quando deixem de ser necessários para a transmissão de uma comunicação, o artigo 15.º, n.º 1, da referida diretiva introduz uma derrogação a este princípio, uma vez que autoriza os Estados-Membros, quando isso for justificado por um dos motivos que enuncia, a limitar esta obrigação de apagar ou de tornar anónimo ou ainda a prever a conservação de dados. Assim, o direito da União permite, em determinadas situações, a conservação dos dados relativos às comunicações eletrónicas.

50 No entanto, o órgão jurisdicional de reenvio interroga-se sobre se uma obrigação generalizada e indiferenciada de conservação dos dados relativos às comunicações eletrónicas, como a que está em causa no processo principal, é compatível, tendo em conta o acórdão Digital Rights, com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.° e 8.°, bem como do artigo 52.º, n.º 1, da Carta. Tendo em conta as opiniões divergentes das partes a este propósito, importa que o Tribunal de Justiça se pronuncie de forma unívoca sobre a questão de saber se, à semelhança daquele que é o entendimento da Tele2 Sverige, a conservação generalizada e indiferenciada dos dados relativos às comunicações eletrónicas é em si mesma incompatível com os artigos 7.° e 8.°, bem como com o artigo 52.º, n.º 1, da Carta, ou se, como resulta do relatório de 2014, a compatibilidade de tal conservação de dados deve ser apreciada à luz das disposições relativas ao acesso aos dados, à sua proteção e à sua segurança, bem como à duração da sua conservação.

51 Nestas condições, o órgão jurisdicional de reenvio decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) É compatível com o artigo 15.º, n.º 1, da Diretiva 2002/58, à luz dos artigos 7.°, 8.° e 52.°, n.º 1, da Carta, uma obrigação geral de conservar dados de tráfego relativos a todas as pessoas, a todos os meios de comunicação eletrónica e a todos os dados de tráfego, sem quaisquer distinções, limitações ou exceções, para efeitos do objetivo de combate à criminalidade […]?

2) Em caso de resposta negativa à primeira questão, pode, não obstante, a conservação ser permitida quando:
   a) o acesso das autoridades nacionais aos dados conservados seja determinado conforme [descrito nos n.os 19 a 36 da decisão de reenvio], e
   b) [as exigências] de segurança sejam regulad[a]s conforme [descrito nos n.os 38 a 43 da decisão de reenvio], e
   c) todos os dados relevantes sejam conservados pelo período de seis meses, calculado a partir do dia em que cessa a comunicação, sendo subsequentemente apagados conforme [descrito no n.º 37 da decisão de reenvio]?»

Processo C-698/15

52 T. Watson, P. Brice e G. Lewis interpuseram, separadamente, na High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [Supremo Tribunal de Justiça (Inglaterra e País de Gales), Secção do Contencioso Administrativo (Secção Divisional), Reino Unido], um recurso jurisdicional com o objetivo de fiscalizar a legalidade da section 1 da DRIPA, invocando, designadamente, a incompatibilidade desta section com os artigos 7.° e 8.° da Carta bem como com o artigo 8.º da CEDH.

53 Por acórdão de 17 de julho de 2015, a High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [Supremo Tribunal de Justiça (Inglaterra e País de Gales), Secção do Contencioso Administrativo (Secção Divisional)] declarou que o acórdão Digital Rights estabelecia «exigências imperativas de direito da União» aplicáveis às regulamentações dos Estados-Membros em matéria de conservação de dados relativos a comunicações bem como ao acesso a esses dados. Segundo este último órgão jurisdicional, uma vez que o Tribunal de Justiça considerou, nesse acórdão, que a Diretiva 2006/24 era incompatível com o princípio da proporcionalidade, uma regulamentação nacional com um conteúdo idêntico ao desta diretiva também não podia ser compatível com este princípio. Resulta da lógica subjacente ao acórdão Digital Rights que uma legislação que estabelece um regime generalizado de conservação dos dados relativos a comunicações viola os direitos garantidos nos artigos 7.° e 8.° da Carta, a menos que essa legislação seja completada por um regime de acesso aos dados, definido pelo direito nacional, que preveja garantias suficientes para a salvaguarda desses direitos. Assim, a section 1 da DRIPA não é compatível com os artigos 7.° e 8.° da

Carta na medida em que não estabelece regras claras e precisas relativas ao acesso e à utilização dos dados conservados e na medida em que não subordina o acesso a esses dados a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente.

54 O Ministro da Administração Interna interpôs recurso desse acórdão na Court of Appeal (England & Wales) (Civil Division) [Tribunal de Recurso (Inglaterra e País de Gales) (Divisão Cível), Reino Unido].

55 Este órgão jurisdicional salienta que a section 1, n.º 1, da DRIPA atribui competência ao Ministro da Administração Interna para aprovar, sem autorização prévia de um órgão jurisdicional ou de uma entidade administrativa independente, um regime geral que imponha aos operadores públicos de telecomunicações a conservação de todos os dados relativos a qualquer serviço postal ou a qualquer serviço de telecomunicações durante um prazo máximo de doze meses, sempre que considere que essa exigência é necessária e proporcionada para prosseguir as finalidades enunciadas na regulamentação do Reino Unido. Mesmo que esses dados não incluam o conteúdo de uma comunicação, podem ter um caráter particularmente intrusivo na vida privada dos utilizadores de serviços de comunicações.

