Tribunal de Justiça da União Europeia
COMUNICADO DE IMPRENSA n.° 145/16
Luxemburgo, 21 de dezembro de 2016

Imprensa e Informação

Acórdão nos processos apensos C-203/15 Tele2 Sverige AB/ Post-och telestyrelsen e C-698/15 Secretary of State for the Home Department/Tom Watson e o.

Os Estados-Membros não podem impor uma obrigação geral de conservação de dados aos prestadores de serviços de comunicações eletrónicas

O direito da União opõe-se a uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, mas os Estados-Membros podem prever, a título preventivo, uma conservação desses dados com o único objetivo de lutar contra a criminalidade grave, desde que essa conservação seja limitada ao estritamente necessário no que respeita às categorias de dados a conservar, aos meios de comunicação visados, às pessoas afetadas e à duração da conservação estabelecida. O acesso das autoridades nacionais aos dados conservados deve ser sujeito a condições, incluindo nomeadamente um controlo prévio por parte de uma autoridade independente e a conservação dos dados no território da União

No seu acórdão Digital Rights Ireland de 2014 [1], o Tribunal de Justiça declarou inválida a diretiva sobre a conservação de dados [2] pelo facto de a ingerência que a obrigação geral de conservação dos dados de tráfego e dos dados de localização, imposta por esta diretiva, comporta nos direitos fundamentais ao respeito da vida privada e à proteção de dados de caráter pessoal não ser limitada ao estritamente necessário.

Na sequência deste acórdão, deram entrada no Tribunal de Justiça dois processos relativos à obrigação geral imposta, na Suécia e no Reino Unido, aos prestadores de serviços de comunicações eletrónicas de conservar os dados relativos a essas comunicações, cuja conservação estava prevista na diretiva declarada inválida.

No dia seguinte à prolação do acórdão Digital Rights Ireland, a empresa de telecomunicações Tele2 Sverige notificou a autoridade sueca de supervisão dos correios e telecomunicações da sua decisão de deixar de proceder à conservação dos dados e da sua intenção de apagar os dados já registados (processo C-203/15). Com efeito, o direito sueco obriga os prestadores de serviços de comunicações eletrónicas a conservar de maneira sistemática e contínua, sem exceção, todos os dados de tráfego e de localização de todos seus assinantes e utilizadores inscritos, relativamente a todos os meios de comunicação eletrónica.

No processo C-698/15, Tom Watson, Peter Brice e Geoffrey Lewis recorreram do regime britânico de conservação de dados que permite ao Ministro do Interior obrigar os operadores de telecomunicações públicas a conservar todos os dados relativos às comunicações pelo período máximo de doze meses, entendendo-se que a conservação do conteúdo dessas comunicações está excluída.

A pedido do Kammarrätten i Stockholm (Tribunal Administrativo de Segunda Instância de Estocolmo, Suécia) e da Court of Appeal (England and Wales) (Civil Division) (Secção Cível do Tribunal de Segunda Instância de Inglaterra e do País de Gales, Reino Unido), o Tribunal de Justiça é convidado a pronunciar-se sobre se os regimes nacionais que impõem aos prestadores uma obrigação geral de conservação de dados e preveem o acesso das autoridades nacionais

[1] Acórdão do Tribunal de Justiça de 8 de abril de 2014, *Digital Rights Ireland e Seitlinger e o.* (processos apensos C-293/12 e C-594/12, v. CI n° 54/14).
[2] 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).

competentes aos dados conservados, sem limitar, nomeadamente, esse acesso aos fins da luta contra a criminalidade grave e sem submeter o acesso a um controlo prévio por um órgão jurisdicional ou uma autoridade administrativa independente, são compatíveis com o direito da União (neste caso, a diretiva «vida privada e comunicações eletrónicas» [3], lida à luz da Carta dos Direitos Fundamentais da UE [4]).

No seu acórdão de hoje, **o Tribunal de Justiça responde que o direito da União se opõe a uma legislação nacional que preveja uma conservação generalizada e indiferenciada dos dados.**

O Tribunal confirma, antes de mais, que **as medidas nacionais** em causa **estão abrangidas pelo âmbito de aplicação da diretiva.** Com efeito, a proteção da confidencialidade das comunicações eletrónicas e dos dados de tráfego, garantida pela diretiva, aplica-se às medidas tomadas por quaisquer pessoas que não sejam utilizadores, quer se trate de pessoas ou entidades privadas ou de entidades públicas.

O Tribunal declara, em seguida, que, embora esta diretiva permita aos Estados-Membros limitar o alcance da obrigação de princípio de assegurar a confidencialidade das comunicações e dos respetivos dados de tráfego, não pode justificar que a derrogação dessa obrigação de princípio e, em especial, a proibição de armazenamento desses dados, nela prevista, se torne a regra.

