Tribunal de Justiça
COMUNICADO DE IMPRENSA n.° 58/22
Luxemburgo, 5 de abril de 2022

Imprensa e Informação

Acórdão no processo C-140/20
Commissioner of the Garda Síochána e o.

O Tribunal de Justiça confirma que o direito da União se opõe a uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização relativos às comunicações eletrónicas para efeitos de luta contra as infrações graves

Um órgão jurisdicional não pode limitar no tempo os efeitos de uma declaração de invalidade de uma legislação nacional que preveja essa conservação

Em março de 2015, G.D. foi condenado a uma pena de prisão perpétua pelo homicídio de uma mulher na Irlanda. No recurso da sua condenação interposto no Court of Appeal (Tribunal de Recurso, Irlanda), o interessado acusou nomeadamente o órgão jurisdicional de primeira instância de ter, erradamente, admitido como meios de prova dados de tráfego e dados de localização relativos a chamadas telefónicas. Para poder impugnar, no âmbito do processo penal, a admissibilidade das referidas provas, G.D. instaurou paralelamente na High Court (Tribunal Superior, Irlanda) uma ação cível com vista a obter a declaração da invalidade de determinadas disposições da Lei irlandesa de 2011 relativa à conservação e ao acesso a esses dados, por considerar que a mesma violava os direitos que lhe são conferidos pelo direito da União. Por Decisão de 6 de dezembro de 2018, a High Court julgou procedente a argumentação de G.D., tendo a Irlanda interposto recurso dessa decisão na Supreme Court (Supremo Tribunal, Irlanda), que é o órgão jurisdicional de reenvio no presente processo.

Com o seu reenvio, a Supreme Court pediu esclarecimentos sobre os requisitos do direito da União em matéria de conservação dos referidos dados para efeitos de luta contra as infrações graves, bem como sobre as garantias necessárias em matéria de acesso a esses mesmos dados. Questiona-se, além disso, sobre o alcance e os efeitos no tempo de uma eventual declaração de incompatibilidade que venha a pronunciar, uma vez que a Lei irlandesa de 2011 foi adotada para transpor a Diretiva 2006/24/CE [1], declarada inválida pelo Tribunal de Justiça no Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. [2].

No seu acórdão, o Tribunal de Justiça, reunido em Grande Secção, confirma, em primeiro lugar, a sua jurisprudência constante [3], segundo a qual o direito da União [4] **se opõe a medidas legislativas nacionais que preveem, a título preventivo, uma conservação generalizada e**

[1] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO 2006, L 105, p. 54).
[2] Acórdão de 8 de abril de 2014, *Digital Rights Ireland,* C-293/12, (v. CI n.º 54/14).
[3] Acórdãos de 8 de abril de 2014, *Digital Rights Ireland,* C-293/12; Acórdão de 21 de dezembro de 2016, *Tele2 Sverige e Watson e o.,* C-203/15 e C--698/15 (v. CI n.º 145/16); de 6 de outubro de 2020, *Privacy International,* C-623/17, *e La Quadrature du Net e o.,* C-511/18, C-512/18, *Ordre des barreaux francophones et germanophone e o.,* C-520/18 (v. CI n.º 123/20); e de 2 de março de 2021, *Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas),* C-746/18 (v. CI n.° 29/21).
[4] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 210, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, (JO 2009, L 337, p. 11) (a seguir «Diretiva relativa à privacidade e às comunicações eletrónicas», lida à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

indiferenciada dos dados de tráfego e dos dados de localização relativos às comunicações eletrónicas, para efeitos da luta contra as infrações graves.

Com efeito, a Diretiva relativa à privacidade e às comunicações eletrónicas não se limita a enquadrar o acesso a esses dados através de garantias destinadas a prevenir abusos, mas consagra, em especial, o **princípio da proibição do armazenamento** dos dados de tráfego e dos dados de localização. A conservação destes dados constitui assim, por um lado, uma derrogação desta proibição de armazenamento e, por outro, uma ingerência nos direitos fundamentais do respeito pela vida privada e da proteção dos dados pessoais, consagrados nos artigos 7.° e 8.° da Carta.