56 Na decisão de reenvio e no seu acórdão de 20 de novembro de 2015, proferido no âmbito do processo de recurso e por meio do qual foi decidido submeter ao Tribunal de Justiça o presente pedido de decisão prejudicial, o órgão jurisdicional de reenvio considera que as normas nacionais relativas à conservação dos dados se enquadram necessariamente no artigo 15.º, n.º 1, da Diretiva 2002/58 e devem, por conseguinte, respeitar as exigências que decorrem da Carta. No entanto, em conformidade com o artigo 1.º, n.º 3, desta diretiva, o legislador da União não harmonizou as normas relativas ao acesso aos dados conservados.

57 No que respeita ao impacto do acórdão Digital Rights nas questões suscitadas no litígio do processo principal, o órgão jurisdicional de reenvio salienta que, no processo que deu origem a esse acórdão, o Tribunal de Justiça tinha sido chamado a pronunciar-se sobre a validade da Diretiva 2006/24 e não sobre a validade de uma regulamentação nacional. Tendo em conta, nomeadamente, a estreita relação existente entre a conservação dos dados e o acesso a esses dados, seria indispensável que esta diretiva fosse acompanhada de uma série de garantias e que o acórdão Digital Rights tivesse analisado, aquando do exame da legalidade do regime de conservação dos dados estabelecido pela referida diretiva, as normas relativas ao acesso a esses dados. Por conseguinte, o Tribunal de Justiça não pretendeu enunciar, nesse acórdão, requisitos imperativos aplicáveis às regulamentações nacionais relativas ao acesso aos dados que não apliquem o direito da União. Além disso, o raciocínio do Tribunal de Justiça estava estreitamente ligado ao objetivo prosseguido por essa mesma diretiva. Todavia, uma regulamentação nacional deve ser apreciada à luz dos objetivos por si prosseguidos e do seu contexto.

58 No que respeita à necessidade de submeter um pedido de decisão prejudicial ao Tribunal de Justiça, o órgão jurisdicional de reenvio salienta o facto de que, na data da adoção da decisão de reenvio, seis órgãos jurisdicionais de outros Estados-Membros, dos quais cinco de última instância, tinham já anulado legislações nacionais ao abrigo do acórdão Digital Rights. Por conseguinte, a resposta às questões suscitadas não é evidente, sendo no entanto necessário para esse órgão jurisdicional decidir os processos que lhe são submetidos.

59 Nestas condições, a Court of Appeal (England & Wales) (Civil Division) [Tribunal de Recurso (Inglaterra e País de Gales) (Divisão Cível)] decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) O acórdão [DRI] (incluindo, em especial, os seus n.os 60 a 62) estabelece exigências imperativas de direito da União, aplicáveis ao regime interno de um Estado-Membro que regula o acesso a dados conservados em conformidade com a legislação nacional, a fim de dar cumprimento aos artigos 7.° e 8.° da [Carta]?

2) O acórdão [DRI] alarga o âmbito de aplicação dos artigos 7.° e/ou 8.° da Carta para além do âmbito de aplicação do artigo 8.º da [CEDH], tal como definido na jurisprudência do Tribunal Europeu dos Direitos do Homem […]?»

Tramitação dos processos no Tribunal de Justiça

60 Por despacho de 1 de fevereiro de 2016, Davis e o. (C-698/15, não publicado, EU:C:2016:70), o presidente do Tribunal de Justiça decidiu deferir o pedido da Court of Appeal (England & Wales) (Civil Division) [Tribunal de Recurso (Inglaterra e País de Gales) (Divisão Cível)] de que o processo C-698/15 fosse submetido à tramitação acelerada prevista no artigo 105.º, n.º 1, do Regulamento de Processo do Tribunal de Justiça.

61 Por decisão do presidente do Tribunal de Justiça de 10 de março de 2016, os processos C-203/15 e C-698/15 foram apensos para efeitos da fase oral e do acórdão.

Quanto às questões prejudiciais

Quanto à primeira questão no processo C-203/15

62 Com a primeira questão no processo C-203/15, o Kammarrätten i Stockholm (Tribunal Administrativo de Segunda Instância de Estocolmo) pergunta, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.° e 8.°, bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional, como a que está em causa no processo principal, que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica.

63 Esta questão tem origem, nomeadamente, no facto de a Diretiva 2006/24, que a regulamentação nacional em causa no processo principal teve por objeto transpor, ter sido declarada inválida pelo acórdão Digital Rights, sendo que as partes não estão de acordo sobre o alcance deste acórdão e sobre a sua incidência nesta regulamentação, a qual rege a conservação dos dados de tráfego e dos dados de localização, bem como o acesso a esses dados pelas autoridades nacionais.

64 Importa analisar previamente se uma regulamentação nacional como a que está em causa no processo principal se enquadra no âmbito de aplicação do direito da União.

Quanto ao âmbito de aplicação da Diretiva 2002/58

65 Os Estados-Membros que apresentaram observações escritas ao Tribunal de Justiça expressaram opiniões divergentes quanto à questão de saber se e em que medida as regulamentações nacionais respeitantes à conservação dos dados de tráfego e dos dados de localização, bem como ao acesso a esses dados pelas autoridades nacionais, para efeitos de luta contra a criminalidade, se enquadram no âmbito de aplicação da Diretiva 2002/58. Com efeito, ao passo que, nomeadamente, os Governos belga, dinamarquês, alemão, estónio, da Irlanda e neerlandês expressaram a opinião de que deve ser dada uma resposta afirmativa a esta questão, o Governo checo propôs que se respondesse negativamente a esta questão, observando que estas regulamentações têm como único objetivo a luta contra a criminalidade. Quanto ao Governo do Reino Unido, alegou que só se enquadram no âmbito de aplicação desta diretiva as regulamentações respeitantes à conservação dos dados e não as respeitantes ao acesso a esses dados pelas autoridades nacionais competentes em matéria de repressão.

