



Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

8 de abril de 2014 *

«Comunicações eletrónicas — Diretiva 2006/24/CE — Serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações — Conservação de dados gerados ou tratados no contexto da oferta desses serviços — Validade — Artigos 7.º, 8.º e 11.º da Carta dos Direitos Fundamentais da União Europeia»

Nos processos apensos C-293/12 e C-594/12,

que têm por objeto pedidos de decisão prejudicial apresentados, nos termos do artigo 267.º TFUE, pela High Court (Irlanda) e pelo Verfassungsgerichtshof (Áustria), por decisões, respetivamente, de 27 de janeiro e 28 de novembro de 2012, que deram entrada no Tribunal de Justiça em 11 de junho e 19 de dezembro de 2012, nos processos

Digital Rights Ireland Ltd (C-293/12)

contra

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Síochána,

Irlanda,

The Attorney General,

sendo intervenientes:

Irish Human Rights Commission,

e

Kärntner Landesregierung (C-594/12),

Michael Seitlinger,

Christof Tschohl e o.,

* Línguas de processo: inglês e alemão.

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: V. Skouris, presidente, K. Lenaerts, vice-presidente, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (relator), E. Juhász, A. Borg Barthet, C. G. Fernlund e J. L. da Cruz Vilaça, presidentes de secção, A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, C. Toader e C. Vajda, juízes,

advogado-geral: P. Cruz Villalón,

secretário: K. Malacek, administrador,

vistos os autos e após a audiência de 9 de julho de 2013,

vistas as observações apresentadas:

- em representação da Digital Rights Ireland Ltd, por F. Callanan, SC, e F. Crehan, BL, mandatados por S. McGarr, solicitor,
- em representação de M. Seitlinger, por G. Otto, Rechtsanwalt,
- em representação de C. Tschohl e o., por E. Scheucher, Rechtsanwalt,
- em representação da Irish Human Rights Commission, por P. Dillon Malone, BL, mandatado por S. Lucey, solicitor,
- em representação da Irlanda, por E. Creedon e D. McGuinness, na qualidade de agentes, assistidos por E. Regan, SC, e D. Fennelly, JC,
- em representação do Governo austríaco, por G. Hesse e G. Kunnert, na qualidade de agentes,
- em representação do Governo espanhol, por N. Díaz Abad, na qualidade de agente,
- em representação do Governo francês, por G. de Bergues, D. Colas e B. Beaupère-Manokha, na qualidade de agentes,
- em representação do Governo italiano, por G. Palmieri, na qualidade de agente, assistida por A. De Stefano, avvocato dello Stato,
- em representação do Governo polaco, por B. Majczyna e M. Szpunar, na qualidade de agentes,
- em representação do Governo português, por L. Inez Fernandes e C. Vieira Guerra, na qualidade de agentes,
- em representação do Governo do Reino Unido, por L. Christie, na qualidade de agente, assistido por S. Lee, barrister,
- em representação do Parlamento Europeu, por U. Rösslein, A. Caiola e K. Zejdová, na qualidade de agentes,
- em representação do Conselho da União Europeia, por J. Monteiro, E. Sitbon e I. Šulce, na qualidade de agentes,
- em representação da Comissão Europeia, por D. Maidani, B. Martenczuk e M. Wilderspin, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 12 de dezembro de 2013,
profere o presente

Acórdão

- 1 Os pedidos de decisão prejudicial têm por objeto a validade 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 L 105, p. 54).
- 2 O pedido apresentado pela High Court (processo C-293/12) é relativo a um litígio que opõe a Digital Rights Ireland Ltd (a seguir «Digital Rights») ao Minister for Communications, Marine and Natural Resources, ao Minister for Justice, Equality and Law Reform, ao Commissioner of the Garda Síochána, à Irlanda e ao Attorney General, acerca da legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas.
- 3 O pedido apresentado pelo Verfassungsgerichtshof (processo C-594/12) é relativo a recursos em matéria constitucional interpostos perante esse órgão jurisdicional, respetivamente, pelo Kärntner Landesregierung (Governo do *Land* da Caríntia), bem como por M. Seitlinger, C. Tschohl e 11 128 outros recorrentes, acerca da compatibilidade da lei que transpõe a Diretiva 2006/24 para o direito interno austríaco com a lei constitucional federal (Bundes-Verfassungsgesetz).

Quadro jurídico

Diretiva 95/46/CE

- 4 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 L 281, p. 31), tem por objeto, nos termos do seu artigo 1.º, n.º 1, assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do seu direito à vida privada, no que diz respeito ao tratamento de dados pessoais.
- 5 Quanto à segurança do tratamento de tais dados, o artigo 17.º, n.º 1, da mesma diretiva dispõe:

«Os Estados-Membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição accidental ou ilícita, a perda accidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito.

Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.»

Diretiva 2002/58/CE

- 6 A 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 L 201, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO L 337, p. 11, a seguir «Diretiva 2002/58»), tem por objeto, de acordo com o seu artigo 1.º, n.º 1, a

harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na União Europeia. Nos termos do n.º 2 do mesmo artigo, as disposições desta diretiva especificam e complementam a Diretiva 95/46 para os efeitos enunciados no n.º 1.

7 No que respeita à segurança do tratamento de dados, o artigo 4.º da Diretiva 2002/58 prevê:

«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/CE, 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.

As autoridades nacionais competentes devem ter competência para auditar as medidas tomadas por prestadores de serviços de comunicações eletrónicas acessíveis ao público e para emitir recomendações sobre melhores práticas relativas ao nível de segurança que estas medidas devem alcançar.

2. Em caso de risco especial de violação da segurança da rede, o prestador de um serviço de comunicações eletrónicas publicamente disponível informará os assinantes desse risco e, sempre que o risco se situe fora do âmbito das medidas a tomar pelo prestador do serviço, das soluções possíveis, incluindo uma indicação dos custos prováveis daí decorrentes.»

8 Quanto à confidencialidade das comunicações e dos dados de tráfego, o artigo 5.º, n.ºs 1 e 3, da referida diretiva dispõe:

«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, em conformidade 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/CE, 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 Nos termos do artigo 6.º, n.º 1, da Diretiva 2002/58:

«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.»