Além disso, o Tribunal recorda a sua jurisprudência constante segundo a qual a proteção do direito fundamental ao respeito da vida privada exige que **as derrogações** à proteção de dados pessoais **sejam realizadas nos limites do estritamente necessário.** O Tribunal aplica esta jurisprudência às regras que regulam a conservação de dados e às que regulam o acesso aos dados conservados.

O Tribunal declara, **no que respeita à conservação**, que os dados conservados considerados no seu todo **podem permitir tirar conclusões muito precisas sobre a vida privada das pessoas** cujos dados foram conservados.

A ingerência resultante de uma legislação nacional que preveja a conservação dos dados de tráfego e dos dados de localização deve, portanto, ser considerada particularmente grave. O facto de a conservação de dados ser efetuada sem que os utilizadores dos serviços de comunicações eletrónicas sejam disso informados pode gerar, no espírito das pessoas afetadas, o sentimento de que a sua vida privada é objeto de constante vigilância. Por conseguinte, **apenas a luta contra a criminalidade grave pode justificar essa ingerência.**

O Tribunal salienta que uma **legislação que preveja uma conservação generalizada e indiferenciada de dados não requer uma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública** e não se limita, nomeadamente, a prever uma conservação de dados referentes a um período temporal e/ou uma zona geográfica e/ou um círculo de pessoas suscetíveis de estar implicadas numa infração grave. **Tal legislação nacional excede assim os limites do estritamente necessário e não pode ser considerada justificada numa sociedade democrática, como exige a diretiva lida à luz da Carta.**

O Tribunal explica, em contrapartida, que **a diretiva não se opõe a uma legislação nacional que imponha uma conservação seletiva dos dados** para efeitos de luta contra a criminalidade grave**, desde que essa conservação seja**, no que respeita às categorias de dados a conservar, aos meios de comunicação visados, às pessoas afetadas e à duração da conservação estabelecida, **limitada ao estritamente necessário**. Segundo o Tribunal, **qualquer legislação nacional que vá neste sentido deve ser clara e precisa e prever garantias suficientes** que protejam os dados contra os riscos de abuso. Deve indicar as circunstâncias e as condições em

[3] 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).

[4] Artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia.

que uma medida de conservação de dados pode ser tomada a título preventivo, de modo a garantir que a amplitude dessa medida seja, na prática, efetivamente limitada ao estritamente necessário. Tal legislação deve, nomeadamente, **basear-se em elementos objetivos** que permitam identificar as pessoas cujos dados possam estar relacionados com atos de criminalidade grave, contribuir para a luta contra a criminalidade grave ou prevenir um risco grave para a segurança pública.

No que se refere ao **acesso das autoridades nacionais competentes aos dados conservados**, o Tribunal declara que a legislação nacional em causa não se pode limitar a exigir que o acesso corresponda a um dos objetivos visados na diretiva, ainda que seja a luta contra a criminalidade grave, mas deve prever igualmente os requisitos materiais e processuais que regulam o acesso das autoridades nacionais competentes aos dados conservados. Esta legislação deve basear-se em **critérios objetivos para definir as circunstâncias e os requisitos em que o acesso aos dados deve ser concedido às autoridades nacionais competentes.** Em princípio, só pode ser concedido o acesso, no que se refere ao objetivo da luta contra a criminalidade, aos dados de pessoas suspeitas de projetar, cometer ou ter cometido uma infração grave ou ainda de estar implicadas, de uma forma ou de outra, numa dada infração. Todavia, em situações particulares, como aquelas em que interesses vitais de segurança nacional, de defesa ou de segurança pública estão ameaçados por atividades de terrorismo, pode ser também concedido o acesso aos dados de outras pessoas quando existam elementos objetivos que permitam considerar que esses dados podem, num caso concreto, dar uma contribuição efetiva na luta contra essas atividades.

Acresce que o Tribunal considera **que é essencial que o acesso aos dados conservados seja subordinado, salvo em caso de urgência, a um controlo prévio** efetuado por um órgão jurisdicional ou uma entidade independente. Além disso, as autoridades nacionais competentes a quem o acesso aos dados conservados foi concedido devem informar desse facto as pessoas em causa.

Tendo em conta a quantidade de dados conservados, o caráter sensível desses dados e o risco de acesso ilícito aos mesmos, **a legislação nacional deve prever que os dados sejam conservados no território da União** e que sejam irremediavelmente destruídos no termo do prazo previsto para a sua conservação.

NOTA: O reenvio prejudicial permite aos órgãos jurisdicionais dos Estados-Membros, no âmbito de um litígio que lhes seja submetido, interrogar o Tribunal de Justiça sobre a interpretação do direito da União ou sobre a validade de um ato da União. O Tribunal de Justiça não resolve o litígio nacional. Cabe ao órgão jurisdicional nacional decidir o processo em conformidade com a decisão do Tribunal de Justiça. Esta decisão vincula também os outros órgãos jurisdicionais nacionais aos quais seja submetido um problema semelhante.

Contacto Imprensa: Liliane Fonseca Almeida ☎ (+352) 4303 3667