66 Por último, relativamente à Comissão, embora esta tenha sustentado, nas suas observações escritas apresentadas ao Tribunal de Justiça no processo C-203/15, que a regulamentação nacional em causa no processo principal se enquadra no âmbito de aplicação da Diretiva 2002/58, referiu, nas suas observações escritas no processo C-698/15, que só as normas nacionais relativas à conservação dos dados, e não as relativas ao acesso das autoridades nacionais a esses dados, se enquadram no âmbito de aplicação desta diretiva. No entanto, na sua opinião, estas últimas normas deveriam ser tomadas em consideração para avaliar se uma regulamentação nacional que rege a conservação dos dados pelos prestadores de serviços de comunicações eletrónicas constitui uma ingerência proporcionada nos direitos fundamentais garantidos nos artigos 7.° e 8.° da Carta.

67 A este respeito, há que salientar que a apreciação do alcance do âmbito de aplicação da Diretiva 2002/58 deve ter em conta, nomeadamente, a economia geral desta.

68 Nos termos do seu artigo 1.º, n.º 1, a Diretiva 2002/58 prevê, designadamente, a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas.

69 O artigo 1.º, n.º 3, desta diretiva exclui do seu âmbito de aplicação as «atividades do Estado» nos domínios aí referidos, a saber, designadamente, as atividades do Estado em matéria do direito 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 (v., por analogia, no que se refere ao artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, acórdãos de 6 de novembro de 2003, Lindqvist, C-101/01, EU:C:2003:596, n.º 43, e de 16 de dezembro de 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, EU:C:2008:727, n.º 41).

70 Quanto ao artigo 3.º da Diretiva 2002/58, este enuncia que esta diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na União, nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação (a seguir «serviços de comunicações eletrónicas»). Por conseguinte, deve considerar-se que a referida diretiva regula as atividades dos prestadores de tais serviços.

71 O artigo 15.º, n.º 1, da Diretiva 2002/58 autoriza os Estados-Membros a adotarem, desde que respeitadas as condições nele previstas, «medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.° e 6.°, nos n.ºs 1 a 4 do artigo 8.º e no artigo 9.º [desta] diretiva». O artigo 15.º, n.º 1, segundo período, da referida diretiva identifica, a título de exemplos de medidas suscetíveis de serem assim adotadas pelo Estados-Membros, medidas «prevendo que os dados sejam conservados».

72 É certo que as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 dizem respeito a atividades próprias dos Estados ou das autoridades estatais, alheias aos domínios de atividade dos particulares (v., neste sentido, acórdão de 29 de janeiro de 2008, Promusicae, C-275/06, EU:C:2008:54, n.º 51). Além disso, as finalidades a que, nos termos desta disposição, essas medidas devem responder, no caso em apreço a salvaguarda da segurança nacional, da defesa e da segurança pública, bem como a implementação da prevenção, da investigação, da deteção e da repressão de infrações penais ou de utilizações não autorizadas do sistema de comunicações eletrónicas, coincidem substancialmente com as finalidades prosseguidas pelas atividades referidas no artigo 1.º, n.º 3, desta diretiva.

73 Todavia, atendendo à economia geral da Diretiva 2002/58, os elementos salientados no número precedente do presente acórdão não permitem concluir que as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 estão excluídas do âmbito de aplicação desta diretiva, sob pena de privarem esta disposição de efeito útil. Com efeito, a referida disposição pressupõe necessariamente que as medidas nacionais aí mencionadas, como as relativas à conservação de dados para efeitos de luta

contra criminalidade, se enquadram no âmbito de aplicação desta mesma diretiva, uma vez que esta última só autoriza expressamente que os Estados-Membros as adotem desde que respeitadas as condições que prevê.

74 Além disso, as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 regulam, para os efeitos mencionados nesta disposição, a atividade dos prestadores de serviços de comunicações eletrónicas. Por conseguinte, este artigo 15.º, n.º 1, lido em conjugação com o artigo 3.º da referida diretiva, deve ser interpretado no sentido de que tais medidas legislativas estão abrangidas pelo âmbito de aplicação desta mesma diretiva.

75 Em particular, enquadra-se neste âmbito de aplicação uma medida legislativa, como a que está em causa no processo principal, que impõe a estes prestadores a conservação dos dados de tráfego e dos dados de localização, uma vez que tal atividade implica necessariamente, da parte destes, o tratamento de dados pessoais.

76 Também se enquadra no referido âmbito de aplicação uma medida legislativa que tem por objeto, como no processo principal, o acesso das autoridades nacionais aos dados conservados pelos prestadores de serviços de comunicações eletrónicas.

77 Com efeito, a proteção da confidencialidade das comunicações eletrónicas e dos dados de tráfego com elas relacionados, garantida no artigo 5.º, n.º 1, da Diretiva 2002/58, aplica-se às medidas tomadas por todas as pessoas que não sejam os utilizadores, independentemente de se tratar de pessoas singulares ou de entidades privadas ou públicas. Como confirma o considerando 21 desta diretiva, esta tem como objetivo impedir «o acesso» não autorizado às comunicações, incluindo a «quaisquer dados com elas relacionados», para proteger a confidencialidade das comunicações eletrónicas.

78 Nestas condições, uma medida legislativa através da qual um Estado-Membro impõe, com fundamento no artigo 15.º, n.º 1, da Diretiva 2002/58, aos prestadores de serviços de comunicações eletrónicas, para os efeitos mencionados nesta disposição, a obrigação de conceder às autoridades nacionais, nas condições previstas nessa medida, o acesso aos dados conservados pelos referidos prestadores tem por objeto o tratamento de dados pessoais por parte destes últimos, tratamento que se enquadra no âmbito de aplicação desta diretiva.