10 O artigo 15.º da Diretiva 2002/58 enuncia, no seu n.º 1:

«Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva, sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva 95/46/CE. 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.»

Diretiva 2006/24

11 Depois de ter efetuado uma consulta aos representantes dos serviços de controlo, do setor das comunicações eletrónicas e dos peritos em matéria de proteção de dados, a Comissão apresentou, em 21 de setembro de 2005, uma avaliação de impacto das opções políticas relativas a regras respeitantes à conservação dos dados de tráfego (a seguir «avaliação de impacto»). Esta avaliação serviu de base à elaboração da proposta de Diretiva do Parlamento Europeu e do Conselho relativa à conservação de dados tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis e que altera a Diretiva 2002/58/CE [COM(2005) 438 final, a seguir «proposta de diretiva»], apresentada na mesma data, que conduziu à adoção da Diretiva 2006/24 ao abrigo do artigo 95.º CE.

12 O considerando 4 da Diretiva 2006/24 enuncia:

«O n.º 1 do artigo 15.º da Diretiva 2002/58/CE enumera as condições em que os Estados-Membros podem restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1, 2, 3 e 4 do artigo 8.º e no artigo 9.º da supracitada diretiva. Qualquer restrição deste tipo deve constituir uma medida necessária, adequada e proporcionada numa sociedade democrática, por razões específicas de ordem pública, ou seja, 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.»

13 De acordo com a primeira frase do considerando 5 da Diretiva 2006/24, «[v]ários Estados-Membros aprovaram legislação relativa à conservação de dados pelos fornecedores de serviços tendo em vista a prevenção, investigação, deteção e repressão de infrações penais».

14 Os considerandos 7 a 11 da Diretiva 2006/24 têm a seguinte redação:

«(7) Nas suas conclusões, o Conselho ‘Justiça e Assuntos Internos’ de 19 de dezembro de 2002 assinalou que, devido a um notável crescimento das possibilidades oferecidas pelas comunicações eletrónicas, os dados gerados pela utilização deste tipo de comunicações constituem um instrumento extremamente importante e útil na prevenção, investigação, deteção e de repressão de infrações penais, em especial contra a criminalidade organizada.

(8) Na sua Declaração de 25 de março de 2004 sobre a luta contra o terrorismo, o Conselho Europeu encarregou o Conselho de proceder à análise de propostas relativas ao estabelecimento de regras sobre a conservação de dados de tráfego das comunicações pelos prestadores de serviços.

(9) Nos termos do artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH) [assinada em Roma, em 4 de novembro de 1950], qualquer pessoa tem direito ao respeito da sua vida privada e da sua correspondência. As autoridades públicas só podem interferir no exercício deste direito nos termos previstos na lei e, quando essa ingerência for necessária, numa sociedade democrática, designadamente, para a segurança nacional ou para a segurança pública, a defesa da ordem e a prevenção das infrações penais, ou a proteção dos direitos e das liberdades de terceiros. Visto que a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários Estados-Membros, nomeadamente em matérias tão graves como o crime organizado e o terrorismo, é necessário assegurar que as autoridades responsáveis pela aplicação da lei possam dispor dos dados conservados por um período determinado, nas condições previstas na presente diretiva. [...]

(10) Em 13 de julho de 2005, na sua Declaração condenando os ataques terroristas em Londres, o Conselho reafirmou a necessidade de aprovar o mais rapidamente possível medidas comuns relativas à conservação de dados de telecomunicações.

(11) Tendo em consideração a importância dos dados de tráfego e dos dados de localização para a investigação, deteção e repressão de infrações penais, é necessário, como os trabalhos de investigação e a experiência prática em vários Estados-Membros o demonstram, garantir a nível europeu a conservação durante um determinado período dos dados gerados ou tratados, no contexto da oferta de comunicações, pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações, nas condições previstas na presente diretiva.»

15 Os considerandos 16, 21 e 22 da referida diretiva especificam:

«(16) As obrigações que incumbem aos fornecedores de serviços, por força do artigo 6.º da Diretiva 95/46/CE, relativamente a medidas destinadas a assegurar a qualidade dos dados, e as obrigações dos mesmos de tomarem medidas para salvaguardar a confidencialidade e a segurança do tratamento de dados por força dos artigos 16.º e 17.º da referida diretiva, são plenamente aplicáveis aos dados conservados em conformidade com a presente diretiva.

[...]

(21) Atendendo a que os objetivos da presente diretiva, ou seja, a harmonização das obrigações que incumbem aos fornecedores de conservarem determinados dados e assegurarem que estes sejam disponibilizados para efeitos de investigação, deteção e repressão de crimes graves tal como definidos no direito nacional de cada Estado-Membro, não podem ser suficientemente realizados

pelos Estados-Membros e podem, pois, devido à dimensão e aos efeitos da presente diretiva, ser melhor alcançados a nível comunitário, a Comunidade pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir aqueles objetivos.

(22) A presente diretiva respeita os direitos fundamentais e os princípios consagrados nomeadamente na Carta dos Direitos Fundamentais da União Europeia. Em especial, a presente diretiva, conjugada com a Diretiva 2002/58/CE, visa assegurar que sejam plenamente respeitados os direitos fundamentais dos cidadãos em matéria de respeito pela privacidade e pelas comunicações e de proteção dos dados pessoais, consagrados nos artigos 7.º e 8.º da Carta.»

16 A Diretiva 2006/24 consagra a obrigação de os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações conservarem determinados dados por eles gerados ou tratados. A este respeito, os artigos 1.º a 9.º, 11.º e 13.º desta diretiva dispõem:

«Artigo 1.º

Objeto e âmbito de aplicação

1. A presente diretiva visa harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro.

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.

Artigo 2.º

Definições

1. Para efeitos da presente diretiva, são aplicáveis as definições constantes da Diretiva 95/46/CE, 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) [...], e da Diretiva 2002/58/CE.

