Processo C-793/19

Resumo do pedido de decisão prejudicial em aplicação do artigo 98.°, n.° 1, do Regulamento de Processo do Tribunal de Justiça

Data de entrada:

29 de outubro de 2019

Órgão jurisdicional de reenvio:

Bundesverwaltungsgericht (Tribunal Administrativo Federal, Alemanha)

Data da decisão de reenvio:

25 de setembro de 2019

Demandante e recorrida em «Revision»:

SpaceNet AG

Demandada e recorrente em «Revision»:

República Federal da Alemanha

Objeto do processo principal

Ação destinada a obter a declaração de que a SpaceNet não é obrigada a conservar os dados de telecomunicações e de tráfego dos seus clientes, referidos no § 113b, n.° 3, da TKG (Lei das telecomunicações), aos quais fornece acesso à internet.

Objeto e fundamento jurídico do pedido de decisão prejudicial

Interpretação do direito da União, em especial, do artigo 15.°, n.° 1, da Diretiva 2002/58, e do Acórdão Tele2 Sverige e Watson e o.; artigo 267.° TFUE.

Questão prejudicial

Deve o artigo 15.° da Diretiva 2002/58/CE, à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, por um lado, e do artigo 6.° da Carta dos Direitos Fundamentais da União Europeia e do artigo 4.° do Tratado da União Europeia, por outro, ser interpretado no sentido de que se opõe a uma regulamentação nacional que obriga os prestadores de serviços de comunicações publicamente disponíveis a conservarem os dados de tráfego e de localização dos utilizadores finais destes serviços, quando

- esta obrigação não pressuponha nenhum motivo específico de ordem local, temporal ou geográfica,
- esta obrigação de conservação no âmbito da prestação de serviços de comunicações publicamente disponíveis, incluindo a transmissão de notícias curtas ou de notícias multimédia ou semelhantes, bem como chamadas não atendidas ou comunicações falhadas, tiver por objeto os seguintes dados:
    - o número de telefone ou outra identificação da linha chamadora e da linha conectada e, no caso de comutações e reencaminhamentos, o de qualquer outra ligação envolvida,
    - a data e a hora do início e do fim da comunicação ou, no caso de transmissão de notícias curtas ou de notícias multimédia ou semelhantes, as datas da transmissão e da receção da notícia, mediante indicação do fuso horário utilizado,
    - dados sobre o serviço utilizado, quando puderem ser utilizados vários serviços no âmbito do serviço telefónico,
    - e ainda, no caso de serviços de comunicação móvel,
        - a identificação internacional dos assinantes móveis da linha chamadora e da linha conectada,
        - a identificação internacional do equipamento terminal da linha chamadora e da linha conectada,
        - a data e a hora da primeira ativação do serviço, com indicação do fuso horário utilizado, se os serviços forem pré-pagos
        - a indicação das células utilizadas para a linha chamadora e a linha conectada no início da ligação,
    - e, no caso de serviços telefónicos através da Internet, o endereço do protocolo IP da linha chamadora e da linha conectada e os códigos de identificação atribuídos ao utilizador,
- a obrigação de conservação, no âmbito da prestação de serviços de Internet publicamente disponíveis, tiver por objeto os seguintes dados:
    - o endereço do protocolo IP atribuído ao assinante para a utilização da Internet,

    – uma identificação inequívoca da ligação através da qual a Internet é utilizada e os identificadores atribuídos aos utilizadores,

    – a data e a hora do início e do fim da utilização da Internet ao abrigo do endereço do protocolo IP atribuído, mediante indicação do fuso horário utilizado,

    – em caso de utilização móvel, a indicação da célula utilizada no início da ligação à Internet,

– os seguintes dados não puderem ser conservados:

    – o conteúdo da comunicação,

    – dados sobre páginas Internet visualizadas,

    – dados sobre serviços de correio eletrónico,

    – dados subjacentes a determinadas ligações de ou para pessoas, autoridades e organizações no âmbito social ou eclesiástico,

– a duração da conservação de dados de localização, ou seja, a identificação da célula utilizada for de quatro semanas e a dos restantes dados, de dez semanas,

– for garantida a proteção eficaz dos dados conservados contra riscos de abuso e contra qualquer acesso não autorizado, e

– os dados conservados só puderem ser utilizados para efeitos de exercício da ação penal por crimes particularmente graves e de defesa contra um perigo real para a integridade física, a vida ou a liberdade de uma pessoa ou para a existência do Estado Federal ou de um *Land*, com exceção do endereço do protocolo IP atribuído ao assinante para efeitos de utilização da Internet, cuja utilização seja permitida no âmbito da obtenção de dados para efeitos de exercício da ação penal por quaisquer crimes, de defesa contra um risco para a segurança pública e para a ordem pública, bem como para o cumprimento das tarefas dos serviços de informação?