79 Além disso, uma vez que a conservação de dados só é feita para, sendo caso disso, tornar os dados acessíveis às autoridades nacionais competentes, uma regulamentação nacional que prevê a conservação de dados implica, em princípio, necessariamente a existência de disposições relativas ao acesso das autoridades nacionais competentes aos dados conservados pelos prestadores de serviços de comunicações eletrónicas.

80 Esta interpretação é corroborada pelo artigo 15.º, n.º 1-B, da Diretiva 2002/58, segundo o qual os prestadores estabelecem procedimentos internos para responder aos pedidos de acesso aos dados pessoais dos utilizadores com base nas disposições nacionais aprovadas nos termos do artigo 15.º, n.º 1, desta diretiva.

81 Resulta do que precede que uma regulamentação nacional, como a que está em causa nos processos principais C-203/15 e C-698/15, se enquadra no âmbito de aplicação da Diretiva 2002/58.

Quanto à interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta

82 Importa salientar que, em conformidade com o disposto no artigo 1.º, n.º 2, da Diretiva 2002/58, as suas disposições «especificam e complementam» a Diretiva 95/46. Como enuncia o seu considerando 2, a Diretiva 2002/58 visa, em especial, assegurar o pleno respeito pelos direitos consagrados nos

artigos 7.° e 8.° da Carta. A este propósito, 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 esteve na origem da Diretiva 2002/58, que o legislador da União entendeu «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».

83 Para este efeito, a Diretiva 2002/58 contém disposições específicas que visam, conforme resulta nomeadamente dos seus considerandos 6 e 7, proteger os utilizadores dos serviços de comunicações eletrónicas contra os riscos que podem afetar os dados pessoais e a privacidade que resultam das novas tecnologias e da capacidade acrescida de armazenamento e de tratamento automatizado de dados.

84 Em especial, o artigo 5.º, n.º 1, desta diretiva prevê que os Estados-Membros devem garantir, 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.

85 O princípio da confidencialidade das comunicações consagrado pela Diretiva 2002/58 implica, entre outros, conforme resulta do artigo 5.º, n.º 1, segundo período, desta, uma proibição dirigida, em princípio, a todas as pessoas que não sejam os utilizadores, de armazenar, sem o consentimento destes, os dados de tráfego correspondentes às comunicações eletrónicas. Só são objeto de derrogação as pessoas legalmente autorizadas em conformidade com o disposto no artigo 15.º, n.º 1, desta diretiva e o armazenamento técnico necessário para o encaminhamento de uma comunicação (v., neste sentido, acórdão de 29 de janeiro de 2008, Promusicae, C-275/06, EU:C:2008:54, n.º 47).

86 Assim, como confirmam os considerandos 22 e 26 da Diretiva 2002/58, o tratamento e o armazenamento dos dados de tráfego só são autorizados, nos termos do artigo 6.º desta diretiva, na medida e para o período de tempo necessários para a faturação de serviços, para a comercialização destes e para a prestação de serviços de valor acrescentado (v., neste sentido, acórdão de 29 de janeiro de 2008, Promusicae, C-275/06, EU:C:2008:54, n.ºs 47 e 48). No que respeita, em especial, à faturação dos serviços, esse tratamento só é autorizado até ao termo do prazo durante o qual a fatura pode ser legalmente contestada ou até ao termo do prazo durante o qual pode ser intentado um processo judicial para obter o pagamento. Depois de expirado esse prazo, 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.

87 O alcance das disposições dos artigos 5.° e 6.°, bem como do artigo 9.º, n.º 1, da Diretiva 2002/58, que visam garantir a confidencialidade das comunicações e dos dados correspondentes, bem como minimizar os riscos de abuso, deve, além disso, ser apreciado à luz do considerando 30 desta diretiva, nos termos do qual «[o]s 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».

88 É certo que o artigo 15.º, n.º 1, da Diretiva 2002/58 permite que os Estados-Membros introduzam exceções à obrigação de princípio, enunciada no artigo 5.º, n.º 1, desta diretiva, de garantir a confidencialidade dos dados pessoais e das obrigações correspondentes, mencionadas, nomeadamente, nos artigos 6.° e 9.° da referida diretiva (v., neste sentido, acórdão de 29 de janeiro de 2008, Promusicae, C-275/06, EU:C:2008:54, n.º 50).

89 Contudo, na medida em que permite que os Estados-Membros limitem o alcance da obrigação de princípio de garantir a confidencialidade das comunicações e dos correspondentes dados de tráfego, o artigo 15.º, n.º 1, da Diretiva 2002/58 deve ser interpretado em sentido estrito, em conformidade com

jurisprudência constante do Tribunal de Justiça (v., por analogia, acórdão de 22 de novembro de 2012, Probst, C-119/12, EU:C:2012:748, n.º 23). Por conseguinte, tal disposição não pode justificar que a exceção a essa obrigação de princípio e, em especial, a proibição de armazenar esses dados, prevista no artigo 5.º desta diretiva, se converta na regra, sob pena de esvaziar em grande medida esta última disposição do seu alcance.

90 Importa, a este respeito, salientar que o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 prevê que as medidas legislativas que refere e que derrogam o princípio da confidencialidade das comunicações e dos correspondentes dados de tráfego devem ter por objetivo «salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa [e] a segurança pública[, bem como] a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas», ou devem prosseguir um dos outros objetivos referidos no artigo 13.º, n.º 1, da Diretiva 95/46, para o qual remete o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 (v., neste sentido, acórdão de 29 de janeiro de 2008, Promusicae, C-275/06, EU:C:2008:54, n.º 53). Tal enumeração de objetivos reveste um caráter exaustivo conforme resulta do artigo 15.º, n.º 1, segundo período, desta última diretiva, nos termos do qual as medidas legislativas devem ser justificadas «pelas razões enunciadas» no artigo 15.º, n.º 1, primeiro período, da referida diretiva. Por conseguinte, os Estados-Membros não podem adotar essas medidas para fins diferentes dos enumerados nesta última disposição.