2. Para efeitos da presente diretiva, entende-se por:

- a) ‘Dados’, os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador;
- b) ‘Utilizador’, qualquer pessoa singular ou coletiva que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

- c) ‘Serviço telefónico’, os serviços de chamada (incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados), os serviços suplementares (incluindo o reencaminhamento e a transferência de chamadas) e os serviços de mensagens e multimédia [incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhorados (EMS) e os serviços multimédia (MMS)];
- d) ‘Código de identificação de utilizador’ (*‘user ID’*), um código único atribuído às pessoas, quando estas se tornam assinantes ou se inscrevem num serviço de acesso à internet, ou num serviço de comunicação pela internet;
- e) ‘Identificador da célula’ (*‘cell ID’*), a identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;
- f) ‘Chamada telefónica falhada’, uma comunicação em que a ligação telefónica foi estabelecida, mas que não obteve resposta, ou em que houve uma intervenção do gestor da rede.

Artigo 3.º

Obrigações de conservação de dados

1. Em derrogação aos artigos 5.º, 6.º e 9.º da Diretiva 2002/58/CE, 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 impostos 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.

Artigo 4.º

Acesso aos dados

Os Estados-Membros devem tomar medidas para assegurar que os dados conservados em conformidade com a presente diretiva só sejam transmitidos às autoridades nacionais competentes em casos específicos e de acordo com a legislação nacional. Os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade devem ser definidos por cada Estado-Membro no respetivo direito nacional, sob reserva das disposições pertinentes do Direito da União Europeia ou do Direito Internacional Público, nomeadamente a CEDH, na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem.

Artigo 5.º

Categorias de dados a conservar

1. Os Estados-Membros devem assegurar a conservação das categorias de dados seguintes em aplicação da presente diretiva:

- a) Dados necessários para encontrar e identificar a fonte de uma comunicação:
 - 1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel:
 - i) o número de telefone de origem,
 - ii) o nome e endereço do assinante ou do utilizador registado;
 - 2) no que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:
 - i) o(s) código(s) de identificação atribuído(s) ao utilizador,
 - ii) o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública,
 - iii) o nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador, ou o número de telefone estavam atribuídos no momento da comunicação;
- b) Dados necessários para encontrar e identificar o destino de uma comunicação:
 - 1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel:
 - i) o(s) número(s) marcado(s) (o número ou números de telefone de destino) e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada,
 - ii) o nome e o endereço do assinante, ou do utilizador registado;
 - 2) no que diz respeito ao correio eletrónico através da internet e às comunicações telefónicas através da internet:
 - i) o código de identificação de utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da internet,
 - ii) o(s) nome(s) e o(s) endereço(s) do(s) subscritor(es), ou do(s) utilizador(es) registado(s), e o código de identificação de utilizador do destinatário pretendido da comunicação;
- c) Dados necessários para identificar a data, a hora e a duração de uma comunicação:
 - 1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

- 2) no que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:
 - i) a data e a hora do início (log-in) e do fim (log-off) da ligação ao serviço de acesso à internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado,
 - ii) a data e a hora do início e do fim da ligação ao serviço de correio eletrónico através da internet ou de comunicações telefónicas através da internet, com base em determinado fuso horário;
- d) Dados necessários para identificar o tipo de comunicação:
 - 1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel: o serviço telefónico utilizado;
 - 2) no que diz respeito ao correio eletrónico através da internet e às comunicações telefónicas através da internet: o serviço internet utilizado;
- e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento:
 - 1) no que diz respeito às comunicações telefónicas na rede fixa os números de telefone de origem e de destino;
 - 2) no que diz respeito às comunicações telefónicas na rede móvel:
 - i) os números de telefone de origem e de destino,
 - ii) a Identidade Internacional de Assinante Móvel (*'International Mobile Subscriber Identity'*, ou IMSI) de quem telefona,
 - iii) a Identidade Internacional do Equipamento Móvel (*'International Mobile Equipment Identity'*, ou IMEI) de quem telefona,
 - iv) a IMSI do destinatário do telefonema,
 - v) a IMEI do destinatário do telefonema,
 - vi) no caso dos serviços pré-pagos de carácter anónimo, a data e a hora da ativação inicial do serviço e o identificador da célula a partir da qual o serviço foi ativado;
 - 3) no que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:
 - i) o número de telefone que solicita o acesso por linha telefónica;
 - ii) a linha de assinante digital (*'digital subscriber line'*, ou DSL), ou qualquer outro identificador terminal do autor da comunicação;

- f) Dados necessários para identificar a localização do equipamento de comunicação móvel:
- 1) o identificador da célula no início da comunicação;
 - 2) os dados que identifiquem a situação geográfica das células, tomando como referência os respetivos identificadores de célula durante o período em que se procede à conservação de dados.
2. Nos termos da presente diretiva, não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações.

Artigo 6.º

Períodos de conservação

Os Estados-Membros devem assegurar que as categorias de dados referidos no artigo 5.º sejam conservadas por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação.

Artigo 7.º

Proteção e segurança de dados

Sem prejuízo das disposições adotadas nos termos da Diretiva 95/46/CE e da Diretiva 2002/58/CE, cada Estado-Membro deve assegurar que os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações respeitem, no mínimo, os seguintes princípios em matéria de segurança de dados no que se refere aos dados conservados em conformidade com a presente diretiva:

- a) Os dados conservados devem ser da mesma qualidade e estar sujeitos à mesma proteção e segurança que os dados na rede;
- b) Os dados devem ser objeto de medidas técnicas e organizativas adequadas que os protejam da destruição acidental ou ilícita, da perda ou alteração acidental, ou do armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;
- c) Os dados devem ser objeto de medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados;
- e
- d) Os dados devem ser destruídos no final do período de conservação, exceto os dados que tenham sido facultados e preservados.

Artigo 8.º

Requisitos para o armazenamento dos dados conservados

Os Estados-Membros devem assegurar que os dados especificados no artigo 5.º sejam conservados em conformidade com a presente diretiva de modo que tais dados e outras informações necessárias relacionadas com esses dados possam ser transmitidos imediatamente, mediante pedido, às autoridades competentes.

Artigo 9.º

Autoridade de controlo

1. Cada Estado-Membro deve designar uma ou mais autoridades públicas para controlar a aplicação, no respetivo território, das disposições adotadas pelos Estados-Membros, nos termos do artigo 7.º, no que diz respeito à segurança dos dados conservados. Essas autoridades podem ser as referidas no artigo 28.º da Diretiva 95/46/CE.

2. As autoridades a que se refere o n.º 1 devem atuar com absoluta independência no exercício do controlo da aplicação a que se refere o mesmo número.