Disposições do direito da União invocadas

Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»), artigos 6.°, 7.°, 8.°, 11.°, 52.°

Tratado da União Europeia (TUE), artigos 4.°, 6.°

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), na redação que lhe foi dada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (a seguir «Diretiva 2002/58/CE», artigos 5.°, 6.°, 8.°, 9.°, em particular, artigo 15.°; considerando 11

Disposições do direito nacional invocadas

Telekommunikationsgesetz (Lei das telecomunicações, a seguir «TKG»), § 113a, n.° 1, primeiro período («Responsáveis»), § 113b («Obrigações de conservação de dados de tráfego»), § 113c («Utilização dos dados»), § 113d («Garantia da segurança dos dados»), § 113e («Registo» [pelo responsável, dos acessos aos dados armazenados]), § 113f («Catálogo de requisitos» [relativos a medidas técnicas e a outras medidas], § 99, n.° 2 («Faturação detalhada», identificação dos organismos excluídos da faturação detalhada)

Strafprozessordnung (Código de Processo Penal, a seguir «StPO»), § 100g, n.° 2 («Recolha de dados de tráfego» nos termos do § 113b da TKG)

Jurisprudência do Tribunal de Justiça invocada

Acórdão do Tribunal de Justiça da União Europeia de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970 (a seguir «Acórdão Tele2 Sverige e Watson e o.»)

Acórdão de 8 de abril de 2014, Digital Rights Ireland e Seitlinger e o., C-293/12 e C-594/12, EU:C:2014:238 (a seguir «Acórdão Digital Rights Ireland e o.»)

Parecer 1/15, de 26 de julho de 2017, EU:C:2017:592

E ainda: Acórdãos de 29 de julho de 2019, Funke Medien (C-469/17, EU:C:2019:623), de 9 de março de 1978, Simmenthal (106/77, EU:C:1978:49), de 3 de maio de 2005, Berlusconi e o. (C-387/02, C-391/02 e C-403/02, EU:C:2005:270), de 22 de junho de 2010, Melki e Abdeli (C-188/10 e C-189/10, EU:C:2010:363), de 18 de setembro de 2014, Vueling Airlines (C-487/12, EU:C:2014:2232).

Apresentação sucinta dos factos e do processo principal

1 A demandante, SpaceNet AG (a seguir «demandante» ou «SpaceNet»), fornece serviços de comunicações eletrónicas publicamente disponíveis. Contesta a obrigação que lhe foi imposta pelo § 113a, n.° 1, em conjugação com o § 113b, da TKG, com a redação da Lei de 10 de dezembro de 2015, de, a partir de 1 de julho de 2017, conservar os dados de tráfego de telecomunicações dos seus clientes.

2 O Verwaltungsgericht (Tribunal Administrativo) declarou, em primeira instância, que a SpaceNet não está obrigada a conservar os dados de tráfego de telecomunicações dos seus clientes aos quais faculta acesso à Internet, referidos

no § 113b, n.° 3, da TKG. A demandada, a República Federal da Alemanha (a seguir «demandada») interpôs recurso direto de «Revision» contra a sentença do Verwaltungsgericht.

3 O recurso de «Revision» só será procedente se a obrigação de conservação dos dados de tráfego de telecomunicações a cargo dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis (a seguir «fornecedores de telecomunicações»), estabelecida nas disposições da TKG acima referidas, não violar o direito da União.

4 Esta obrigação dos fornecedores de telecomunicações de conservar determinados dados de tráfego durante um período limitado foi adotada pela Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten de 10 de dezembro de 2015 (Lei de 10 de dezembro de 2015 de introdução de uma obrigação de conservação e de uma obrigação máxima de conservação de dados de tráfego, a seguir «Lei de 10 de dezembro de 2015»).