91 Além disso, o artigo 15.º, n.º 1 terceiro período, da Diretiva 2002/58 dispõe que «[t]odas as medidas referidas [no artigo 15.º, n.º 1, desta diretiva] deverão ser conformes com os princípios gerais do direito [da União], incluindo os mencionados nos n.ºs 1 e 2 do artigo 6.º [UE]», entre os quais constam os princípios gerais e os direitos fundamentais atualmente garantidos pela Carta. Assim, o artigo 15.º, n.º 1, da Diretiva 2002/58 deve ser interpretado à luz dos direitos fundamentais garantidos pela Carta (v., por analogia, no que se refere à Diretiva 95/46, acórdãos 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 68; de 13 de maio de 2014, Google Spain e Google, C-131/12, EU:C:2014:317, n.º 68; e de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 38).

92 A este respeito, importa sublinhar que a obrigação imposta aos prestadores de serviços de comunicações eletrónicas, por uma regulamentação nacional como a que está em causa no processo principal, de conservar os dados de tráfego para, se for caso disso, os disponibilizar às autoridades nacionais competentes levanta questões relativas ao respeito não apenas dos artigos 7.º e 8.º da Carta, que são explicitamente mencionados nas questões prejudiciais, mas também da liberdade de expressão garantida no artigo 11.º da Carta (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.ºs 25 e 70).

93 Assim, a importância tanto do direito ao respeito da vida privada, garantido no artigo 7.º da Carta, como do direito à proteção dos dados pessoais, garantido no artigo 8.º desta, conforme resulta da jurisprudência do Tribunal de Justiça (v., neste sentido, acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 39 e jurisprudência referida), deve ser tomada em conta aquando da interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58. O mesmo sucede com o direito à liberdade de expressão atendendo à especial importância que esta liberdade reveste em qualquer sociedade democrática. Este direito fundamental, garantido pelo artigo 11.º da Carta, 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 12 de junho de 2003, Schmidberger, C-112/00, EU:C:2003:333, n.º 79, e de 6 de setembro de 2011, Patriciello, C-163/10, EU:C:2011:543, n.º 31).

94 A este propósito, importa recordar que, em conformidade com o disposto no artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades por ela reconhecidos deve estar prevista por lei e respeitar o seu conteúdo essencial. Na observância do princípio da proporcionalidade, só podem ser introduzidas restrições ao exercício desses direitos e dessas

liberdades se forem necessárias e corresponderem, efetivamente, a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros (acórdão de 15 de fevereiro de 2016, N., C-601/15 PPU, EU:C:2016:84, n.º 50).

95 Quanto a este último aspeto, o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 prevê que os Estados-Membros podem adotar uma medida que derrogue o princípio da confidencialidade das comunicações e dos correspondentes dados de tráfego quando for «necessária, adequada e proporcionada numa sociedade democrática», à luz dos objetivos que esta disposição enuncia. Quanto ao considerando 11 desta diretiva, esclarece que uma medida desta natureza deve ser «rigorosamente» proporcionada ao objetivo a alcançar. No que se refere, em especial, à conservação dos dados, o artigo 15.º, n.º 1, segundo período, da referida diretiva exige que essa conservação só tenha lugar «durante um período limitado» e «pelas razões enunciadas» no artigo 15.º, n.º 1, primeiro período, desta mesma diretiva.

96 O respeito pelo princípio da proporcionalidade também decorre da jurisprudência constante do Tribunal de Justiça segundo a qual a proteção do direito fundamental ao respeito da vida privada a nível da União exige que as derrogações e as limitações à proteção dos dados pessoais operem na estrita medida do necessário (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.º 77; Digital Rights, n.º 52; e de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 92).

97 Quanto à questão de saber se uma regulamentação nacional, como a que está em causa no processo C-203/15, cumpre essas condições, importa salientar que esta prevê uma conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização de todos os assinantes e utilizadores registados relativos a todos os meios de comunicação eletrónica, e que obriga os prestadores de serviços de comunicações eletrónicas a conservarem esses dados de forma sistemática, contínua e sem nenhuma exceção. Conforme resulta da decisão de reenvio, as categorias de dados visadas por esta regulamentação correspondem, em substância, àquelas cuja conservação estava prevista na Diretiva 2006/24.

98 Assim, os dados que os prestadores de serviços de comunicações eletrónicas devem conservar permitem encontrar e identificar a origem de uma comunicação e o seu destino, determinar a data, a hora, a duração e o tipo de uma comunicação, o equipamento de comunicação dos utilizadores, bem como localizar o equipamento de comunicação móvel. De entre estes dados constam, designadamente, o nome e o endereço do assinante ou do utilizador registado, o número de telefone do chamador e o número chamado bem como, em relação aos serviços de Internet, um endereço IP. Estes dados permitem, designadamente, saber quem é a pessoa com a qual um assinante ou um utilizador registado comunicou e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Além disso, permitem saber com que frequência o assinante ou o utilizador registado comunicam com certas pessoas durante um determinado período (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 26).

99 Considerados no seu todo, estes dados são suscetíveis de 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 (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 27). Em especial, estes dados fornecem os meios para determinar, conforme salientou o advogado-geral nos n.ºs 253, 254 e 257 a 259 das suas conclusões, o perfil das pessoas em causa, informação tão sensível, à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações.