Embora a Diretiva relativa à privacidade e às comunicações eletrónicas permita aos Estados-Membros restringirem esses direitos e essas obrigações para efeitos, nomeadamente, da luta contra as infrações penais, essas restrições devem, contudo, respeitar nomeadamente o princípio da proporcionalidade. Este princípio exige o respeito não apenas dos requisitos de adequação e de necessidade, como também do requisito relativo ao **caráter proporcional** dessas medidas relativamente ao objetivo prosseguido. Assim, o Tribunal de Justiça já declarou que o objetivo de luta contra a criminalidade grave, por muito fundamental que seja, não pode, por si só, justificar que uma medida de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, como a que foi instituída pela Diretiva 2006/24, seja considerada necessária. Na mesma ordem de ideias, mesmo as obrigações positivas dos Estados-Membros relativas à aplicação de regras que permitem uma luta efetiva contra as infrações penais não podem ter por efeito justificar ingerências tão graves, como as que comporta uma legislação nacional que prevê essa conservação, nos direitos fundamentais de quase toda a população, sem que os dados das pessoas em causa sejam suscetíveis de revelar uma ligação, no mínimo indireta, com o objetivo prosseguido.

O Tribunal de Justiça recorda ainda que incumbem aos poderes públicos diferentes obrigações positivas por força da Carta, que consistem, por exemplo, na adoção de medidas jurídicas destinadas a proteger a vida privada e familiar, à proteção do domicílio e das comunicações, mas também à proteção da integridade física e psíquica das pessoas e à proibição da tortura e dos tratos desumanos e degradantes. Cabe-lhes, por conseguinte, proceder a uma **conciliação dos diferentes interesses legítimos e direitos em causa**. Com efeito, um objetivo de interesse geral não pode ser prosseguido sem se ter em conta o facto de que deve ser conciliado com os direitos fundamentais abrangidos pela medida, e isso mediante uma **ponderação equilibrada** entre, por um lado, esse objetivo de interesse geral e, por outro, os direitos em causa, através da verificação simultânea de que a importância do referido objetivo está relacionada com a gravidade da ingerência que essa medida implica.

Estas considerações levam o Tribunal de Justiça a rejeitar, nomeadamente, a argumentação de que a criminalidade particularmente grave pode ser equiparada a uma ameaça para a segurança nacional que se revele real e atual ou previsível e de que pode, durante um período temporalmente limitado, justificar uma medida de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização. Com efeito, essa ameaça distingue-se, pela sua natureza, a sua gravidade e o caráter específico das circunstâncias que a constituem, do risco geral e permanente de ocorrência de tensões ou de perturbações, ainda que graves, à segurança pública ou do risco de infrações penais graves.

Em contrapartida, o Tribunal de Justiça declara, em segundo lugar e confirmando a sua jurisprudência anterior, que o direito da União não se opõe a medidas legislativas que prevejam, nas condições enunciadas no seu acórdão, para efeitos de luta contra a criminalidade grave e de prevenção de ameaças graves contra a segurança pública:

- **uma conservação seletiva dos dados de tráfego e dos dados de localização** em função de categorias de pessoas em causa ou através de um critério geográfico;

- **uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação;**

- **uma conservação generalizada e indiferenciada dos dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos,** e

- uma **conservação** rápida (*quick freeze*) dos dados de tráfego e dos dados de localização de que esses **prestadores** de serviços dispõem.

O Tribunal de Justiça procede a diversas precisões em relação a estas diferentes categorias de medidas.

Em primeiro lugar, as autoridades nacionais competentes podem adotar uma medida de conservação seletiva baseada num critério geográfico, como nomeadamente a taxa média de criminalidade numa zona geográfica, sem disporem necessariamente de indícios concretos relativos à preparação ou à prática, nas zonas em causa, de atos de criminalidade grave. Mais acrescenta que, se uma medida de conservação seletiva desse tipo visar locais ou infraestruturas regularmente frequentados por um número muito elevado de pessoas ou locais estratégicos, como aeroportos, estações, portos marítimos ou zonas de portagens, a mesma é suscetível de permitir às autoridades competentes obter informações sobre a presença, nesses locais ou zonas geográficas, das pessoas que aí utilizam um meio de comunicação eletrónica e daí retirar conclusões sobre a sua presença e a sua atividade nos referidos locais ou zonas geográficas para efeitos da luta contra a criminalidade grave.