[...]

Artigo 11.º

Alteração da Diretiva 2002/58/CE

No artigo 15.º da Diretiva 2002/58/CE é inserido o seguinte número:

‘1-A. O n.º 1 não é aplicável aos dados cuja conservação seja especificamente exigida pela Diretiva [2006/24] para os fins mencionados no n.º 1 do artigo 1.º dessa diretiva.’

[...]

Artigo 13.º

Recursos, responsabilidade e sanções

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as medidas nacionais que dão execução ao capítulo III da Diretiva 95/46/CE relativo a recursos judiciais, responsabilidade e sanções sejam plenamente aplicadas no que se refere ao tratamento de dados no âmbito da presente diretiva.

2. Os Estados-Membros devem tomar, em particular, as medidas necessárias para assegurar que o acesso ou a transferência intencional de dados conservados em conformidade com a presente diretiva, não permitido pelo direito nacional adotado em virtude da presente diretiva, seja punível por sanções, incluindo sanções administrativas ou penais, que sejam efetivas, proporcionadas e dissuasivas.»

Litígios no processo principal e questões prejudiciais

Processo C-293/12

- 17 A Digital Rights interpôs, em 11 de agosto de 2006, um recurso na High Court, no qual alega que é proprietária de um telefone móvel, registado em 3 de junho de 2006, que utiliza desde essa data. Põe em causa a legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas e pede, designadamente, ao órgão jurisdicional de reenvio que declare a nulidade da Diretiva 2006/24 e da sétima parte da Lei de 2005, sobre Justiça Penal (infrações terroristas) [Criminal Justice (Terrorist Offences) Act 2005], que prevê que os fornecedores de serviços de comunicações telefónicas devem conservar os dados respeitantes a estas últimas,

relativos ao tráfego e à localização durante um período determinado por lei, com o objetivo de prevenção e deteção das infrações, de investigação e repressão das mesmas e para garantir a segurança do Estado.

18 A High Court, considerando que não pode dirimir as questões relativas ao direito nacional que lhe foram submetidas sem que a validade da Diretiva 2006/24 tenha sido apreciada, decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) A restrição dos direitos da [recorrente], no que respeita à utilização da rede telefónica móvel, resultante das exigências dos artigos 3.º, 4.º e 6.º da Diretiva 2006/24/CE é incompatível com o artigo 5.º, n.º 4, TUE, na medida em que é desproporcionada e desnecessária ou inadequada para alcançar os objetivos legítimos de:

a) assegurar que determinados dados são disponibilizados para efeitos de investigação, deteção e repressão de crimes graves?

e/ou

b) assegurar o funcionamento adequado do mercado interno da União Europeia?

2) Concretamente,

a) A Diretiva 2006/24/CE é compatível com o direito dos cidadãos de circular e permanecer livremente no território dos Estados-Membros, consagrado no artigo 21.º TFUE?

b) A Diretiva 2006/24/CE é compatível com o direito ao respeito pela vida privada, consagrado no artigo 7.º da Carta [dos Direitos Fundamentais da União Europeia (a seguir 'Carta')] e no artigo 8.º da CEDH?

c) A Diretiva 2006/24/CE é compatível com o direito à proteção dos dados pessoais, consagrado no artigo 8.º da Carta?

d) A Diretiva 2006/24/CE é compatível com o direito à liberdade de expressão, consagrado no artigo 11.º da Carta e no artigo 10.º da CEDH?

e) A Diretiva 2006/24/CE é compatível com o direito a uma boa administração, consagrado no artigo 41.º da Carta?

3) Em que medida os Tratados — e, em concreto, o princípio da cooperação leal previsto no artigo 4.º, n.º 3, TUE — exigem que os tribunais investiguem e apreciem a compatibilidade das medidas nacionais de transposição da Diretiva 2006/24/CE com as garantias conferidas pela [Carta], incluindo o seu artigo 7.º (cujo conteúdo é inspirado no artigo 8.º da CEDH)?»

Processo C-594/12

19 Na origem do pedido de decisão prejudicial no processo C-594/12 estão vários recursos interpostos no Verfassungsgerichtshof, respetivamente, pela Kärntner Landesregierung e por M. Seitlinger, C. Tschohl e 11 128 outros recorrentes, que pedem a anulação do artigo 102.º-A da Lei de 2003, sobre as telecomunicações (Telekommunikationsgesetz 2003), introduzido nesta lei pela lei de alteração (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl. I,

27/2011)), para efeitos da transposição da Diretiva 2006/24 para o direito interno austríaco. Estas partes consideram, designadamente, que este artigo 102.º-A viola o direito fundamental dos particulares à proteção dos seus dados.

- 20 O Verfassungsgerichtshof pergunta-se, designadamente, se a Diretiva 2006/24 é compatível com a Carta na medida em que permite o armazenamento de um volume de tipos de dados relativos a um número ilimitado de pessoas, durante um longo período. A conservação dos dados diz respeito quase exclusivamente a pessoas cujo comportamento não justifica sequer que os seus dados sejam conservados. Estas pessoas ficam expostas a um risco superior de que as autoridades investiguem os seus dados, tomem conhecimento do seu conteúdo, se informem acerca da sua vida privada e utilizem estes dados com múltiplas finalidades, tendo designadamente em conta o número incommensurável de pessoas que têm acesso aos dados durante um período de, pelo menos, seis meses. Segundo o órgão jurisdicional de reenvio, há dúvidas, por um lado, quanto ao facto de esta diretiva poder alcançar os objetivos que prossegue e, por outro, quanto ao carácter proporcionado da ingerência nos direitos fundamentais em causa.
- 21 Nestas condições, o Verfassungsgerichtshof decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Quanto à validade dos atos adotados pelas instituições da União:

Os artigos 3.º a 9.º da Diretiva [2006/24] são compatíveis com os artigos 7.º, 8.º e 11.º da [Carta]?