100 A ingerência que tal regulamentação comporta nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta é muito ampla e deve ser considerada particularmente grave. O facto de a conservação dos dados ser efetuada sem que os utilizadores dos serviços de comunicações eletrónicas disso sejam informados é suscetível de gerar no espírito das pessoas em causa a sensação de que a sua vida privada é objeto de constante vigilância (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 37).

101 Ainda que tal regulamentação não autorize a conservação do conteúdo de uma comunicação e, por conseguinte, não seja suscetível de violar o conteúdo essencial dos referidos direitos (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 39), a conservação dos dados de tráfego e dos dados de localização pode, todavia, ter um impacto na utilização dos meios de comunicação eletrónica e, consequentemente, no exercício, pelos utilizadores desses meios, da sua liberdade de expressão, garantida pelo artigo 11.º da Carta (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 28).

102 Atendendo à gravidade da ingerência nos direitos fundamentais em causa que constitui uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, a conservação de dados de tráfego e de dados de localização, só a luta contra a criminalidade grave pode justificar uma medida deste tipo (v., por analogia, a propósito da Diretiva 2006/24, acórdão Digital Rights, n.º 60).

103 Além disso, embora a eficácia da luta contra a criminalidade grave, nomeadamente contra a criminalidade organizada e o terrorismo, possa depender em larga medida da utilização de técnicas modernas de investigação, um objetivo de interesse geral desse tipo, por muito fundamental que seja, não pode por si só justificar que uma regulamentação nacional que prevê a conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização seja considerada necessária para efeitos da referida luta (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 51).

104 A este respeito, importa salientar, por um lado, que uma regulamentação deste tipo tem por efeito, atendendo às características descritas no n.º 97 do presente acórdão, que a conservação dos dados de tráfego e dos dados de localização constitui a regra, ao passo que o sistema implementado pela Diretiva 2002/58 exige que essa conservação dos dados seja a exceção.

105 Por outro lado, uma regulamentação nacional como a que está em causa no processo principal, que abrange de forma generalizada todos os assinantes e utilizadores registados e que visa todos os meios de comunicação eletrónica, bem como todos os dados de tráfego, não prevê nenhuma diferenciação, limitação ou exceção em função do objetivo prosseguido. Essa regulamentação 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 infrações penais graves. Além disso, não prevê nenhuma exceção, pelo que também é aplicável a pessoas cujas comunicações estão sujeitas ao segredo profissional, segundo as regras do direito nacional (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.ºs 57 e 58).

106 Uma regulamentação deste tipo não exige nenhuma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a segurança pública. Nomeadamente, 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 uma maneira ou de outra numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus dados, podiam contribuir para a luta contra a criminalidade (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 59).

107 Por conseguinte, uma regulamentação nacional como a que está em causa no processo principal 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.°, 8.° e 11.°, bem como do artigo 52.º, n.º 1, da Carta.

108 Em contrapartida, o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 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 de luta contra a criminalidade grave, desde que a conservação dos dados seja limitada ao estritamente necessário, no que se refere às categorias de dados a conservar, aos equipamentos de comunicação visados, às pessoas em causa e à duração de conservação fixada.

109 Para cumprir os requisitos enunciados no número anterior do presente acórdão, esta regulamentação nacional deve, em primeiro lugar, prever normas claras e precisas que regulem o âmbito e a aplicação dessa medida de conservação dos dados e que imponham exigências mínimas, de modo a que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. Deve, em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida de conservação dos dados, a título preventivo, garantindo assim que essa medida se limita ao estritamente necessário (v., por analogia, a propósito da Diretiva 2006/24, acórdão Digital Rights, n.º 54 e jurisprudência referida).

110 Em segundo lugar, relativamente às condições materiais que uma regulamentação nacional deve satisfazer que permitam, no âmbito da luta contra a criminalidade, a conservação, a título preventivo, dos dados de tráfego e dos dados de localização, para garantir que se limita ao estritamente necessário, há que salientar que, embora essas condições possam variar em função das medidas adotadas para efeitos da prevenção, da investigação, da deteção e da repressão da criminalidade grave, a conservação dos dados deve sempre responder, em todo o caso, a critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido. Em especial, tais condições devem revelar-se, na prática, suscetíveis de limitar efetivamente o alcance da medida e, consequentemente, o público afetado.

111 No que se refere à delimitação de uma medida deste tipo quanto ao público e às situações potencialmente abrangidas, a regulamentação nacional deve basear-se em elementos objetivos que permitam visar um público cujos dados sejam 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. Tal delimitação pode ser assegurada através de um critério geográfico quando as autoridades nacionais competentes considerem, com base em elementos objetivos, que existe um risco elevado de preparação ou de execução desses atos, numa ou em mais zonas geográficas.

112 Atendendo a todas as considerações que precedem, importa responder à primeira questão no processo C-203/15 que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica.

Quanto à segunda questão no processo C-203/15 e à primeira questão no processo C-698/15

113 Importa salientar a título preliminar que o Kammarrätten i Stockholm (Tribunal Administrativo de Segunda Instância de Estocolmo) só suscitou a segunda questão no processo C-203/15 para o caso de vir a ser dada uma resposta negativa à primeira questão no referido processo. Todavia, esta segunda questão é independente do caráter generalizado ou circunscrito de uma conservação de dados, no

sentido referido nos n.os 108 a 111 do presente acórdão. Por conseguinte, importa responder de forma conjunta à segunda questão no processo C-203/15 e à primeira questão no processo C-698/15, a qual é apresentada independentemente do âmbito da obrigação de conservação de dados imposta aos prestadores de serviços de comunicações eletrónicas.