Em seguida, o Tribunal de Justiça indica que nem a Diretiva relativa à privacidade e às comunicações eletrónicas nem nenhum outro ato do direito da União se opõem a uma legislação nacional que tenha por objeto a luta contra a criminalidade grave, nos termos da qual a aquisição de um meio de comunicação eletrónica, como um cartão SIM pré-pago, esteja sujeita à verificação de documentos oficiais que comprovem a identidade do comprador e ao registo, pelo vendedor, das informações daí resultantes, sendo o vendedor obrigado, se for caso disso, a dar acesso a essas informações às autoridades nacionais competentes.

Por último, o Tribunal de Justiça salienta que a Diretiva relativa à privacidade e às comunicações eletrónicas não se opõe a que as autoridades nacionais competentes ordenem uma medida de conservação rápida desde a primeira fase do inquérito sobre uma ameaça grave para a segurança pública ou sobre um eventual ato de criminalidade grave, a saber, a partir do momento em que, segundo as disposições pertinentes do direito nacional, essas autoridades podem dar início a esse inquérito. Essa medida pode ser alargada aos dados de tráfego e aos dados de localização relativos a pessoas diferentes das que são suspeitas de ter planeado ou cometido uma infração grave ou uma ofensa à segurança nacional, desde que tais dados possam, com base em elementos objetivos e não discriminatórios, contribuir para o esclarecimento dessa infração ou dessa ofensa à segurança nacional, tais como os dados da vítima desta e do seu meio social ou profissional.

Estas diferentes medidas podem, consoante a escolha do legislador nacional e respeitando os limites do estritamente necessário, ser aplicadas conjuntamente.

O Tribunal de Justiça rejeita ainda a argumentação segundo a qual as autoridades competentes deveriam poder aceder, para efeitos da luta contra a criminalidade grave, aos dados de tráfego e aos dados de localização que foram conservados de maneira generalizada e indiferenciada em conformidade com a sua jurisprudência, para dar resposta a uma ameaça grave para a segurança nacional que se revele real e atual ou previsível. Com efeito, esta argumentação faz depender esse acesso de circunstâncias alheias ao objetivo de luta contra a criminalidade grave. Além disso, segundo a referida argumentação, o acesso poderia ser justificado por um objetivo de menor importância do que o que justificou a conservação, a saber a salvaguarda da segurança nacional, o que iria contra a hierarquia dos objetivos de interesse geral no âmbito da qual se deve apreciar a proporcionalidade de uma medida de conservação. Por outro lado, autorizar esse acesso poderia privar de qualquer efeito útil a proibição de proceder a essa conservação generalizada e indiferenciada para efeitos da luta contra a criminalidade grave.

Em terceiro lugar, o Tribunal de Justiça confirma que o direito da União se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas, que emanam da polícia no âmbito da investigação e da repressão de infrações penais graves, incumbe a um agente de polícia, mesmo quando este é assistido por uma unidade instituída no âmbito da polícia que goza de um certo grau de autonomia no exercício da sua missão e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional. A este respeito, o Tribunal confirma, com efeito, a sua jurisprudência segundo a qual a fim de garantir, na prática, o pleno respeito das condições estritas de acesso a dados pessoais tais como os dados de tráfego e de localização, o acesso das autoridades nacionais competentes aos dados conservados deve estar sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente, devendo a decisão desse órgão jurisdicional ou dessa entidade ser tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal. Ora, um agente de polícia não constitui um órgão jurisdicional e não apresenta todas as garantias de independência e de imparcialidade exigidas para poder ser qualificado de entidade administrativa independente.

Em quarto e último lugar, o Tribunal de Justiça confirma a sua jurisprudência segundo a qual o direito da União se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com a Diretiva relativa à privacidade e às comunicações eletrónicas.

Dito isto, o Tribunal de Justiça recorda que a admissibilidade dos meios de prova obtidos através dessa conservação cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade.

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 não resolve o litígio nacional. Cabe ao órgão jurisdicional nacional decidir o processo em conformidade com a decisão do Tribunal. Esta decisão vincula do mesmo modo os outros órgãos jurisdicionais nacionais aos quais seja submetido um problema semelhante.

Contacto Imprensa: Cristina López Roca ☎ (+352) 4303 3667.