2) Quanto à interpretação dos Tratados:

- a) À luz das anotações ao artigo 8.º da Carta, as quais, nos termos do artigo 52.º, n.º 7, da Carta, devem ser tidas em devida conta pelo Verfassungsgerichtshof como orientações para a interpretação da referida Carta, a Diretiva [95/46] e o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados [(JO 2001, L 8, p. 1)], devem ser tidos em consideração de forma equivalente às condições constantes do artigo 8.º, n.º 2, e do artigo 52.º, n.º 1, da Carta, ao apreciar a admissibilidade das ingerências?
- b) Qual é a relação existente entre o ‘direito da União’, referido na última frase do artigo 52.º, n.º 3, da Carta, e as diretivas em matéria do direito à proteção de dados?
- c) Atendendo ao facto de a Diretiva [95/46] e o Regulamento [...] n.º 45/2001 imporem condições e restrições na salvaguarda do direito fundamental à proteção de dados constante da Carta, as alterações resultantes do direito derivado posterior devem ser tidas em consideração ao interpretar o artigo 8.º da Carta?
- d) Considerando o artigo 52.º, n.º 4, da Carta, resulta do princípio da salvaguarda de um nível de proteção mais elevado, consagrado no artigo 53.º da Carta, que os limites, estabelecidos pela Carta, para as restrições que podem ser colocadas pelo direito derivado devem ser definidos de acordo com critérios mais exigentes?
- e) Considerando o artigo 52.º, n.º 3, da Carta, o artigo 5.º do preâmbulo e as anotações ao artigo 7.º da Carta, nos termos das quais os direitos aí garantidos correspondem aos direitos garantidos pelo artigo 8.º da CEDH, é possível deduzir da jurisprudência do Tribunal Europeu dos Direitos do Homem em relação ao artigo 8.º da CEDH a existência de elementos de interpretação do artigo 8.º da Carta que possam influenciar a interpretação deste último artigo?»

- 22 Por decisão do presidente do Tribunal de Justiça de 11 de junho de 2013, os processos C-293/12 e C-594/12 foram apensados para efeitos da fase oral e do acórdão.

Quanto às questões prejudiciais

Quanto à segunda questão, alíneas b) a d), no processo C-293/12 e à primeira questão no processo C-594/12

- 23 Com a segunda questão, alíneas b) a d), no processo C-293/12 e com a primeira questão no processo C-594/12, que devem ser analisadas conjuntamente, os órgãos jurisdicionais de reenvio pedem, em substância, ao Tribunal de Justiça que aprecie a validade da Diretiva 2006/24 à luz dos artigos 7.º, 8.º e 11.º da Carta.

Quanto à pertinência dos artigos 7.º, 8.º e 11.º da Carta, no que respeita à questão da validade da Diretiva 2006/24

- 24 Resulta do artigo 1.º e dos considerandos 4, 5, 7 a 11, 21 e 22 da Diretiva 2006/24 que esta visa harmonizar as disposições dos Estados-Membros relativas à conservação, pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações, de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de infrações graves, como os associados ao crime organizado e ao terrorismo, no respeito dos direitos consagrados nos artigos 7.º e 8.º da Carta.
- 25 A obrigação de os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações, prevista no artigo 3.º da Diretiva 2006/24, conservarem os dados enumerados no artigo 5.º da mesma, para, se necessário, os disponibilizarem às autoridades nacionais competentes, suscita questões relativas à proteção tanto da vida privada como das comunicações, consagrada no artigo 7.º da Carta, à proteção de dados pessoais, prevista no artigo 8.º da mesma, assim como ao respeito da liberdade de expressão, garantida pelo artigo 11.º da Carta.
- 26 A este respeito, importa salientar que os dados que os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações devem conservar, nos termos dos artigos 3.º e 5.º da Diretiva 2006/24, são, designadamente, os dados necessários para encontrar e identificar a fonte e o destino de uma comunicação, para determinar a data, a hora, a duração e o tipo de uma comunicação, o equipamento de comunicação dos utilizadores, bem como para localizar o equipamento de comunicação móvel, dados entre os quais figuram, designadamente, o nome e o endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário e também um endereço IP para os serviços Internet. Estes dados permitem, designadamente, saber qual é a pessoa com quem 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.
- 27 Estes dados, considerados no seu todo, 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 e os meios sociais frequentados.
- 28 Em tais circunstâncias, apesar de a Diretiva 2006/24 não autorizar, como resulta dos seus artigos 1.º, n.º 2, e 5.º, n.º 2, a conservação do conteúdo da comunicação e das informações consultadas através de uma rede de comunicações eletrónicas, não está excluído que a conservação dos dados em causa

possa ter incidência na utilização, pelos assinantes ou pelos utilizadores registados, dos meios de comunicação previstos por esta diretiva e, conseqüentemente, no exercício, por estes últimos, da sua liberdade de expressão, garantida pelo artigo 11.º da Carta.

- 29 A conservação dos dados, para efeitos do eventual acesso aos mesmos pelas autoridades nacionais competentes, como prevista pela Diretiva 2006/24, diz direta e especificamente respeito à vida privada e, assim, aos direitos garantidos pelo artigo 7.º da Carta. Além disso, essa conservação dos dados está abrangida pelo âmbito de aplicação do artigo 8.º desta, uma vez que constitui um tratamento de dados pessoais na aceção deste artigo e deve, assim, necessariamente, respeitar as exigências de proteção de dados resultantes deste artigo (acórdão Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, n.º 47).
- 30 Embora suscitem designadamente a questão de princípio de saber se os dados dos assinantes e dos utilizadores registados podem ou não, à luz do artigo 7.º da Carta, ser conservados, os reenvios prejudiciais nos presentes processos colocam igualmente a questão de saber se a Diretiva 2006/24 responde às exigências de proteção dos dados pessoais resultantes do artigo 8.º da Carta.
- 31 À luz das considerações precedentes, para responder à segunda questão, alíneas b) a d), no processo C-293/12, e à primeira questão no processo C-594/12, importa analisar a validade da Diretiva 2006/24 à luz dos artigos 7.º e 8.º da Carta.