114 Com a segunda questão no processo C-203/15 e com a primeira questão no processo C-698/15, os órgãos jurisdicionais de reenvio perguntam, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º e 8.º, bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial o acesso das autoridades nacionais competentes aos dados conservados, sem limitar esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por um órgão jurisdicional ou por uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados no território da União.

115 No que se refere aos objetivos suscetíveis de justificar uma regulamentação nacional que derrogue o princípio da confidencialidade das comunicações eletrónicas, há que recordar que, na medida em que, como se constatou nos n.os 90 e 102 do presente acórdão, a enumeração dos objetivos que figuram no artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 reveste um caráter exaustivo, o acesso aos dados conservados deve responder efetiva e estritamente a um desses objetivos. Além disso, dado que o objetivo prosseguido por esta regulamentação deve estar relacionado com a gravidade da ingerência nos direitos fundamentais que esse acesso gera, daqui decorre que, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, só a luta contra a criminalidade grave pode justificar um acesso dessa natureza aos dados conservados.

116 No que se refere ao respeito pelo princípio da proporcionalidade, uma regulamentação nacional que estipule as condições em que os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes o acesso aos dados conservados deve assegurar, em conformidade com o que foi constatado nos n.os 95 e 96 do presente acórdão, que esse acesso ocorra apenas dentro dos limites do estritamente necessário.

117 Além disso, uma vez que as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 devem, em conformidade com o considerando 11 desta diretiva, «estar sujeitas […] a salvaguardas adequadas», uma medida deste tipo deve, conforme resulta da jurisprudência referida no n.º 109 do presente acórdão, prever normas claras e precisas que indiquem em que circunstâncias e em que condições os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes acesso aos dados. Do mesmo modo, uma medida desta natureza deve também ser vinculativa em direito interno.

118 Para garantir que o acesso das autoridades nacionais competentes aos dados conservados seja limitado ao estritamente necessário, é certo que compete ao direito nacional determinar as condições em que os fornecedores de serviços de comunicações eletrónicas devem conceder esse acesso. Todavia, a regulamentação nacional em causa não se pode limitar a exigir que o acesso responda a um dos objetivos referidos no artigo 15.º, n.º 1, da Diretiva 2002/58, ainda que esteja em causa a luta contra a criminalidade grave. Com efeito, tal regulamentação nacional deve também prever as condições materiais e processuais que regulam o acesso das autoridades nacionais competentes aos dados conservados (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 61).

119 Assim, e uma vez que um acesso generalizado a todos os dados conservados, independentemente de uma qualquer relação, no mínimo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário, a regulamentação nacional em causa deve basear-se em critérios objetivos para definir as circunstâncias e as condições nas quais deve ser concedido às autoridades nacionais competentes o acesso aos dados dos assinantes ou dos utilizadores registados. A este respeito, só poderá, em princípio, ser concedido acesso, em relação com o objetivo da luta contra a

criminalidade, aos dados de pessoas suspeitas de terem planeado, de estarem a cometer ou de terem cometido uma infração grave ou ainda de estarem envolvidas de uma maneira ou de outra numa infração deste tipo (v., por analogia, TEDH, 4 de dezembro de 2015, Zakharov c. Rússia, CE:ECHR:2015:1204JUD004714306, § 260). Todavia, em situações específicas, como aquelas em que os interesses vitais da segurança nacional, da defesa ou da segurança pública estejam ameaçados por atividades terroristas, pode também ser concedido acesso aos dados de outras pessoas quando existam elementos objetivos que permitam considerar que esses dados podem, num caso concreto, trazer uma contribuição efetiva para a luta contra essas atividades.

120 Para garantir, na prática, o pleno cumprimento destas condições, é essencial que o acesso das autoridades nacionais competentes aos dados conservados seja, em princípio, salvo em casos de urgência devidamente justificados, sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente, e que a decisão desse órgão jurisdicional ou dessa entidade ocorra na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.º 62; v. também, por analogia, no que se refere ao artigo 8.º da CEDH, TEDH, 12 de janeiro de 2016, Szabó e Vissy c. Hungria, CE:ECHR:2016:0112JUD003713814, §§ 77 e 80).

121 Do mesmo modo, importa que as autoridades nacionais competentes às quais foi concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível comprometer as investigações levadas a cabo por essas autoridades. Com efeito, essa informação é, de facto, necessária para permitir que essas pessoas exerçam, nomeadamente, o direito de recurso, explicitamente previsto no artigo 15.º, n.º 2, da Diretiva 2002/58, lido em conjugação com o artigo 22.º da Diretiva 95/46, em caso de violação dos seus direitos (v., por analogia, acórdãos de 7 de maio de 2009, Rijkeboer, C-553/07, EU:C:2009:293, n.º 52, e de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 95).

122 No que se refere às regras relativas à segurança e à proteção dos dados conservados pelos prestadores de serviços de comunicações eletrónicas, há que constatar que o artigo 15.º, n.º 1, da Diretiva 2002/58 não permite que os Estados-Membros estabeleçam exceções ao seu artigo 4.º, n.º 1, nem ao seu artigo 4.º, n.º 1-A. Estas últimas disposições exigem que esses prestadores de serviços adotem medidas de ordem técnica e de organização adequadas para garantir uma proteção eficaz dos dados conservados contra os riscos de abuso e contra qualquer acesso ilícito a esses dados. Tendo em conta a quantidade de dados conservados, o caráter sensível desses dados bem como o risco de acesso ilícito aos mesmos, os prestadores de serviços de comunicações eletrónicas devem, para assegurar a plena integridade e a confidencialidade dos referidos dados, garantir um nível particularmente elevado de proteção e de segurança através de medidas técnicas e de organização adequadas. Em especial, a regulamentação nacional deve prever a conservação no território da União bem como a destruição definitiva dos dados no termo do respetivo período de conservação (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.ºs 66 a 68).