5 Foi necessário adotar um novo regime jurídico na sequência de um acórdão do Bundesverfassungsgericht (Tribunal Constitucional Federal) de 2010 ter declarado nulas as disposições anteriores que regulavam a conservação de dados, devido a uma violação de um direito fundamental e também depois de a Diretiva 2006/24 para cuja transposição as disposições anteriores tinham sido adotadas, ter sido declarada inválida, em 2014, pelo Acórdão Digital Rights Ireland e o.. A Lei de 10 de dezembro de 2015 visa suprir lacunas do processo penal e da proteção contra riscos e, simultaneamente, ter em conta as diretrizes constitucionais e do direito da União, resultantes das referidas decisões.

6 Para responder à questão de saber se a obrigação de conservação estabelecida no § 113a, n.° 1, em conjugação com o § 113b da TKG viola o direito da União, é necessário que o Tribunal de Justiça interprete a Diretiva 2002/58, em particular, que esclareça como deve ser entendido o Acórdão Tele2 Sverige e Watson e o..

Apresentação sucinta da fundamentação do pedido de decisão prejudicial

7 A obrigação estabelecida no § 113a, n.° 1, primeiro período, em conjugação com o § 113b da TKG, de conservação dos dados de tráfego de telecomunicações restringe os direitos consagrados nos artigos 5.°, n.° 1, 6.°, n.° 1 e 9.°, n.° 1, da Diretiva 2002/58.

8 Esta obrigação constitui uma ingerência na confidencialidade das comunicações eletrónicas protegida pelo artigo 5.°, n.° 1, primeiro período, da diretiva e viola o princípio de que nenhuma outra pessoa além do utilizador pode, em regra, conservar os dados de tráfego relacionados com comunicações eletrónicas sem o seu consentimento.

9 Além disso, a referida obrigação não está em conformidade com a orientação estabelecida no artigo 6.° da diretiva, segundo a qual os dados de tráfego só

podem ser tratados e armazenados para efeitos de faturação dos serviços, da sua comercialização e da prestação de um serviço de valor acrescentado, devendo ser limitado ao necessário para efeitos das referidas atividades.

10 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, o artigo 9.°, n.° 1, primeiro período, da Diretiva 2002/58 dispõe que 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. A disposição legal também diverge desta orientação, na medida em que, nos termos do § 113b, n.° 1, segundo parágrafo, em conjugação com o n.° 4, da TKG, os dados de localização nela referidos também devem ser armazenados.

11 A restrição dos direitos nos termos dos artigos 5.°, n.° 1, 6.°, n.° 1 e 9.°, n.° 1, da Diretiva 2002/58 só é justificada se o disposto no § 113a, n.° 1, primeiro período, em conjugação com o § 113b, da TKG, se puder basear no artigo 15.°, n.° 1, da Diretiva 2002/58.

12 Segundo este artigo, 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.° e no artigo 9.° 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.° 1 do artigo 13.° 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.° do Tratado da União Europeia (a seguir «TUE»).

13 Segundo as considerações do Tribunal de Justiça tecidas no Acórdão Tele2 Sverige e Watson e o., em particular, nos n.os 82 e seguintes e 108 e seguintes, deste acórdão, a admissibilidade de um regime nacional de conservação de dados pressupõe, nos termos do artigo 15.°, n.° 1, da Diretiva 2002/58, que exista um motivo suficiente. Tal significa que só são abrangidas as pessoas em relação às quais haja um indício de ligação a crimes graves, que tem de haver uma delimitação quanto à região, ao período e aos meios de comunicação relevantes para o motivo e que só são abrangidos os dados imprescindíveis para a investigação das referidas infrações penais.

14 Assim, o entendimento da demandada de que a utilização de serviços de acesso à Internet ou de serviços telefónicos deve ser, desde logo, considerada como um