Quanto à existência de uma ingerência nos direitos consagrados pelos artigos 7.º e 8.º da Carta

- 32 Ao impor a conservação dos dados enumerados no artigo 5.º, n.º 1, da Diretiva 2006/24 e ao permitir o acesso das autoridades nacionais competentes aos mesmos, esta diretiva derroga, como salientou o advogado-geral, designadamente, nos n.ºs 39 e 40 das suas conclusões, o regime de proteção do direito ao respeito da vida privada, instituído pelas Diretivas 95/46 e 2002/58, em relação ao tratamento de dados pessoais no setor das comunicações eletrónicas, visto que estas diretivas consagram a confidencialidade das comunicações e dos dados relativos ao tráfego, bem como a obrigação de eliminar ou de tornar anónimos esses dados, quando deixem de ser necessários para a transmissão de uma comunicação, salvo se forem necessários para a faturação e unicamente enquanto esta necessidade persistir.
- 33 Para demonstrar a existência de uma ingerência no direito fundamental ao respeito da vida privada, pouco importa que as informações relativas à vida privada em questão tenham ou não caráter sensível, ou que os interessados tenham ou não sofrido eventuais inconvenientes em razão dessa ingerência (v., neste sentido, acórdão Österreichischer Rundfunk e o., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, n.º 75).
- 34 Daí resulta que a obrigação imposta pelos artigos 3.º e 6.º da Diretiva 2006/24 aos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações, de conservarem durante um determinado período dados relativos à vida privada de uma pessoa e às suas comunicações, como os previstos no artigo 5.º desta diretiva, constitui em si mesma uma ingerência nos direitos garantidos pelo artigo 7.º da Carta.
- 35 Além disso, o acesso das autoridades nacionais competentes aos dados constitui uma ingerência suplementar neste direito fundamental (v., no que respeita ao artigo 8.º da CEDH, acórdãos TEDH, Leander c. Suécia de 26 de março de 1987, série A, n.º116, § 48; Rotaru c. Roménia [GC], n.º 28341/95, § 46, CEDH 2000-V; e Weber e Saravia c. Alemanha (dec.), n.º 54934/00, § 79, CEDH 2006-XI). Assim, os artigos 4.º e 8.º da Diretiva 2006/24, ao estabelecerem regras para o acesso das autoridades nacionais competentes aos dados, são igualmente constitutivos de uma ingerência nos direitos garantidos pelo artigo 7.º da Carta.

- 36 Do mesmo modo, a Diretiva 2006/24 é constitutiva de uma ingerência no direito fundamental à proteção dos dados pessoais, garantido pelo artigo 8.º da Carta, visto que prevê um tratamento dos dados pessoais.
- 37 Há que constatar que a ingerência que a Diretiva 2006/24 comporta nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, como também salientou o advogado-geral, entre outros, nos n.ºs 77 e 80 das suas conclusões, é de grande amplitude e deve ser considerada particularmente grave. Além disso, o facto de a conservação dos dados e a sua utilização posterior serem efetuadas sem que o assinante ou o utilizador registado sejam informados disso é suscetível de gerar no espírito das pessoas em causa, como salientou o advogado-geral nos n.ºs 52 e 72 das suas conclusões, a sensação de que a sua vida privada é constantemente vigiada.

Quanto à justificação da ingerência nos direitos garantidos pelos artigos 7.º e 8.º da Carta

- 38 Em conformidade com o artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos por esta deve ser prevista por lei, respeitar o conteúdo essencial desses direitos e liberdades, e, na observância do princípio da proporcionalidade, só podem ser introduzidas restrições a esses direitos e 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.
- 39 No que respeita ao conteúdo essencial do direito fundamental ao respeito da vida privada e dos outros direitos consagrados no artigo 7.º da Carta, deve observar-se que, embora a conservação dos dados imposta pela Diretiva 2006/24 constitua uma ingerência particularmente grave nesses direitos, não é suscetível de afetar o referido conteúdo, tendo em conta que, como resulta do seu artigo 1.º, n.º 2, esta diretiva não permite tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal.
- 40 Esta conservação dos dados também não é suscetível de afetar o conteúdo essencial do direito fundamental à proteção dos dados pessoais, consagrado no artigo 8.º da Carta, uma vez que a Diretiva 2006/24 prevê, no seu artigo 7.º, uma regra relativa à proteção e à segurança dos dados, segundo a qual, sem prejuízo das disposições adotadas em aplicação das Diretivas 95/46 e 2002/58, devem ser respeitados certos princípios de proteção e de segurança dos dados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, princípios de acordo com os quais os Estados-Membros devem assegurar a adoção de medidas técnicas e organizacionais adequadas contra a destruição acidental ou ilícita, a perda ou a alteração acidental dos dados.
- 41 Quanto à questão de saber se a referida ingerência responde a um objetivo de interesse geral, importa salientar que, embora a Diretiva 2006/24 vise harmonizar as disposições dos Estados-Membros relativas às obrigações dos referidos fornecedores em matéria de conservação de determinados dados por eles gerados ou tratados, o objetivo material desta diretiva, como resulta do seu artigo 1.º, n.º 1, tem em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de infrações graves, tal como definidas no direito interno de cada Estado-Membro. O objetivo material desta diretiva é, pois, contribuir para a luta contra a criminalidade grave e, assim, em última análise, para a segurança pública.
- 42 Resulta da jurisprudência do Tribunal de Justiça que a luta contra o terrorismo internacional constitui um objetivo de interesse geral da União, com vista à manutenção da paz e da segurança internacionais (v., neste sentido, acórdãos Kadi e Al Barakaat International Foundation/Conselho e Comissão, C-402/05 P e C-415/05 P, EU:C:2008:461, n.º 363, e Al-Aqsa/Conselho, C-539/10 P e C-550/10 P, EU:C:2012:711, n.º 130). O mesmo acontece com a luta contra a criminalidade grave, com o objetivo

de garantir a segurança pública (v., neste sentido, acórdão Tsakouridis, C-145/09, EU:C:2010:708, n.ºs 46 e 47). Além disso, importa salientar, a este respeito, que o artigo 6.º da Carta enuncia o direito das pessoas não só à liberdade mas também à segurança.