123 Seja como for, os Estados-Membros devem garantir o controlo, por parte de uma autoridade independente, do respeito do nível de proteção garantido pelo direito da União em matéria de proteção das pessoas singulares relativamente ao tratamento dos dados pessoais, sendo esse controlo explicitamente exigido pelo artigo 8.º, n.º 3, da Carta e constituindo, em conformidade com jurisprudência constante do Tribunal de Justiça, um elemento essencial do respeito da proteção das pessoas relativamente ao tratamento dos dados pessoais. Se assim não fosse, as pessoas cujos dados pessoais estivessem conservados ficariam privadas do direito, garantido pelo artigo 8.º, n.ºs 1 e 3, da Carta, de apresentar pedidos às autoridades nacionais de controlo para efeitos da proteção dos seus dados (v., neste sentido, acórdão Digital Rights, n.º 68, e de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.ºs 41 e 58).

124 Cabe aos órgãos jurisdicionais de reenvio verificar se e em que medida as regulamentações nacionais em causa nos processos principais respeitam as exigências que decorrem do artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta, conforme explicitadas no n.ºs 115 a 123 do presente acórdão, no que se refere tanto ao acesso das autoridades nacionais competentes aos dados conservados como à proteção e ao nível de segurança desses dados.

125 Atendendo a todas as considerações que precedem, há que responder à segunda questão no processo C-203/15 e à primeira questão no processo C-698/15 que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União.

Quanto à segunda questão no processo C-698/15

126 Com a segunda questão no processo 698/15, a Court of Appeal (England & Wales) (Civil Division) [Tribunal de Recurso (Inglaterra e País de Gales) (Divisão Cível)] pergunta em substância se, no acórdão Digital Rights, o Tribunal de Justiça interpretou os artigos 7.º e/ou 8.º da Carta num sentido mais amplo do que aquele que é atribuído pelo Tribunal Europeu dos Direitos do Homem ao artigo 8.º da CEDH.

127 A título preliminar, há que recordar que, embora, como é confirmado pelo artigo 6.º, n.º 3, TUE, os direitos fundamentais reconhecidos pela CEDH façam parte do direito da União enquanto princípios gerais, a referida Convenção não constitui, enquanto a União a ela não aderir, um instrumento jurídico formalmente integrado na ordem jurídica da União (v., neste sentido, acórdão de 15 de fevereiro de 2016, N., C-601/15 PPU, EU:C:2016:84, n.º 45 e jurisprudência referida).

128 Assim, a interpretação da Diretiva 2002/58, em causa no caso em apreço, deve ser realizada à luz unicamente dos direitos fundamentais garantidos pela Carta (v., neste sentido, acórdão de 15 de fevereiro de 2016, N., C-601/15 PPU, EU:C:2016:84, n.º 46 e jurisprudência referida).

129 Além disso, há que recordar que as anotações relativas ao artigo 52.º da Carta indicam que o artigo 52.º, n.º 3, desta visa garantir a coerência necessária entre a Carta e a CEDH, «sem que tal atente contra a autonomia do direito da União e do Tribunal de Justiça da União Europeia» (acórdão de 15 de fevereiro de 2016, N., C-601/15 PPU, EU:C:2016:84, n.º 47). Em especial, como expressamente previsto no artigo 52.º, n.º 3, segundo período, da Carta, o artigo 52.º, n.º 3, primeiro período, desta não obsta a que o direito da União conceda uma proteção mais alargada do que a CEDH. A isto acresce, por último, o facto de o artigo 8.º da Carta dizer respeito a um direito fundamental diferente do consagrado no artigo 7.º desta e de não ter equivalente na CEDH.

130 Ora, segundo jurisprudência constante do Tribunal de Justiça, a justificação de um pedido de decisão prejudicial não consiste na formulação de opiniões consultivas sobre questões gerais ou hipotéticas, mas na necessidade inerente à solução efetiva de um litígio que diga respeito ao direito da União (v., neste sentido, acórdãos de 24 de abril de 2012, Kamberaj, C-571/10, EU:C:2012:233, n.º 41; de 26 de fevereiro de 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, n.º 42; e de 27 de fevereiro de 2014, Pohotovosť, C-470/12, EU:C:2014:101, n.º 29).

131 No caso em apreço, atendendo às considerações que figuram, nomeadamente, nos n.os 128 e 129 do presente acórdão, a questão de saber se a proteção conferida aos artigos 7.° e 8.° da Carta é mais ampla do que a garantida no artigo 8.º da CEDH não é suscetível de influenciar a interpretação da Diretiva 2002/58, lida à luz da Carta, que está em causa no litígio principal no processo C-698/15.

132 Assim, não parece que uma resposta à segunda questão no processo C-698/15 possa trazer elementos de interpretação do direito da União que sejam necessários para a solução, à luz deste direito, do referido litígio.

133 Daqui resulta que a segunda questão no processo C-698/15 é inadmissível.

Quanto às despesas

134 Revestindo os processos, quanto às partes nas causas principais, a natureza de incidentes suscitados 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 eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica.**

2) **O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.°, 8.° e 11.° bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União.**

3) **A segunda questão submetida pela Court of Appeal (England & Wales) (Civil Division) [Tribunal de Recurso (Inglaterra e País de Gales) (Divisão Cível), Reino Unido] é inadmissível.**

Assinaturas