motivo suficiente para a conservação é manifestamente incompatível com o acima exposto. A presunção expressa no Acórdão Tele2 Sverige e Watson e o. de incompatibilidade geral com o direito da União de qualquer conservação de dados sem motivo também não é posta em causa pela remissão da demandada para o Parecer do Tribunal de Justiça de 26 de julho de 2017 sobre o Acordo entre o Canadá e a União Europeia sobre a transferência dos dados dos registos de identificação dos passageiros. Com efeito, embora o Tribunal de Justiça tenha salientado, a respeito da necessidade das ingerências nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados de caráter pessoal, que a transferência dos dados PNR para o Canadá é feita independentemente de qualquer elemento objetivo que permita considerar que os passageiros são suscetíveis de representar um risco para a segurança pública no Canadá, não se trata, contudo, de uma conservação de dados sem motivo, uma vez que a conservação e a transmissão estão relacionadas com os controlos nas fronteiras aos quais estão sujeitos todos os passageiros aéreos que pretendam entrar no Canadá ou sair deste país, nos termos das leis e regulamentos em vigor no Canadá. Com a saída dos passageiros aéreos deixa de haver motivo para a conservação. Por conseguinte, a continuação da conservação após aquele momento pressupõe, como novo motivo, que existam indícios objetivos de que estes passageiros aéreos podem representar um risco em matéria de terrorismo ou de criminalidade transnacional grave.

15 Se a jurisprudência do Tribunal de Justiça dever ser entendida no sentido de que a conservação sem motivo não pode, em circunstância alguma, ser compatível com o direito da União, o recurso de «Revision» interposto pela demandada contra a sentença do Verwaltungsgericht não poderá obter provimento. Com efeito, à semelhança das normas suecas e britânicas relativas à conservação de dados, que foram objeto do Acórdão Tele2 Sverige e Watson e o., o § 113a, n.° 1, primeiro período, em conjugação com o § 113b, da TKG, não exige nem um motivo – mais amplo do que a mera utilização de serviços de acesso à internet ou de serviços telefónicos – para a conservação, nem uma relação entre os dados armazenados e uma infração penal ou um risco para a segurança pública. Pelo contrário, trata-se de uma medida legislativa que impõe a conservação sem motivo, universal e indiferenciada em termos pessoais, temporais e geográficos, da maior parte de todos os dados relevantes de tráfego de telecomunicações.

16 Contudo, o órgão jurisdicional de reenvio considera, sem prejuízo das conclusões do Acórdão Tele2 Sverige e Watson e o., que não é de excluir que a obrigação prevista no § 113a, n.° 1, primeiro período, em conjugação com o § 113b, da TKG, de conservação sem motivo de dados de tráfego de telecomunicações se possa basear no artigo 15.°, n.° 1, da Diretiva 2002/58, designadamente, pelas seguintes razões:

17 <u>Em primeiro lugar</u>, o regime das disposições controvertidas da TKG não exige a conservação de todos os dados de tráfego de telecomunicações de todos os assinantes e utilizadores registados no que diz respeito a todos os meios de comunicação eletrónicos. Não é apenas o conteúdo da comunicação que é

excluído da obrigação de conservação, os dados relativos a páginas de Internet consultadas, os dados de serviços de correio eletrónico e os dados subjacentes às ligações ou a certas comunicações no âmbito social ou eclesiástico também não podem ser armazenados (v. § 113b, n.os 5 e 6, da TKG). Embora a exclusão de alguns meios de comunicação ou de algumas categorias de dados da obrigação de conservação não afaste totalmente o risco de obtenção de um perfil global das pessoas em causa, é, pelo menos, suscetível de o reduzir consideravelmente.

18 Em segundo lugar, o órgão jurisdicional de reenvio entende, além disso, que outra diferença ainda mais relevante entre as disposições da TKG aqui em causa e o regime anterior da Diretiva 2006/24 ou as legislações sueca e britânica, baseadas neste último, e sobre as quais se debruçou o Acórdão Tele2 Sverige e Watson e o., consiste no facto de, nos termos do § 113b, n.° 1, da TKG, o prazo de conservação entre seis meses e dois anos, no máximo (v. artigo 6.° da Diretiva 2006/24) ter sofrido uma redução significativa para quatro ou dez semanas.

19 O perigo da obtenção de um perfil global das pessoas em causa também deve ser considerado tanto menor quanto mais curtos forem os períodos de conservação dos dados de tráfego. Quanto mais curto for o período de conservação, mais fragmentado é, necessariamente, o perfil da pessoa e, por conseguinte, menor é a intensidade da ingerência no direito fundamental.