- 43 A este respeito, resulta do considerando 7 da Diretiva 2006/24 que, devido a um notável crescimento das possibilidades oferecidas pelas comunicações eletrónicas, o Conselho «Justiça e Assuntos Internos» de 19 de dezembro de 2002 considerou que os dados gerados pela utilização desse tipo de comunicações são extremamente importantes e constituem, portanto, um instrumento útil na prevenção das infrações e na luta contra a criminalidade, designadamente a criminalidade organizada.
- 44 Impõe-se pois observar que a conservação dos dados com vista a permitir o eventual acesso aos mesmos pelas autoridades nacionais competentes, tal como imposta pela Diretiva 2006/24, responde efetivamente a um objetivo de interesse geral.
- 45 Nestas condições, há que analisar a proporcionalidade da ingerência constatada.
- 46 A este propósito, cabe recordar que o princípio da proporcionalidade exige, segundo jurisprudência constante do Tribunal de Justiça, que os atos das instituições da União sejam adequados à realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário à realização desses objetivos (v., neste sentido, acórdãos Afton Chemical, C-343/09, EU:C:2010:419, n.º 45; Volker und Markus Schecke e Eifert, EU:C:2010:662, n.º 74; Nelson e o., C-581/10 e C-629/10, EU:C:2012:657, n.º 71; Sky Österreich, C-283/11, EU:C:2013:28, n.º 50; e Schaible, C-101/12, EU:C:2013:661, n.º 29).
- 47 Quanto à fiscalização jurisdicional do respeito destes requisitos, uma vez que estão em causa ingerências em direitos fundamentais, o alcance do poder de apreciação do legislador da União pode revelar-se limitado em função de um certo número de elementos, entre os quais figuram, designadamente, o domínio em questão, a natureza do direito em causa garantido pela Carta, a natureza e a gravidade da ingerência, bem como a sua finalidade (v., por analogia, no que respeita ao artigo 8.º da CEDH, acórdão TEDH, S e Marper c. Reino Unido [GC], n.ºs 30562/04 e 30566/04, § 102, CEDH 2008-V).
- 48 No caso vertente, tendo em conta, por um lado, o importante papel desempenhado pela proteção dos dados pessoais na perspetiva do direito fundamental ao respeito da vida privada e, por outro, a amplitude e a gravidade da ingerência neste direito que a Diretiva 2006/24 comporta, o poder de apreciação do legislador da União fica reduzido, havendo que proceder a uma fiscalização estrita.
- 49 No que respeita à questão de saber se a conservação dos dados é adequada à realização do objetivo prosseguido pela Diretiva 2006/24, cumpre observar que, tendo em conta a crescente importância dos meios de comunicação eletrónica, os dados que devem ser conservados em aplicação desta diretiva permitem às autoridades nacionais competentes em matéria penal dispor de possibilidades suplementares de elucidação das infrações graves e, portanto, nesta perspetiva, constituem um instrumento útil nas investigações penais. Assim, a conservação desses dados pode ser considerada adequada à realização do objetivo prosseguido pela dita diretiva.
- 50 Esta apreciação não pode ser posta em causa pela circunstância, invocada designadamente por C. Tschohl e M. Seitlinger, bem como pelo Governo português nas observações escritas que apresentou ao Tribunal de Justiça, de haver várias modalidades de comunicações eletrónicas que não estão abrangidas pelo âmbito de aplicação da Diretiva 2006/24 ou que permitem uma comunicação anónima. Embora, é certo, esta circunstância seja suscetível de limitar a adequação da medida de conservação dos dados à realização do objetivo prosseguido, não é, todavia, suscetível de a tornar inapta, como salientou o advogado-geral no n.º 137 das suas conclusões.

- 51 No que respeita ao caráter necessário da conservação dos dados imposta pela Diretiva 2006/24, cabe observar que é verdade que a luta contra a criminalidade grave, designadamente a criminalidade organizada e o terrorismo, assume primordial importância para garantir a segurança pública, e a sua eficácia pode depender em larga medida da utilização das técnicas modernas de investigação. No entanto, tal objetivo de interesse geral, por muito fundamental que seja, não pode, por si só, justificar que uma medida de conservação como a que foi instituída pela Diretiva 2006/24 seja considerada necessária para efeitos da referida luta.
- 52 Quanto ao direito ao respeito da vida privada, a proteção deste direito fundamental exige, segundo a jurisprudência constante do Tribunal de Justiça, em quaisquer circunstâncias, que as derrogações à proteção dos dados pessoais e as suas limitações devam ocorrer na estrita medida do necessário (acórdão IPI, C-473/12, EU:C:2013:715, n.º 39 e jurisprudência referida).
- 53 A este respeito, cabe recordar que a proteção dos dados pessoais, que resulta da obrigação expressa prevista no artigo 8.º, n.º 1, da Carta, assume particular importância para o direito ao respeito da vida privada consagrado no artigo 7.º desta.
- 54 Assim, a regulamentação da União em causa deve estabelecer regras claras e precisas que regulem o âmbito e a aplicação da medida em causa e 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 e contra qualquer acesso e utilização ilícita dos mesmos (v., por analogia, no que respeita ao artigo 8.º da CEDH, acórdãos TEDH, Liberty e outros c. Reino Unido de 1 de julho de 2008, n.º 58243/00, §§ 62 e 63; Rotaru c. Roménia, já referido, §§ 57 a 59; e S e Marper c. Reino Unido, já referido, § 99).
- 55 A necessidade de dispor de tais garantias é ainda mais importante quando, como previsto na Diretiva 2006/24, os dados pessoais são sujeitos a tratamento automático e existe um risco significativo de acesso ilícito aos mesmos (v., por analogia, no que respeita ao artigo 8.º da CEDH, acórdãos TEDH, S e Marper c. Reino Unido, já referido, § 103, e M. K. c. França de 18 de abril de 2013, n.º 19522/09, § 35).
- 56 Quanto à questão de saber se a ingerência que a Diretiva 2006/24 comporta se limita ao estritamente necessário, importa salientar que esta diretiva impõe, nos termos do seu artigo 3.º, conjugado com o seu artigo 5.º, n.º 1, a conservação de todos os dados relativos ao tráfego respeitante à rede telefónica fixa, à rede telefónica móvel, ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet. Assim, visa todos os meios de comunicação eletrónica cuja utilização está muito divulgada e é de crescente importância na vida quotidiana de todos. Além disso, em conformidade com o seu artigo 3.º, a referida diretiva abrange todos os assinantes e utilizadores registados. Comporta, portanto, uma ingerência nos direitos fundamentais de quase toda a população europeia.
- 57 A este propósito, importa observar, em primeiro lugar, que a Diretiva 2006/24 abrange de maneira geral todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada nenhuma diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações graves.
- 58 Com efeito, por um lado, a Diretiva 2006/24 abrange, em geral, todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que, no entanto, as pessoas cujos dados são conservados se encontrem, ainda que indiretamente, numa situação suscetível de dar lugar a ações penais. Assim, aplica-se mesmo 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 graves. Além disso, não prevê nenhuma exceção, pelo que é aplicável mesmo a pessoas cujas comunicações estão sujeitas ao segredo profissional, segundo as regras do direito nacional.