20 Em terceiro lugar, as disposições da TKG aqui em causa estão significativamente restringidas no que diz respeito à proteção dos dados conservados e ao acesso ao mesmo. Por um lado, o disposto nos §§ 113d e seguintes, da TKG garante a proteção eficaz dos dados conservados contra riscos de utilização abusiva e contra qualquer acesso não autorizado. Por outro lado, nos termos do § 113c, n.° 1, da TKG, os dados conservados só podem ser utilizados para efeitos de exercício da ação penal por crimes particularmente graves e de defesa contra um perigo real para a integridade física, a vida ou a liberdade de uma pessoa ou para a existência do Estado Federal ou de um *Land*.

21 A recolha de dados de tráfego para efeitos de investigação de infrações penais pressupõe, nos termos do § 100g, n.° 2, do StPO, que exista a suspeita de prática de uma das infrações penais graves enumeradas na lei de forma exaustiva, que a infração também seja particularmente grave no caso concreto, que, de outro modo, a investigação da matéria de facto ou a localização do paradeiro do arguido fossem seriamente dificultadas ou impossíveis e que a recolha de dados seja proporcional à relevância do caso. Nos termos do § 100g, n.° 4, do StPO não é permitida a recolha ou a utilização de dados de tráfego das pessoas sujeitas a segredo profissional ao abrigo do § 53, n.° 1, primeiro período, entre as quais, advogados, médicos ou jornalistas. Além disso, o § 101a, n.° 1, do StPO prevê a sujeição a decisão judicial da recolha de dados de tráfego ao abrigo do § 100 do StPO.

22 No entanto, estas regras de acesso restritivas não se aplicam ao endereço IP atribuído aos assinantes para efeitos de utilização da Internet. Com efeito, nos

termos do § 113c, n.° 1, terceiro parágrafo, da TKG, este também pode ser utilizado no âmbito da obtenção de dados para efeitos de investigação de quaisquer infrações penais, de defesa contra riscos para a segurança pública e para a ordem pública, bem como, em termos gerais, para o cumprimento das tarefas dos serviços de informação. Contudo, há que presumir que a informação sobre o assinante que se conectou à Internet ao abrigo de um endereço IP já conhecido não é adequada para obter perfis de personalidade e de movimentação.

23 Ainda que se atendesse à argumentação da SpaceNet e se presumisse que são cada vez mais utilizados procedimentos técnicos no âmbito dos quais já não se consegue reconduzir claramente o endereço IP a um determinado endereço de telecomunicação, mas apenas a um conjunto maior de endereços e, que, consequentemente, a obtenção de dados de localização evoluiu para uma medida com uma amplitude significativa, a intensidade da ingerência dessa obtenção de dados de localização continuaria a ser claramente inferior à correspondente à própria consulta e utilização dos dados de tráfego de telecomunicações.

24 Em quarto lugar, também contribui para considerar que a obrigação de conservação de dados de tráfego de telecomunicações sem motivo prevista nos §§ 113a, n.° 1, primeiro período, em conjugação com o § 113 b, da TKG, se pode basear no artigo 15.°, n.° 1, da Diretiva 2002/58 o facto de o legislador nacional ter com a mesma cumprido o dever de intervenção que o direito à segurança garantido pelo artigo 6.° da Carta impõe aos Estados-Membros. No Acórdão Digital Rights Ireland e o., o Tribunal de Justiça mencionou expressamente o artigo 6.° da Carta e salientou, a este respeito, 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 e que o mesmo acontece com a luta contra a criminalidade grave, com o objetivo de garantir a segurança pública.

25 Neste contexto, o órgão jurisdicional de reenvio tem dúvidas sobre se a jurisprudência existente do Tribunal de Justiça deve ser entendida no sentido de que a conservação de dados sem motivo não se pode basear no artigo 15.°, n.° 1, da Diretiva 2002/58, não apenas se tiver a configuração concreta que tinha na Diretiva 2006/24 e na qual se basearam as legislações suecas e britânicas, mas em termos gerais. Com efeito, o conceito de base da conservação de dados não é consentâneo com a exigência que o Tribunal de Justiça formula sem limitação de que os dados conservados sejam diferenciados em função das pessoas, das datas e das zonas geográficas.

26 No entender do órgão jurisdicional de reenvio, a exigência de equilíbrio, por um lado, entre a obrigação dos Estados-Membros de garantirem a segurança das pessoas que se encontrem no seu território e, por outro, de respeitarem os direitos fundamentais consagrados nos artigos 7.° e 8, da Carta, também indicia que a conservação de dados sem motivo é, *per se*, incompatível com a Carta.