- 59 Por outro lado, sem deixar de ter por objetivo contribuir para a luta contra a criminalidade grave, a referida diretiva não exige nenhuma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública e, designadamente, não se limita a uma conservação nem de dados relativos a um período de tempo e/ou a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de uma maneira ou de outra, numa infração grave, nem de dados relativos a pessoas, cuja conservação, por outros motivos, pudesse contribuir para a prevenção, a deteção ou a repressão de infrações graves.
- 60 Em segundo lugar, a esta ausência geral de limites acresce que a Diretiva 2006/24 não estabelece critérios objetivos que permitam delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas suficientemente graves, à luz da amplitude e da gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, para justificar tal ingerência. Pelo contrário, a Diretiva 2006/24 limita-se a remeter, no seu artigo 1.º, n.º 1, de forma genérica, para as infrações graves tal como definidas no direito nacional de cada Estado-Membro.
- 61 Além disso, quanto ao acesso das autoridades nacionais competentes aos dados e à sua utilização posterior, a Diretiva 2006/24 não contém as correspondentes condições materiais e processuais. O artigo 4.º desta diretiva, que regula o acesso destas autoridades aos dados conservados, não dispõe expressamente que este acesso e a utilização posterior dos dados em causa devem ser estritamente restringidos a fins de prevenção e de deteção de infrações graves delimitadas com precisão ou de ações penais contra as mesmas, limitando-se a dispor que cada Estado-Membro define os procedimentos que devem ser seguidos e as condições que devem ser preenchidas para se ter acesso aos dados conservados no respeito dos requisitos da necessidade e da proporcionalidade.
- 62 Em particular, a Diretiva 2006/24 não estabelece critérios objetivos que permitam limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário à luz do objetivo prosseguido. Sobretudo, o acesso aos dados conservados pelas autoridades nacionais competentes não está sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente cuja decisão vise limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido e ocorra na sequência de um pedido fundamentado destas autoridades, apresentado no âmbito de procedimentos de prevenção, de deteção ou de uma ação penal. Também não foi prevista uma obrigação precisa de os Estados-Membros estabelecerem tais limitações.
- 63 Em terceiro lugar, no que respeita à duração da conservação dos dados, a Diretiva 2006/24 impõe, no seu artigo 6.º, que sejam conservados por períodos não inferiores a seis meses, não procedendo a uma distinção entre as categorias de dados previstas no artigo 5.º desta diretiva em função da sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa.
- 64 Além disso, a referida duração situa-se entre um mínimo de seis meses e um máximo de vinte e quatro meses, sem que se especifique que a determinação do período de conservação se deve basear em critérios objetivos a fim de garantir que se limita ao estritamente necessário.
- 65 Resulta do que precede que a Diretiva 2006/24 não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta. Impõe-se pois concluir que esta diretiva comporta uma ingerência nestes direitos fundamentais, de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário.
- 66 Acresce que, no que respeita às regras relativas à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, há que concluir que a Diretiva 2006/24 não prevê garantias suficientes, como exige o

artigo 8.º da Carta, que permitam assegurar uma proteção eficaz dos dados conservados contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos. Com efeito, em primeiro lugar, o artigo 7.º da Diretiva 2006/24 não estabelece regras específicas e adaptadas à grande quantidade de dados cuja conservação é imposta por esta diretiva, ao caráter sensível destes dados e ao risco de acesso ilícito aos mesmos, regras que se destinariam, designadamente, a regular de maneira clara e estrita a proteção e a segurança dos dados em causa, a fim de garantir a sua plena integridade e confidencialidade. Além disso, também não foi prevista uma obrigação precisa de os Estados-Membros estabelecerem tais regras.

- 67 O artigo 7.º da Diretiva 2006/24, conjugado com os artigos 4.º, n.º 1, da Diretiva 2002/58 e 17.º, n.º 1, segundo parágrafo, da Diretiva 95/46, não garante a aplicação pelos referidos fornecedores de um nível particularmente elevado de proteção e de segurança através de medidas técnicas e organizacionais, mas autoriza designadamente estes fornecedores a terem em conta considerações económicas na determinação do nível de segurança que aplicam, no que respeita aos custos de execução das medidas de segurança. Em especial, a Diretiva 2006/24 não garante a destruição definitiva dos dados no termo do período de conservação dos mesmos.
- 68 Em segundo lugar, deve acrescentar-se que a referida diretiva não impõe que os dados em causa sejam conservados no território da União, pelo que não se pode considerar que esteja plenamente garantida a fiscalização, por uma entidade independente, expressamente exigida pelo artigo 8.º, n.º 3, da Carta, do respeito das exigências de proteção e de segurança, tal como referidas nos dois números anteriores. Ora, semelhante fiscalização, efetuada com base no direito da União, constitui um elemento essencial do respeito da proteção das pessoas relativamente ao tratamento dos dados pessoais (v., neste sentido, acórdão Comissão/Áustria, C-614/10, EU:C:2012:631, n.º 37).
- 69 Face ao exposto, há que considerar que, ao adotar a Diretiva 2006/24, o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta.
- 70 Nestas condições, não há que apreciar a validade da Diretiva 2006/24 à luz do artigo 11.º da Carta.
- 71 Por conseguinte, há que responder à segunda questão, alíneas b) a d), no processo C-293/12 e à primeira questão no processo C-594/12 que a Diretiva 2006/24 é inválida.

Quanto à primeira questão, à segunda questão, alíneas a) e e), e à terceira questão no processo C-293/12 e quanto à segunda questão no processo C-594/12

- 72 Resulta do que foi decidido no número anterior que não há que responder à primeira questão, à segunda questão, alíneas a) e e), e à terceira questão no processo C-293/12, nem à segunda questão no processo C-594/12.

Quanto às despesas

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

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

A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, é inválida.

Assinaturas