27 Por conseguinte, o órgão jurisdicional de reenvio não consegue retirar claramente da jurisprudência do Tribunal de Justiça que os legisladores nacionais já não

devem ter nenhuma possibilidade de introduzir a conservação de dados sem motivo, eventualmente complementada por rigorosas normas de acesso, com base numa apreciação global, a fim de terem em conta o potencial específico de risco que é associado aos novos meios de telecomunicação.

28 Em quinto lugar, o órgão jurisdicional de reenvio salienta que, caso a conservação de dados sem motivo não se possa basear, em termos gerais, no artigo 15.°, n.° 1, da Diretiva 2002/58 e se, por conseguinte, as normas concretas relativas aos meios de comunicação abrangidos, às categorias dos dados a conservar, à duração da conservação, aos requisitos de acesso aos dados conservados e à proteção contra abusos forem irrelevantes, a margem de atuação dos legisladores nacionais no domínio da ação penal e da segurança pública, que, nos termos do artigo 4.°, n.° 2, terceiro período, TUE, continua, em todo o caso, a ser da responsabilidade exclusiva dos Estados-Membros, seria consideravelmente restringida.

29 Por último, em sexto lugar, o órgão jurisdicional de reenvio considera que a questão de saber se as considerações do Tribunal de Justiça no Acórdão Tele2 Sverige e Watson e o. devem ser entendidas como uma proibição dirigida aos Estados-Membros, de basearem a introdução de uma obrigação de conservação de dados de tráfego de telecomunicações sem motivo no artigo 15.°, n.° 1, da Diretiva 2002/58, também parece não estar esclarecida, no contexto da jurisprudência mais recente do Tribunal Europeu dos Direitos do Homem (TEDH).

30 O TEDH declarou recentemente, num Acórdão de 19 de junho de 2018, que o regime jurídico sueco relativo à vigilância em larga escala do tráfego de dados transfronteiriço é compatível com o artigo 8.°, da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH). Tendo em conta as ameaças a que os Estados estão atualmente sujeitos, incluindo o flagelo do terrorismo global e outros crimes graves tais como o tráfico de drogas, o tráfico de seres humanos, a exploração sexual infantil e a criminalidade na Internet, assim como o progresso da tecnologia que ajuda os terroristas e os criminosos a evitarem ser identificados na Internet, e ainda a imprevisibilidade das vias de transmissão de dados eletrónicos, a decisão de criar um sistema de vigilância em larga escala a fim de detetar ameaças até agora desconhecidas à segurança nacional continua a estar inserida na margem de apreciação do Estado (TEDH, Acórdão de 19 de junho de 2018, n.° 35252/08 [ECLI:CE:ECHR:2018:0619JUD003525208], Centrum för Rättvisa/Suécia, n.° 112). O TEDH, ao referir a imprevisibilidade das vias de transmissão de dados eletrónicos e o desenvolvimento da tecnologia que ajuda os terroristas e os criminosos a evitarem ser identificados na Internet, salienta de um modo mais veemente do que o Tribunal de Justiça da União Europeia o potencial de risco específico associado aos novos meios de telecomunicação.

31 O órgão jurisdicional de reenvio remete para o considerando 11 da Diretiva 2002/58 e para o artigo 52.°, n.° 3, da Carta, dos quais resulta que deve ser criada a necessária coerência entre os direitos consagrados na Carta e os direitos

correspondentes garantidos pela CEDH, sem prejuízo da independência do direito da União e do Tribunal de Justiça da União Europeia.

32 Por último, o órgão jurisdicional de reenvio cita outros processos de decisão prejudicial nos quais está em causa a interpretação do Acórdão Tele2 Sverige e Watson e o., ou seja, a questão de saber se dele resulta uma proibição geral de conservação de dados sem motivo que não pode ser contornada tendo em conta a importância dos perigos para a segurança pública a combater, nem pode ser contornada mediante «compensação» através de disposições restritivas relativas ao acesso e um elevado nível de exigências de segurança.

33 São referidos os pedidos de decisão prejudicial do Investigatory Powers Tribunal - London (Reino Unido) (C-623/17), os pedidos de decisão prejudicial do Conseil d'État (França) (C-511/18 e C-512/18) e o pedido de decisão prejudicial do Tribunal Constitucional belga (C-520/18).